Cisco Virtualized Infrastructure Manager Documentation, 3.4.3 to 3.4.5

First Published: 2020-03-19

Last Modified: 2021-04-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Release Notes

Release Notes

Cisco VIM 3.4.3 Release Notes

Cisco VIM 3.4.3 Release Notes

Release Date

First Published: March 19, 2020

Updated:

- March 24, 2020: Added the *Documentation* section to include a list of pages that are updated.
- March 25, 2020: Updated the *Documentation* section.
- March 26, 2020: Updated the *Documentation* section.
- March 30, 2020: Updated the *Documentation* section.
- March 31, 2020: Updated the *Documentation* section and *Known Caveats*.
- April 02, 2020: Updated the *Documentation* section.
- April 03, 2020: Updated the *Documentation* section.
- April 08, 2020: Updated the *Features of Cisco VIM* and *Documentation* section.
- April 10, 2020: Updated the *Features of Cisco VIM* and *Documentation* section.
- April 13, 2020: Updated the *Documentation* section.
- April 15, 2020: Updated the *Documentation* section.
- April 22, 2020: Updated the *Documentation* section.
- April 23, 2020: Updated the *Documentation* section.
- April 27, 2020: Updated the *Documentation* section.
- April 30, 2020: Updated the *Documentation* section.
- May 06, 2020: Updated the *Documentation* section.
- May 20, 2020: Updated the *Documentation* section.
- May 25, 2020: Updated the *Documentation* section.
- June 08, 2020: Updated the *Documentation* section.
- June 18, 2020: Updated the *Documentation* section.
- June 25, 2020: Updated the *Documentation* section.
- July 21, 2020: Updated the *Documentation* section.
- July 27, 2020: Updated the *Documentation* section.
- Aug 06, 2020: Updated the *Documentation* section.
- Aug 14, 2020: Updated the *Documentation* section.
- Aug 20, 2020: Updated the *Documentation* section.
- Sep 04, 2020: Updated the *Documentation* section.
- Sep 09, 2020: Updated the *Documentation* section.
- Sep 11, 2020: Updated the *Documentation* section.
- Sep 14, 2020: Updated the *Documentation* section.
- Oct 07, 2020: Updated the *Documentation* section.
- Oct 16, 2020: Updated the *Documentation* section.
- Oct 21, 2020: Updated the *Documentation* section.
- Oct 23, 2020: Updated the *Documentation* section.
- Oct 28, 2020: Updated the *Documentation* section.
- Nov 11, 2020: Updated the *Documentation* section.
- Nov 16, 2020: Updated the *Documentation* section.
- Dec 09, 2020: Updated the *Documentation* section.
- Dec 17, 2020: Updated the *Documentation* section

Introduction

Cisco Network Function Virtualization Infrastructure (Cisco NFVI) provides the virtual layer and hardware environment in which virtual network functions (VNFs) operate. VNFs provide a well-defined network function that offers routing, intrusion, detection, Domain Name Service (DNS), caching, Network Address Translation (NAT), and other network functions. While the network functions required a tight integration between a network software and hardware in the past, VNFs decouple the software from the underlying hardware.

Cisco NFVI 3.4.3 is based on the Queens release of OpenStack, an open source cloud operating system that controls large pools of compute, storage, and networking resources. The Cisco version of OpenStack is Cisco Virtualized Infrastructure Manager (Cisco VIM). Cisco VIM manages the OpenStack compute, network, and storage services, and all Cisco NFVI build and control functions.

Key roles of Cisco NFVI pods are:

- Control (including Networking)
- Computes
- Storage

- Management, logging, and monitoring

Hardware that is used to create the Cisco NFVI pods include:

- Cisco Unified Computing System (UCS) C240 M4 or C240 M5 or C220 M5-Performs management and storage functions, and services. Includes dedicated Ceph (UCS 240-M4 or UCS 240-M5) distributed object store and the file system. Only Red Hat Ceph is supported.
- Cisco UCS C220/240 M4 or M5-Performs control and compute services.
- HP DL 360 Gen9-Supports as a third-party compute, where the control plane is Cisco UCS servers.
- Cisco UCS B200 M4 blades-Can be used instead of the UCS C220 for compute and control services. The B200 blades and C240 Ceph server are joined with redundant Cisco Fabric Interconnects that are managed by UCS Manager.
- Combination of M5 series servers for VIC or NIC (40G) based hyper-converged and Micropod offering.
- Quanta servers-An alternate for Cisco UCS servers used for the installation of the cloud both at the core and edge. Supports automated installation of the Central Ceph cluster on the edge pod for Glance image services.

The UCS C240 and C220 servers are M4/M5 Small Form Factor (SFF) models, where the operating systems boot from Hard Disk Drive (HDD)/Solid State Drive (SDD) for control/compute nodes, and boot from internal SSD for Ceph nodes. Cisco supports pure Intel NIC configuration and Cisco 40G VIC with Intel NIC configuration.

Software applications that manage Cisco NFVI hosts and services include:

- Red Hat Enterprise Linux (RHEL) 7.6 with OpenStack Platform 13.0-Provides the core Operating system with OpenStack capability. RHEL 7.6 and OSP 13.0 are installed on all Cisco NFVI UCS servers.
- Cisco VIM-An OpenStack orchestration system that helps to deploy and manage an OpenStack cloud offering from bare metal installation to OpenStack services, considering the hardware and software redundancy, security, and monitoring. OpenStack Queens release with more features and usability enhancements are tested for functionality, scale, and performance.
- Cisco Unified Management (UM)-Deploys, provisions, and manages Cisco VIM on Cisco UCS servers. It provides UI to manage multiple pods, when installed on a dedicated server Unified Management node.
- Cisco VIM Monitor-Used to provide integrated monitoring and alerting of the NFV Infrastructure layer.
- Cisco UCS Manager-Used to perform certain management functions, when UCS B200 blades are installed.
- Cisco Integrated Management Controller (IMC)-When installing Cisco VIM, Cisco IMC 2.0(13i) or later is supported, but certain IMC versions are recommended and listed in the below table.
  For the Cisco IMC 2.0 lineup, the recommended version information is as follows:

UCS-M4 servers	Cisco recommends Cisco IMC 2.0(13n) or later

  For the Cisco IMC 3.x lineup, the recommended version is as follows:

UCS-M4 servers	• Cisco IMC versions are 3.0(3a) or later, except for 3.0(4a). • Cisco recommends Cisco IMC 3.0(4d). • Extended support of 4.0(1a), 4.0(1b), and 4.0(1c).
UCS-M5 servers	• Support CIMC 3.1(2b), 4.0(1a), 4.0(1c), 4.0(2f), 4.0(4d), 4.0(4h) and 4.0(4i) • Do not use 3.1(3c) to 3.1(3h), 3.0(4a), 4.0(2c), or 4.0(2d). • A minimum bundle version of CIMC 4.0(4d) is required for Cascade Lake support. • For GPU support, you must ensure that the server has CIMC 4.0(2f).

  ⚠ The CIMC versions are tested and available in the allowed list. However, the higher versions might work as well.

- Cisco Virtual Topology System (VTS): It is a standard-based, open, overlay management and provisioning system for data center networks. It automates DC overlay fabric provisioning for physical and virtual workloads.
- Cisco Virtual Topology Forwarder (VTF): Includes VTS. VTF leverages Vector Packet Processing (VPP) to provide high performance Layer 2 and Layer 3 VXLAN packet forwarding.

Layer 2 networking protocols include:

- VXLAN supported using Linux Bridge.
- VTS VXLAN supported using ML2/VPP.
- VLAN supported using Open vSwitch (OVS).
- VLAN supported using ML2/VPP. It is supported only on Intel NIC.
- VLAN supported using ML2/ACI.

For pods based on C-series with Intel NIC Single Root I/O Virtualization (SRIOV), the SRIOV allows a single physical PCI Express to be shared on a different virtual environment. The SRIOV offers different virtual functions to different virtual components over the same physical NIC.
You can use any connection protocol unless you install UCS B200 blades with the UCS Manager plugin, in which case, only OVS over VLAN can be used.

If you use only VIC, VPP as a mechanism driver is not supported, and the B-series deployment is limited to OVS.

Features of Cisco VIM

Cisco VIM is the only standalone fully automated cloud lifecycle manager offered by Cisco for the private cloud. It integrates with Cisco C-series or B-series UCS servers and, Cisco VIC and Intel NIC and helps cloud administrators set up and manage private clouds.

The following are the features of Cisco VIM:

Feature Name	Comments
OpenStack version	RHEL 7.6 with OSP 13 (Queens) Kernel Details: RedHat 7.6 EUS Kernel and OSP13 from 1/21/2020. • RHEL 7.6 Real Time Version: 3.10.0-957.46.1.rt56.963.el7 • RHEL 7.6 Version: 3.10.0-957.43.1.el7.x86_6
Hardware support matrix	• UCS C220/B200 M4 controller or compute with Intel V3 (Haswell) • UCS C240/220 M4 controller or compute with Intel V4 (Broadwell) • UCS C240/220 M5 controller or compute with Intel Skylake or Cascade Lake • HP DL360 Gen 9 with control plane on Cisco UCS M4 servers • UCS C220/240 M5 in a Micropod environment, with an option to add up to 16 UCS C220/240 M5 computes • UCS C240/220 M5 controller or compute with Intel X710 NIC and SR-IOV and Cisco Nexus 9000 or Cisco NCS 5500 series switch as ToR • UCS C240/220 M5 servers with Cisco 1457 (for control plane) and Intel XXV710 NIC (for data plane with VPP) and SR-IOV • Support of physical GPU in M5 • Support of vGPU in M5* (Tech-preview) • Quanta servers as an alternative to Cisco UCS servers for fullon, micro (D52BQ-2U 3UPI), and edge (D52BE-2U) deployment of the cloud • Quanta sever support with Skylake or Cascade Lake* Intel CPUs • Quanta servers for Central Glance (D52BQ-2U 3UPI) server to offer glance image services to edge pod • SATA M.2 (960G) as an option for a boot drive
NIC support	• Cisco VIC: VIC 1227, 1240, 1340, 1380, 1387 (for M5) in 40G VIC/NIC offering, 1457 • Intel NIC: X710, 520, XL710, xxv710 (25G)

Pod type	• Dedicated control, compute, and storage (C-series) node running on Cisco VIC (M4) or Intel X710 (for M4 or M5) (full on) with Cisco Nexus 9000 or Cisco NCS 5500 series switch (only for Intel NIC and VPP as mechanism driver) as ToR. For fullon pods based on Quanta (D52BE-2U) servers, the NIC is xxv710 (25G) with Cisco Nexus 9000 as ToR. Support of UCS-M4 (10G VIC with 2-XL710) compute with UCS-M5 (Cisco VIC 1457 with 2-XL710). • Dedicated control, compute, and storage (C-series) node running on Cisco VIC and Intel NIC (full on) with Cisco Nexus 9000 as ToR. Only SRIOV is supported on Intel NIC. Support of Intel X520 (with 2 NIC cards or compute) on M4 pods or XL710 (2 or 4 NIC cards or compute) on M4/M5 pods for SRIOV cards in the VIC/NIC combination. For M4 pods, VIC or NIC computes running XL710 and X520 can reside in the same pod. Few computes can run with or without SRIOV in a given pod. • Dedicated control, compute, and storage (UCS M5 SFF C-series) node running on Cisco VIC 1457 and Intel xxv710 NIC (full on) with Cisco Nexus 9000 as ToR. Only SRIOV is supported on Intel NIC. With VPP and OVS as the mechanism driver, the number of SRIOV ports are 2 or 4, respectively. • VTS support extended to include UCS-M5 computes with Cisco VIC 1457 in an existing M4-based pod running on VIC 1227. • Dedicated control, compute, and storage (B-Series) node running on Cisco NIC. • Micropod: Integrated (AIO) control, compute, and storage (C-series) node running on Cisco VIC, Intel X710X, or VIC and NIC combinations. Micropod can be optionally expanded to accommodate more computes (up to 16) running with the same NIC type. This can be done as a Day 0 or Day 1 activity. The computes can boot off HDD or SSD. From Cisco VIM 3.4.1, the Micropod option has been extended to Quanta (D52BE-2U) servers with Intel XXV710 NIC (25G) and Cisco Nexus 9000 (-FX series) as ToR. • Hyper-converged on M4 (UMHC): Dedicated control and compute nodes with all storage acting as compute nodes (M4 C-series) and running on a combination of 1xCisco VIC (1227) and 2x10GE 520 or 2x40GE 710XL Intel NIC with an option to migrate from one to another. You can extend the pod to M5-based computes with 40G Cisco VIC along with 2x40GE 710XLNIC (optionally). • NGENA Hyper-Converged (NGENAHC): Dedicated control and compute nodes, with all storage acting as compute (C-series) nodes. All nodes have a combination of 1xCisco VIC (1227) for control plane, and 1x10GE 710X Intel NIC for data plane over VPP. • Support of M5 as a controller and hyper-converged nodes (with 1457 for the control plane, and 1x10GE X710 (2 port) Intel NIC for data plane) in an existing M4 based pod. • Hyper-converged on M5: Dedicated control and compute nodes with all storage acting as compute (C-series) nodes, running on a combination of 1xCisco VIC (40G) and 2x40GE 710XL Intel NIC. Support of M5 as controller and hyper-converged nodes (with 1457 for control plane, and 1x10GE X710 (2 port) Intel NIC for data plane) in an existing M4-based pod. • Edge: Available with restricted power and limited rack space. Quanta (D52BQ-2U 3UPI) servers with three converged control and compute nodes, expandable to 16 additional compute nodes. The edge cloud communicates with Quanta server based Central Ceph cluster for glance service. Persistent storage is not available. • Ceph: Designed to provide glance image services to edge cloud. Quanta (D52BE-2U) servers with three converged ccephontrol and cephosd nodes, expandable to additional cephosd nodes for additional storage. ⚠ • In a full-on (VIC based), or hyper-converged pod, computes can either have a combination of 1-Cisco VIC (1227) and (2x10GE 520/2x40GE 710XL Intel NIC) or 1-CiscoVIC (1227). The compute running pure Cisco VIC does not run SR-IOV. In 2.4, Cisco supports HP DL360 Gen9 as a third-party compute. • Cisco VIM does not support a combination of computes from different vendors.
ToR and FI support	1. For VTS-based installation, use the following Nexus versions: 7.0(3)I2(2a) 7.0(3)I6(2) andd 7.0(3)I7(5a) 2. For the mechanism driver other than VTS, use the following Nexus software version 7.0(3)I4(6) 7.0(3)I6(1). If you are using auto-ToR configuration and CONFIGURE_TORS is set to True, the NXOS version 7.0(3)I6(1) automation fails irrespective of the mechanism driver due to the defect CSCve16902. 3. UCS-FI-6296 4. Support of Cisco NCS 5500 (with recommended Cisco IOS XR version 6.1.33.02I or 6.5.1) with splitter cable. Day 0 configuration can support user-defined route-target and ethernet segment ID (ESI).
IPV6 support for management network	• Static IPv6 management assignment for servers. • Support of IPv6 for NTP, DNS, LDAP, external syslog server, and AD. • Support of IPv6 for the cloud API endpoint. • Support of CIMC over IPv6. • RestAPI over IPv6. • Support for IPv6 filters for administration source networks. • Support of UM over IPv6.
Centralization of management node	Value Engineering to reduce the overhead of one physical server per pod.*

Mechanism drivers	OVS/VLAN, VPP (19.08*)/VLAN (Fast Networking, Fast Data FD.io VPP/VLAN, based on the FD.io VPP fast virtual switch over intel NIC).
SDN controller integration	• VTS 2.6.2 with an optional feature of managed VTS • ACI (ships in the night, or ToR automation using APIC API) with Cisco VIC/Intel NIC on the UCS C-series M4 platform, and with Intel NIC on Quanta (D52BQ-2U 3UPI) servers.
Installation or update method	• Fully automated online or offline installation. • Support of offline installation via USB or file-based image.* • Support of Cisco VIM Software Hub to mitigate the problem associated with the logistics of USB distribution for air-gapped installation. • Support of USB 3.0 64GB for M5 and Quanta-based management node. Support of UCS 2.0 64GB for M4-based management node.
Scale	• Total of 128 nodes (compute and OSD) with Ceph OSD max at 20. ⚠ Ensure that you deploy a maximum of 60 nodes at a time. Also, after Day 0, you can add only one ceph node at a time. • Micropod: Supports a maximum of 16 standalone compute nodes. • Hyper-converged (HC): Total of 64 nodes including three controllers is available. Maximum number of nodes is 15 HC (compute and OSD) . ⚠ Ceph OSDs can be HDD or SSD based, but must be uniform across the pod. Computes can boot off 2x1.2TB HDD or 2x960 GB SSD). In the same pod, some computes have SSD, while others can have HDD. Contact Cisco VIM product management team for specific use cases and BOM details applicable to each type of pod.
Automated pod life cycle management	• Add or remove compute and Ceph nodes and replace the controller node. • Static IP management for storage network. • Reduction of tenant or provider VLAN through reconfiguration to a minimum of two. • Reconfiguration of passwords and selected optional services. • Automated software update.
Platform security	• Secure OS, RBAC, network isolation, TLS, source IP filtering (v4 and v6), Keystone v3, Bandit, CSDL-compliant, hardened OS, and SELinux. • Change CIMC password post-installation for maintenance and security. • Non-root login for administrators. • Read-only role is available for OpenStack users. • Enabling custom policy for VNF Manager. • Option to disable the management node reachability to the cloud API network. • Hosting of Horizon behind NAT or with a DNS alias. • Cinder volume encryption using Linux Unified Key Setup (LUKS). • Support of configurable login banner for SSH sessions. • Access to management node using LDAP. • Support for IPv6 filters for administration source networks. • Access of NFVIMON for non-root users. • Introduction of Vault to encrypt secrets with reconfigure option. • Enablement of Vault as an option on Day 2. • Extended permit_root_login to Unified Management node. • CIMC authentication using LDAP. • Support of RedHat identity, policy and audit (IPA) system. • Support of Horizon and Keystone login settings. • Support of LDAP on Unified Management node. • SSH and password vulnerabilities for management node.* • Kernel changes to address vulnerabilities.* • Support of FPGA 1.1 image for Qunata GC SKU (2RU1N)* • FQDN support for Cisco VIM management API.
Enhanced Platform Awareness (EPA)	• Supports NUMA, CPU pinning, huge pages, and SRIOV with Intel NIC. • Ability to allocate user-defined CPU (up to 6) cores to VPP. • Ability to bring in trusted_vf as a reconfigure option on a per server basis. • Ability to allocate user-defined CPU (up to 12) cores to Ceph for Micropod and hyper-converged nodes. • Ability to allocated user-defined CPU (upto 12) cores to controller for AIO nodes in Micropod and control/compute nodes in edge pod.

HA and reliability	• Redundancy at hardware and software level. • Automated backup and restore of the management node. • Relaxation of Security Enhanced Linux (SELinux) requirement for backup and restore of the management node.* • Optimization of automated backup and restore of the management node in a connected install.*
Unified Management (UM) support	Single pane of glass in a single or multi-instance (HA) mode. Supports multi-tenancy and manages multiple pods from one instance.
Cisco VIM monitor	Collects the metrics from the entire pod. Supports customizing alerts, sending SNMP traps, and exporting to external metric collectors.
Central logging	EFK integrated with external Syslog (over v4 or v6) for a log offload, with optional support of NFS with EFK snapshot.
External Syslog servers	Supports multiple external Syslog servers over IPv4 or IPv6. The minimum and maximum number of supported external Syslog servers are 1 and 3, respectively.
VM migration	• Cold migration and resizing. • Live migration with OVS as a mechanism driver.
Storage	• Block storage with Ceph, or NetApp. • Option to use Ceph for Glance and Solidfire for Cinder. • Option to have multi-backend (HDD and SSD based) Ceph in the same cluster to support various I/O requirements and latency. • Integration of Zadara as an alternate to Ceph.*
Monitoring	• Monitor the Cisco VIM pods centrally using the Highly Available Cisco VIM Monitor (HA CVIM-MON) over v4 and v6. • Monitor the Cisco VIM pods individually using the local Cisco VIM Monitor (CVIM-MON) over v4 and v6. • CVIM MON Lcoal LDAP support with Grafana, Prometheus,* and Alert Manager*. • Support of non Cisco VIM managed external servers running RHEL or CentOS. • Ceilometer for resource tracking and alarming capabilities across core OpenStack components is applicable only for fullon pod. • Third-party integration with Zenoss (called NFVIMON) • Traffic Monitoring with OVS for debugging.
Optional OpenStack features	• Enable trusted virtual function on a per-server basis. • DHCP reservation for virtual MAC addresses. • Enable VM_HUGE_PAGE_SIZE and VM_HUGE_PAGE percentage on a per-server basis. • Enable CPU and RAM allocation ratio on a per-server basis via add/remove compute or reconfigure*
Support of external authentication system	• LDAP with anonymous bind option. • Active Directory (AD).
Software update	Update of cloud software for bug fixes on the same release.
Software upgrade	• Upgrade of non-VTS cloud from release 3.2.1 or 3.2.2 to release 3.4.3. • Software upgrade of non-VTS cloud from Cisco VIM 2.4.y to Cisco VIM 3.4.3, where y=15, 16, 17, or 18.
CIMC upgrade capability	Central management tool to upgrade the CIMC bundle image of one or more servers.
VPP port mirroring	• Ability to trace or capture packets for debugging and other administrative purposes. • Automated update of BMC or BIOS and firmware of Quanta server.

VXLAN extension into the cloud	• Extended native external VXLAN network into VNFs in the cloud. • Support of Layer 3 adjacency for BGP. • Support of single VXLAN network or multi-VXLAN network (with head-end-replication option) terminating on the same compute node. • Support of re-binding of Neutron port to another port.* • Support of L3 fabric via VXLAN (as Tech-preview)* ⚠ Only two-VXLAN network is supported.
Technical support for CIMC	Collection of technical support for CIMC.
Enable TTY logging as an option	Enables TTY logging and forwards the log to an external syslog server and EFK stack running on the management node. Optionally, it forwards the log to the remote syslog if that option is available.
Remote installation of management node	Automated remote installation of management node over a Layer 3 network.
Unified Management authentication	Authentication support through local and LDAP.
CIMC authentication using LDAP	Authentication support through LDAP.
Automated enablement of Intel X710/XL710 NIC's PXE configuration on Cisco UCS-C series	Utility to update Intel X710/XL710 NIC's PXE configuration on Cisco UCS-C series.
Power management of computes	Option to selectively turn OFF or ON the power of computes to conserve energy.
Disk maintenance for pod nodes	Ability to replace faulty disks on the pod nodes without the need to add, remove, or replace node operation.
Branding of VM workload	Ability to check whether the VMs are running on Cisco VIM platform from VM.* ⚠ This feature is reverted in Cisco VIM 3.4.4.
Support of workload types	• Supports baremetal (ironic-based) and container (Cisco Container Platform (CCP)) based workloads. • Support of bonding on the Ironic network.
Cloud adaptation for low latency workload	• Enable real-time kernel to support edge pod. • Automated BIOS configuration. • Introduction of custom flavor. • Support of Intel N3000 card on selected servers to handle vRAN workloads. • Support of Cache Allocation Technology (CAT) to handle vRAN workloads. • Support of INTEL_SRIOV_VFS (SRIOV support for Intel NIC) and INTEL_FPGA_VFS (support for Intel N3000 FPGA card) at a per-server level.
Integrated test tools	• Open-source data plane performance benchmarking: VMTP (an open-source data plane VM to VM performance benchmarking tool) and NFVbench (NFVI data plane and a service chain performance benchmarking tool). • Extending VMTP to support v6 over the provider network. • NFVbench support for VXLAN. • Services Health Checks Integration: Cloudpulse and Cloudsanity.

⚠ * Indicates the features introduced in Cisco VIM 3.4.3.

⚠

- For supported BOM details, reach out to nfvi-plm@cisco.com or your account team.
- Configure LACP on the data plane ports of the Cisco Nexus 9000 ToR when Cisco VIM is running on Intel NIC for data plane with VPP as the mechanism driver. When Cisco NCS 5500 is ToR (with VPP), the LACP configuration on the data plane is done through Auto-ToR configuration feature of Cisco VIM.

Documentation

The following sections are updated for 3.4.3:

- Restoring Management Node (updated for technical accuracy and addressed VIMBUGS-3457)
- Quanta Firmware Upgrade (updated for VIMBUGS-3422)
- Upgrade/Update UM (updated for VIMBUGS-3436)
- Known Caveats (added CSCvt42065 and CSCvt79972)
- Container Support (addressed VIMBUGS-3483)
- Monitoring with CVIM-MON (added for VIMBUGS-3452)
- Branding VM Workloads (addressed VIMBUGS-3464)
- Management Node on UCS C-series (M4/M5), Supporting RMA for Auto-ToR, and Servers and Network Option (addressed VIMBUGS-3516)
- Cisco NFVI Overview and Upgrading Cisco VIM Using Network Installation (addressed VIMBUGS-3516)
- Servers and Network Option (updated for technical accuracy)
- Managing Hosts and Reconfiguration (updated for technical accuracy)
- Alert Rules and Alert Manager (addressed CSCvt92108)
- Upgrading Cisco VIM Using USB, Management Node on UCS C-series (M4/M5) and DHCP Reservations (updated for VIMBUGS-3516)
- UM with Internet Access (addressed Zendesk: 12462)
- Control and Data Plane Testing (addressed CSCvu13312)
- Managing Hosts, Managing Power and Reboot, Managing Hardware (addressed CSCvs23759)
- Restoring Management Node (updated for technical accuracy)
- Updating APIC Parameters (addressed CSCvu37052)
- Features of Cisco VIM (addressed VIMBUGS-3516)
- CVIM-MON and CVIM Monitor and Inventory Service Configuration (addressed VIMBUGS-4070)
- Unified Management and Day 2 Operations of UM (addressed VIMBUGS-4070)
- Upgrade/Update UM and Updating Nodes (addressed VIMBUGS-3987)
- Centralizing Management Node and Virtual GPU Support (addressed VIMBUGS-3516)
- OpenStack Configuration, Enabling NFVBench, and Managing VIM Administrators (updated for VIMBUGS-3516)
- Cisco VIM Software Hub, Ceph Storage, and Restoring Management Node (addressed VIMBUGS-3516)
- Reinstallation of CVIM-MON HA Pod (added for technical accuracy)
- Restoring Management Node and CVIM Monitor and Inventory Service Configuration (addressed VIMBUGS-3516)
- Network Topologies, Managing Power and Reboot, Pod Recovery, Upgrading Cisco VIM Using USB (addressed VIMBUGS-3516)
- Known Caveats (added CSCvt33521)
- Certificates (updated for VIMBUGS-3516)
- Management Node VMs Lifecycle (addressed VIMBUGS-4987)
- OpenStack Telemetry Service (updated for technical accuracy)
- Hardening Cisco VIM Deployment (addressed VIMBUGS-5187)
- Backing Up Management Node and Restoring Management Node (addressed VIMBUGS-3516)
- NetApp Integration, NetApp from http to https, and Storage Node Overview (addressed VIMBUGS-3516)
- CVIM Monitor and Inventory Service Configuration (updated for technical accuracy)

Known Caveats

The following list describes the known caveats in Cisco VIM 3.4.3:

- **CSCvt45271**

  Rollback of CVIM MON HA is not supported from Cisco VIM 3.4.3 to 3.4.2.

- **CSCvt45605**

  needs-restarting -r does not show that a reboot is required after updating the RT kernel to 7.6.

- **CSCvt42065**

After the restoration of Cisco VIM management node, centralized VM *setup_data.yaml* file might go out of sync.

- **CSCvt79972**

  cvim-mon: Custom alerting rule creation after reconfiguration is not working.

- **CSCvu48128**

LLDP agent on Intel NIC firmware is disabled for DPDK bound ports.

- **CSCvt33521**

  The reconfiguration fails as part of validation, after the renewal of TLS certificate.

Resolved Caveats/Enhancements

The following list describes the issues that are resolved in Cisco VIM 3.4.3:

- **CSCvt25901**

  UCS-Monitor: SSL Error when configuring remote syslog on UCS M4/5.

- **CSCvt33262**

  CVIM 2.4.x/3.2.x - compute/controller node hostname is not reflecting in Syslog message.
- **CSCvs86859**

  In Quanta pod, multicast_snooping must be disabled in controllers as well.
- **CSCvt19286**

  Kernel crash due to divide error: 0000 [#1] SMP.
- **CSCvr83707**

  Seeing two entries cinder-volume services in OpenStack. Ideally, it must always be 1.
- **CSCvs86855**

  Modify UCS firmware upgrade script to use nping.
- **CSCvs04055**

  Need an alternative method to copy the backup of management node.

Using the Cisco Bug Search Tool

You can use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Procedure

1. Go to the Cisco Bug Search Tool.
2. In the **Log In** screen, enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
4. To search for bugs in the current release:

    a. In the **Search For** field, enter **Cisco Network Function Virtualization Infrastructure** with release version and press **Enter**. (Leave the other fields empty.)
    b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

Cisco VIM 3.4.4 Release Notes

Cisco VIM 3.4.4 Release Notes

Release Date

First Published: April 10, 2020

Overview

Cisco VIM 3.4.4 is available as a bug fix release. Except for the list of resolved caveats/enhancements, all other aspects of Cisco VIM 3.4.3 are applicable to Cisco VIM 3.4.4. For more information, see *Cisco VIM 3.4.3 Documentation.*

Resolved Caveats/Enhancements

The following list describes the issues that are resolved in Cisco VIM 3.4.4:

- **CSCvs72544**

  Cisco VIM update from 3.4.1 to 3.4.2 fails due to the failure in the recovery of MariaDB.

- **CSCvt42065**

  After Cisco VIM management node restoration, centralized VM *setup_data.yaml* file may go out of sync.
- **CSCvt59504**

  Skip upgrade fails on pending cinder migrations from 2.4.x to 3.4.3.
- **CSCvt59664**

  Day 0 configuration is not applied on CSR1000v using Openstack.
- **CSCvt61914**

  Handle Zadara validation for V4 end point.
- **CSCvt66344**

  Unified Management update from Cisco VIM 3.4.2 to Cisco VIM 3.4.3 with UM LDAP fails.
- **CSCvt67288**

  Upgrade fails with mariadb InnoDB corruption.
- **CSCvt69595**

  Fix bug in VPP for transmitting IPv6 packets.
- **CSCvt72296**

  NFVbench --force-cleanup is deleting more ports than required.

> ⚠ CIMC 4.0(4m) and CIMC 4.1(2a) are supported and tested with Intel NIC BOM. Other versions of CIMC may work, but you must test Cisco VIM deployment with those versions, before rolling it into production.

Using the Cisco Bug Search Tool

You can use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Procedure

1. Go to the Cisco Bug Search Tool.
2. In the **Log In** screen, enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
4. To search for bugs in the current release:

    a. In the **Search For** field, enter **Cisco Network Function Virtualization Infrastructure** with release version and press **Enter**. (Leave the other fields empty.)

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

Cisco VIM 3.4.5 Release Notes

Cisco VIM 3.4.5 Release Notes

Release Date

First Published: July 10, 2020

Updated:

- Sep 21, 2020: Updated the *Known Caveats*.
- Dec 03, 2020: Updated the *Known Caveats*.

Overview

Cisco VIM 3.4.5 is available as a bug fix release. Except for the list of resolved caveats/enhancements, all other aspects of Cisco VIM 3.4.3 are applicable to Cisco VIM 3.4.5. For more information, see *Cisco VIM 3.4.3 Documentation.*

Known Caveats

The following list describes the known caveats in Cisco VIM 3.4.5:

- **CSCvv25734**

  Handle admin user across many projects for*rabbit_api.py.*
- **CSCvv16612**

  Unpinned VM has significant performance issues because of ISOLCPU being a default parameter.
- **CSCvv13931**

  CVIM-MON: RabbitMQ alerting rule may produce false positive with duplicate metrics.
- **CSCvu62402**

  Container restart on host causes latency spikes in VM.
- **CSCvv33093**

  Tech-support: Remove *rt* commands, *sosreport, lstopo* and *processor* plug-in.
- **CSCvv62914**

  Support CPU pinning for central VM management.
- **CSCvv60253**

  Handle variants in Quanta server output.
- **CSCvv71343**

  Tuned profile not applied when upgraded from Cisco VIM 2.4.x.
- **CSCvv42716**

  HugePage configuration is missing when upgraded from Cisco VIM 2.4.x.
- **CSCvw65892**

  IPA host entry is missing i*n /etc/hosts* after power management operations.

Resolved Caveats

The following list describes the issues that are resolved in Cisco VIM 3.4.5:

- **CSCvs39206**

  ciscovim reconfigure takes very long to complete.
- **CSCvs47492**

Handles apic login failure appropriately.

- **CSCvt79972**

  CVIM-MON: Custom alerting rules and alert manager configuration cannot be applied through *ciscovim* reconfigure.
- **CSCvt80637**

  VPP exits upon loss of control plane connectivity.
- **CSCvt90615**

  Support NR_RESERVED_HOST_PCORES as an option to HC nodes.
- **CSCvt96505**

  vpp-agent cleaning up process is incomplete with stale port entries in fib.
- **CSCvu04043**

  Handle APIC granular to pre-provision vlan checks.
- **CSCvu05165**

  ciscovim client connection fails with trusted CA certificate.
- **CSCvu08419**

  Allow network_id change with different projects honoring RBAC.
- **CSCvu23174**

  Support LDAP over IPv6 for VIM admin LDAP authentication.
- **CSCvu23968**

  Remove unique check of *engine_id* for SNMPv3.
- **CSCvy22062**

  SDS : Observed fatal error while performing reconfiguration.
- **CSCvu48128**

  LLDP agent on intel NIC firmware is disabled for DPDK bound ports.
- **CSCvu88613**

  Enabling Horizon syslogs in Cisco VIM.
- **CSCvt75789**

  Avoid using *lacp* key 0 for compatibility.

> ⚠ CIMC 4.0(4m) and CIMC 4.1(2a) are supported and tested with Intel NIC BOM. Other versions of CIMC may work, but you must test Cisco VIM deployment with those versions, before rolling it into production.

Enhancements

- Kernel upgrade of RedHat 7.6 EUS Kernel and OSP13 to that of 01/21/2020
    - RHEL 7.6 Real Time Version: 3.10.0-957.46.1.rt56.964.el7 (with point fix of event poll)
    - RHEL 7.6 Version: 3.10.0-957.48.1.el7.x86_64
- Support forwarding of security related logs to Syslog server
- Auto register controllers for Zadara NFS
- New CLI/options for Unified Management node installation and Day 2 management operations such as update, rollback, and so on

Using the Cisco Bug Search Tool

You can use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Procedure

1. Go to the Cisco Bug Search Tool.
2. In the **Log In** screen, enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
4. To search for bugs in the current release:
    a. In the **Search For** field, enter **Cisco Network Function Virtualization Infrastructure** with release version and press **Enter**. (Leave the other fields empty.)
    b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

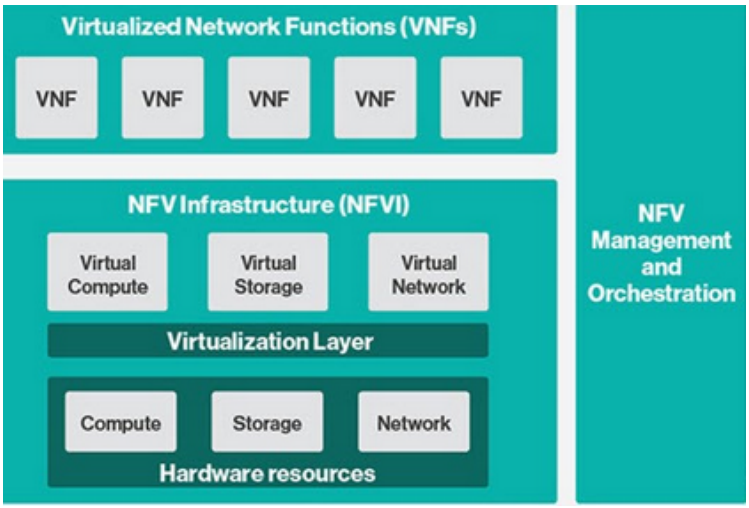
Cisco NFVI Architecture

Cisco NFVI Architecture

Cisco NFVI Overview

Cisco Network Function Virtualization Infrastructure Overview

Cisco Network Function Virtualization Infrastructure (NFVI) provides the virtual layer and hardware environment in which virtual network functions (VNFs) can operate. VNFs provide well-defined network functions such as routing, intrusion detection, domain name service (DNS), caching, network address translation (NAT), and other network functions. While these network functions require tight integration between network software and hardware, the use of VNF enables to decouple the software from the underlying hardware.
The following figure shows the high-level architecture of Cisco NFVI.



Cisco NFVI includes a virtual infrastructure layer (Cisco VIM) that embeds the Red Hat OpenStack Platform (OSP 13). Cisco VIM includes the Queens release of OpenStack, which is an open source cloud operating system that controls large pools of compute, storage, and networking resources. Cisco VIM manages the OpenStack compute, network, and storage services, and all NFVI management and control functions. Cisco VIM is an embedded solution and must be treated as one or else it violates the support agreement of the product. Activities such as changing system files and directories, installing/upgrading rpm, and/or enabling repositories outside Cisco VIM, are examples of such violations. For more details, contact Cisco Support.

Key Cisco NFVI roles include:

- Control (including Networking)
- Compute
- Storage
- Management (including logging, and monitoring)

Hardware that is used to create the Cisco NFVI pods includes a specific combination of the following based on pre-defined BOMs. For more details, contact Cisco VIM Product Management.

- Cisco UCS® C240 M4/M5: Performs management and storage functions and services. Includes dedicated Ceph (UCS 240-M4 or UCS 240-M5) distributed object store and file system. (Only Red Hat Ceph is supported).
- Cisco UCS C220/240 M4/M5: Performs control and compute services.
- HP DL360 Gen9: It is a third-party compute where the control plane is Cisco UCS servers.
- Cisco UCS 220/240 M4/M5 (SFF): In a Micropod environment, expandable to a maximum of 16 computes.
- Cisco UCS B200 M4 blades: It can be used instead of the UCS C220 for compute and control services. The B200 blades and C240 Ceph server are connected with redundant Cisco Fabric Interconnects managed by UCS Manager.
- A combination of M5 series servers are supported in M5-based Micropod and VIC/NIC (pure 40G) based hyper-converged and micropod offering.
- Quanta servers are an alternative to Cisco UCS servers: Use of specific Quanta servers for the installation of the cloud both at the core and edge. An automated install of the Central Ceph cluster to the edge pods is supported for Glance image services.

The UCS C240 and C220 servers are of type M4 or M5 Small Form Factor (SFF) models where the nodes can boot off a pair of HDDs or SSD as specified in BOM. Each UCS C240, UCS C220, and UCS B200 have two 10 GE Cisco UCS Virtual Interface Cards.

The B-Series pod consists of Cisco UCS B200 M4 blades for the Cisco NFVI compute and controller nodes with dedicated Ceph on a UCS C240 M4. The blades and Ceph server are connected via redundant fabric interconnects (FIs) managed by Cisco UCS Manager. The Cisco VIM installer performs bare metal installation and deploys OpenStack services using Docker™ containers to allow for OpenStack services and pod management software updates. The following table shows the functions, hardware, and services managed by Cisco NFVI nodes.

Function	Number	Hardware	Services

Management	1	• UCS C240 M4 SFF with 8, 16, or 24 1.2 TB HDDs (24 is recommended) • UCS C240 M5 SFF with 8, 16, or 24 1.2 TB HDDs (24 is recommended) • UCS C220 M5 SFF with 8x1.2 TB HDDs • Quanta Server (D52BE-2U) with 2x1.2TB HDD • Quanta Server (D52BQ-2U 3UPI) with 2x.3.8TB HDD	• Cisco VIM Installer • Cobbler server • Docker Registry • ELK server • CVIM MON components: Prometheus and TSDB
Control	3	• UCS C220/C240 M4/M5 with 2x 1.2 TB HDDs or 2x960G SSDs (in a Micropod or Full Pod environment) • UCS B200 with two 1.2 TB HDDs • Quanta Server (D52BE-2U) with 2x960 G SSD • Quanta Server (D52BQ-2U 3UPI) with 2x960 G SSD for edge pod	• Maria Database/Galera • RabbitMQ • HA Proxy/Keepalive • Identity Service • Image Service • Compute management • Network service • Storage service • Horizon dashboard • Fluentd
Compute	2+	• UCS C220/C240 M4/M5 with two1.2 TB HDDs, or 2x9.6 GB SSDs (in a Micropod or Full Pod environment) • UCS B200 with two 1.2 TB HDDs • HP DL360 Gen9 • Quanta Server (D52BE-2U/ D52BQ-2U 3UPI) with 2x960 G SSD	• Virtual Networking Service • Compute service • Fluentd
Storage	3 or more	SSD and HDD drives must be in a 1:4 ratio per storage node minimum. Storage node configuration options: Fullon environment: • UCS C240 M4/M5 with two internal SSDs, 1-4 external SSD, 4-20x-1.2 TB HDDs • SSD-based Ceph: UCS C240 M4/M5 with 2 internal SSDs, minimum of 4 external SSDs, expandable to 24 SSDs • Quanta Server (D52BE-2U) HDD Based: 4 SSD 960GB for Journal + 16 SAS HDD (16x2.4 TB) for OSD + 2 (2x2.4 TB SAS 10krpm HDD) for OS • Quanta Server (D52BE-2U) SSD Based: 20 SSD (3.8 TB) OSD + 2 OSBoot (2x3.8TB SSD) Micropod/UMHC/NGENAHC environment: • UCS C240 M4/M5 with two 1.2TB HDD for OS boot, one/2 SSDs and 5/10x1.2 TB HDDs • UCS C240 M4/M5 with 2x960GB SSD for OS boot and 4 or 8 x960 GB SSDs	• Storage service
Top of Rack (ToR)	2	Recommended Cisco Nexus 9000 series switch software versions: • 7.0(3)I4(6) • 7.0(3)I6(1) • 9.3(2) Cisco NCS 5500 as ToRs or Cisco Nexus 9000 switches running ACI 3.0 (when ACI is used)	ToR services • Cisco NCS 5500 provides ToR service with VIM running on C-series with Intel NIC and VPP as the mechanism driver for deployment.

- Internal SSD is the boot device for the storage node
- You can use any ToR that supports virtual port channel. Cisco recommends that you use Cisco Nexus 9000 SKUs as ToR, which is released as part of Cisco VIM. When Cisco NCS 5500 acts as a ToR, auto-ToR config is mandatory.
- You must use the automated ToR configuration feature for Cisco NCS 5500.

Software applications that manage Cisco NFVI hosts and services include:

- Red Hat Enterprise Linux 7.6 with OpenStack Platform 13.0: Provides the core operating system with OpenStack capability. RHEL 7.6 and OPS 13.0 are installed on all target Cisco NFVI nodes.
- Cisco Virtual Infrastructure Manager (VIM): An OpenStack orchestration system that helps to deploy and manage an OpenStack cloud offering from bare metal installation to OpenStack services, taking into account hardware and software redundancy, security and monitoring. Cisco VIM includes the OpenStack Queens release with more features and usability enhancements that are tested for functionality, scale, and performance.
- Cisco Unified Management: Deploys, provisions, and manages Cisco VIM on Cisco UCS servers.
- Cisco UCS Manager: Used to perform certain management functions when UCS B200 blades are installed. Supported UCS Manager firmware versions are 2.2(5a) and above.
- Cisco Integrated Management Controller (IMC): Cisco IMC 2.0(13i) or later is supported.

For the Cisco IMC lineup, the recommended version is as follows:

UCS-M4 servers	We recommended that you: • Use Cisco IMC 2.0(13n) or later. • Switch to 3.0(3a) or later for pure intel NIC based pods.

For the Cisco IMC 3.x and 4.y lineup, the recommended version is as follows:

UCS-M4 servers	• Cisco IMC versions are 3.0(3a) or later, except for 3.0(4a). Cisco recommends Cisco IMC 3.0(4d). • Expanded support of CIMC 4.0(1a), 4.0(1b), and 4.0(1c). • You can move to 4.0(2f) only if your servers are based on Cisco VIC. • Cisco recommends you to use CIMC 4.0(2L).
UCS-M5 servers	• Cisco recommends you to use CIMC 3.1(2b) or higher. • Do not use 3.1(3c) to 3.1(3h), 3.0(4a), 4.0(2c), or 4.0(2d). • Cisco recommends you to use CIMC 4.0(4i). • For Cascade Lake support, you need a bundle version of a minimum of CIMC 4.0(4d). • For GPU support, you must ensure that the server is running with a minimum of CIMC 4.0(2f).

Enables embedded server management for Cisco UCS C-Series rack servers. Supports Cisco IMC firmware versions of 2.0(13i) or greater for the fresh install of Cisco VIM. Because of recent security fixes, we recommend you to upgrade Cisco IMC to 2.0(13n) or higher. Similarly, Cisco IMC version of lineup is supported. For this, you must install Cisco IMC 3.0 (3a) or above.

The Quanta servers also need to run with a minimum version of BMC and BIOS version, which is listed below:

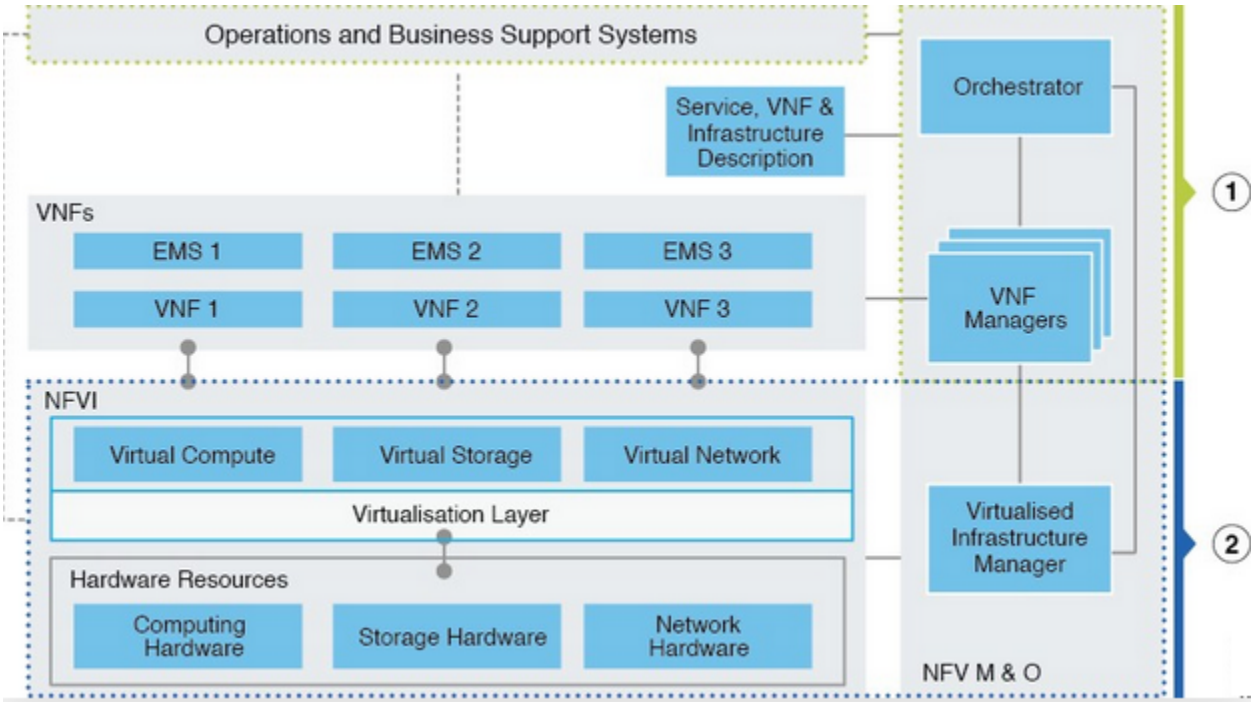
SKU Type	BMC Version	BIOS Version
D52BQ-2U 3UPI (CDC SKU)	4.68.22	3A11.BT17
D52BE-2U (GC SKU)	4.68.22	3A11.BT17

- Cisco Virtual Topology System (VTS)—It is an open, overlay management and provisioning system for data center networks. VTS automates DC overlay fabric provisioning for physical and virtual workloads. This is an optional service that is available through Cisco VIM.
- Cisco Virtual Topology Forwarder (VTF)—Included with VTS. VTF leverages Vector Packet Processing (VPP) to provide high-performance Layer 2 and Layer 3 VXLAN packet forwarding.

Two Cisco VNF orchestration and management applications that are used with Cisco NFVI include:

- Cisco Network Services Orchestrator, enabled by Tail-f—Provides end-to-end orchestration spanning multiple network domains to address NFV management and orchestration (MANO) and software-defined networking (SDN). For information about Cisco NSO, see Network Services Orchestrator Solutions.
- Cisco Elastic Services Controller—Provides a single point of control to manage all aspects of the NFV lifecycle for VNFs. Cisco ESC allows you to automatically instantiate, monitor, and elastically scale VNFs end-to-end. For information about Cisco ESC, see Cisco Elastic Services Controller Data Sheet.

The following figure shows the NFVI architecture with Cisco NSO and Cisco ESC.



At a high level, the NFVI architecture includes a VNF Manager and NFV Infrastructure.

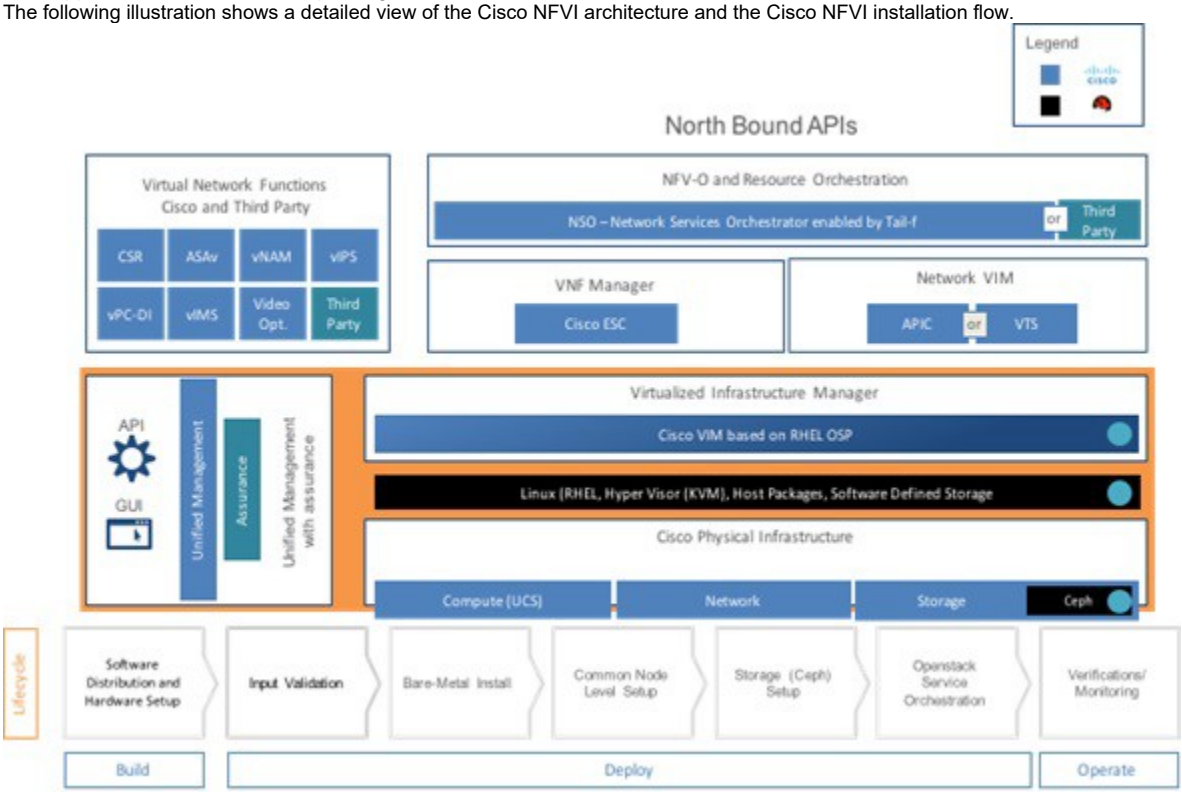
1	• Cisco Network Services Orchestrator • Cisco Elastic Services Controller
2	Cisco NFVI: • Cisco VIM + • Cisco UCS/Quanta/3rd Party Compute and Cisco Nexus Hardware + • Logging and Monitoring Software + • Cisco Virtual Topology Services (optional) + • Accelerated Switching with VPP (optional) • Cisco Unified Management (optional) • Pod Monitoring (optional)

For cloud networking, Cisco NFVI supports Open vSwitch over VLAN as the cloud network solution for both UCS B-series and UCS C-Series pods. Both B-Series and C-Series deployments support provider networks over VLAN.

In addition, with a C-series pod, you can choose:

- To run with augmented performance mechanism by replacing OVS/LB with VPP/VLAN (for Intel NIC).
- To have a cloud that is integrated with VTC which is an SDN controller option.

The Cisco NFVI uses OpenStack services running inside containers with HAProxy load balancing and providing high availability to API and management network messaging. Transport Layer Security (TLS) protects the API network from external users to the HAProxy. Cisco VIM installation also includes service assurance, OpenStack CloudPulse, built-in control, and data plane validation. Day two pod management allows you to add and remove both compute and Ceph nodes, and replace the controller nodes. The Cisco VIM installation embeds all necessary RHEL licenses as long as you use the Cisco VIM supported BOM and the corresponding release artifacts.
The following illustration shows a detailed view of the Cisco NFVI architecture and the Cisco NFVI installation flow.



Cisco VIM Overview

Cisco Virtualized Infrastructure Manager Overview

Cisco Virtualized Infrastructure Manager (VIM) is a fully automated cloud lifecycle management system. Cisco VIM helps to bring up a fully functional cloud in hours, with integrated end-to-end control and data plane verification in place. Cisco VIM offers fully automated Day 1 to Day n cloud lifecycle management. These include capabilities such as pod scaling (expansion), software update, upgrade, or reconfiguration parameters, consolidated logging with rotation and export, software update, and upgrade. These have been implemented in line with the operational and security best practices of the service providers and enterprises.
The following figure provides the high-level overview of all Day 0 and Day n items of Cisco VIM.

Networking Overview

Networking Overview

Introduction

Cisco VIM supports installation on two different types of pods. The blade B-series and rack C-series based offerings support NICs that are from Cisco (called as Cisco VIC). You can choose the C-series pod to run in a pure Intel NIC environment, and thereby obtaining SRIOV support on the C-series pod. This section calls out the differences in networking between the Intel NIC and Cisco VIC installations.

To achieve network level security and isolation of tenant traffic, Cisco VIM segments the various OpenStack networks. The Cisco NFVI network includes six different segments in the physical infrastructure (underlay). These segments are presented as VLANs on the Top-of-Rack (ToR) Nexus switches (except for the provider network) and as vNIC VLANs on Cisco UCS servers. You must allocate subnets and IP addresses to each segment. Cisco NFVI network segments include API, external, management and provisioning, storage, tenant, and provider.

API Segment

The API segment needs one VLAN and two IPv4 addresses (four if you are installing Cisco VTS) in an externally accessible subnet different from the subnets assigned to other Cisco NFVI segments. These IP addresses are used for:

- OpenStack API endpoints. These are configured within the control node HAProxy load balancer.
- Management node external connectivity.
- Cisco Virtual Topology Services (VTS) if available in your Cisco NFVI package.
- Virtual Topology Controller (VTC). It is optional for VTS.

External Segment

The external segment needs one VLAN to configure the OpenStack external network. You can provide the VLAN during installation in the Cisco NFVI setup_data.yaml file, but you must configure the actual subnet using the OpenStack API after the installation. Use the external network to assign OpenStack floating IP addresses to VMs running on Cisco NFVI.

Management and Provisioning Segment

The management and provisioning segment needs one VLAN and one subnet with an address pool large enough to accommodate all the current and future servers planned for the pod for initial provisioning (PXE boot Linux) and, thereafter, for all OpenStack internal communication. This VLAN and subnet can be local to Cisco NFVI for C-Series deployments. For B-Series pods, the UCS Manager IP and management network must be routable. You must statically configure Management IP addresses of Nexus switches and Cisco UCS server Cisco IMC IP addresses, and not through DHCP. They must be through the API segment. The management/provisioning subnet can be either internal to Cisco NFVI (that is, in a lab, it can be a non-routable subnet limited to Cisco NFVI only for C-Series pods), or it can be an externally accessible and routable subnet. All Cisco NFVI nodes (including the Cisco VTC node) need an IP address from this subnet.

Storage Segment

Cisco VIM has a dedicated storage network used for Ceph monitoring between controllers, data replication between storage nodes, and data transfer between compute and storage nodes. The storage segment needs one VLAN and /29 or larger subnet internal to Cisco NFVI to carry all Ceph replication traffic. All the participating nodes in the pod will have IP addresses on this subnet.

Tenant Segment

The tenant segment needs one VLAN and a subnet large enough to manage pod tenant capacity internal to Cisco NFVI to carry all tenant virtual network traffic. Only Cisco NFVI control and compute nodes have IP addresses on this subnet. The VLAN/subnet can be local to Cisco NFVI.

Provider Segment

Provider networks are optional for Cisco NFVI operations but are often used for real VNF traffic. You can allocate one or more VLANs for provider networks after installation is completed from OpenStack.
Cisco NFVI renames interfaces based on the network type it serves. The segment Virtual IP (VIP) name is the first letter of the segment name. Combined segments use the first character from each segment for the VIP, with the exception of provisioning whose interface VIP name is "mx" instead of "mp" to avoid ambiguity with the provider network. The following table shows Cisco NFVI network segments, usage, and network and VIP names.

Network	Usage	Network Name	VIP Name
Management /Provisioning	• OpenStack control plane traffic. • Application package downloads. • Server management; management node connects to servers on this network. • Host default route. • PXE booting servers during bare metal installations.	Management and provisioning	mx
API	• Clients connect to API network to interface with OpenStack APIs. • OpenStack Horizon dashboard. • Default gateway for HAProxy container. • Integration with endpoints served by SwiftStack cluster for native object storage, cinder backup service or Identity service with LDAP or AD.	api	a
Tenant	VM to VM traffic. For example, VXLAN traffic.	tenant	t
External	Access to VMs using floating IP addresses.	external	e
Storage	Transit network for storage back-end. Storage traffic between VMs and Ceph nodes.	storage	s
Provider Network	Direct access to existing network infrastructure.	provider	p
ACIINFRA	Internal ACI Network for Policy management (only allowed when deployed with ACI)	aciinfra	o
Installer API	• Administrator uses the installer API network to ssh to the management node. • Administrator connects to installer API to interface with secured services. For example, Kibana on the management node.	VIM installer API	br_api

For each C-series pod node, two vNICs are created using different ports and bonded for redundancy for each network. Each network is defined in **setup_data.yaml** using the naming conventions listed in the preceding table. The VIP Name column provides the bonded interface name (for example, mx or a) while each vNIC name has a 0 or 1 appended to the bonded interface name (for example, mx0, mx1, a0, a1).

The Cisco NFVI installer creates the required vNICs, host interfaces, bonds, and bridges with mappings created between all elements. The number and type of created vNICs, interfaces, bonds, and bridges depend on the Cisco NFVI role assigned to the UCS server. For example, the controller node has more interfaces than the compute or storage nodes. The following table shows the networks that are associated with each Cisco NFVI server role.

	Management Node	Controller Node	Compute Node	Storage Node
Management/Provisioning	+	+	+	+
ACIINFRA*		+	+	
API		+		
Tenant		+	+	
Storage		+	+	+
Provider		+**	+	
External		+		

⚠ *ACIINFRA is only applicable when using ACI as a mechanism driver.

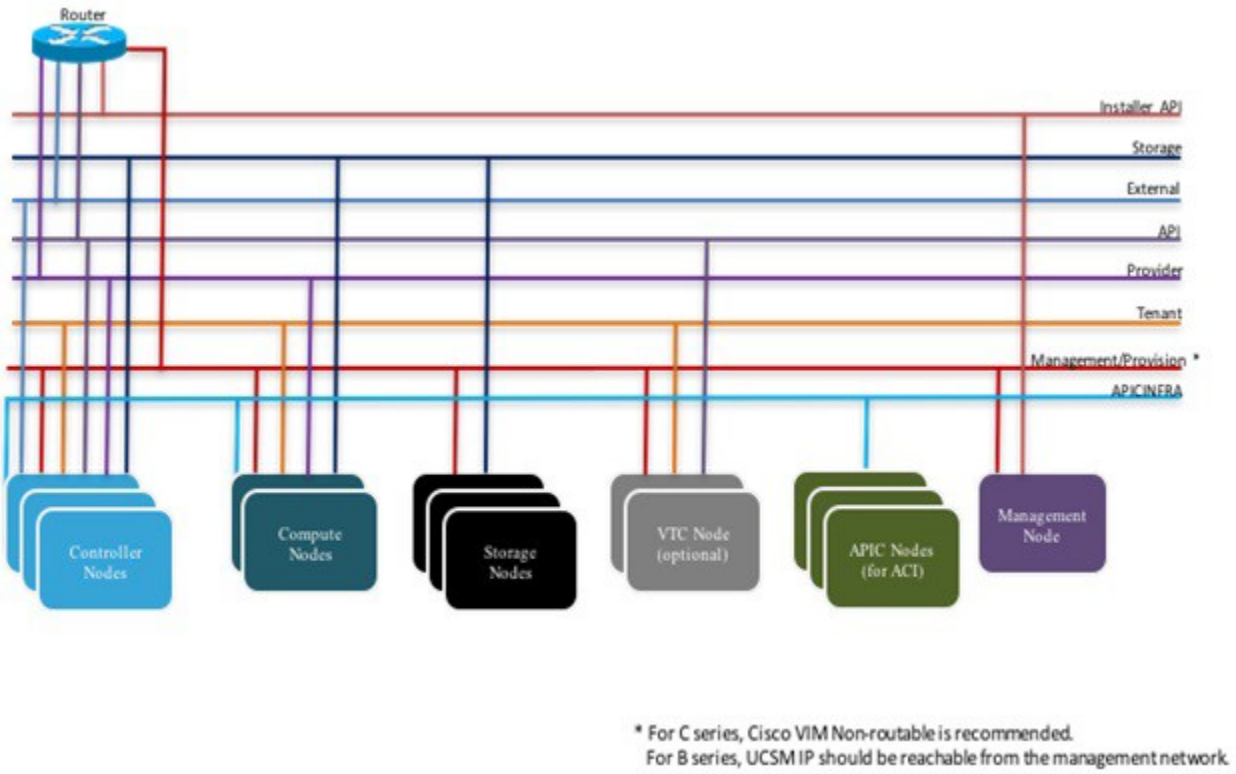
** Provider network is extended to controller nodes when VMs are on provider network with virtio.

The network arrangement on third-party HP compute is slightly different from that of Cisco compute running with Intel NIC, because the HP computes have 2 less NIC ports than that are available in the Cisco Intel NIC BOM.
Following table lists the differences in the network arrangement between the Cisco compute and third-party HP compute.

Network Interface	Cisco UCS Ce220 /Ce240M4/M5 Compute	HPE ProLiant DL360 Gen9 and Quanta Compute

mx	Management control plane network	N/A
samxpet		Control and data plane network for everything other than SRIOV: 1. Management network on "br_mgmt" bridge interface with "samxpet" main interface as one of the member interface (native VLAN configuration required on the top-of-rack switches) 2. Storage network on the sub-interface "samxpet.<storage VLAN>" 3. Tenant and provider networks on veth interface "pet/pet-out" as one of the member interface with "br_mgmt" bridge interface
p	Provider data plane network	
sriov[0-3]	Provider data plane SRIOV networks	Provider data plane SRIOV networks
s	Storage control and data plane network	N/A
t	Tenant data plane network	N/A

In the initial Cisco NFVI deployment, two bridges are created on the controller nodes, and interfaces and bonds are attached to these bridges. The br_api bridge connects the API (a) interface to the HAProxy. The HAProxy and Keepalive container has VIPs running for each OpenStack API endpoint. The br_mgmt bridge connects the Management and Provisioning (mx) interface to the HAProxy container as well.
The following diagram shows the connectivity between Cisco NFVI nodes and networks.



Supported Layer 2 networking protocols include:

- VLAN over Open vswitch(SRIOV with Intel 710NIC).
- VLAN over VPP/VLAN for C-series Only.
- Single Root Input/Output Virtualization (SRIOV) for UCS B-Series pods. SRIOV allows a single physical PCI Express to be shared on a different virtual environment. The SRIOV offers different virtual functions to different virtual components, for example, network adapters, on a physical server.

The footprint of the cloud offering supported by Cisco VIM has continued to evolve over multiple releases to support customer needs that can vary across multiple dimensions such as cloud capacity, power, physical space, and affordability. The following table shows the available Cisco NFVI hardware and data path deployment combinations.

POD Type	NIC Type	Hardware Vendor	Mechanism Driver	TOR Type

fullon	Cisco VIC	UCS C series M4 UCS C series M5	OVS/VLAN	N9K
fullon	Cisco VIC	UCS B Series	OVS/VLAN with SRIOV	N9K
fullon	Cisco VIC	UCS C series M4 UCS C series M5 with 1457 computes	VTF with VTC (VXLAN)	N9K
fullon	Intel NIC	UCS C series M4 UCS C series M5	OVS/VLAN with SRIOV	N9K
fullon	Intel NIC	Quanta D52BQ-2U 3UPI	OVS/VLAN with SRIOV	N9K
fullon	Intel NIC	UCS C series M4 UCS C series M5	VPP/VLAN with SRIOV	N9K NCS-5500
fullon	VIC for Control & Intel NIC for Data Plane	UCS C series M4 with HP as third-party Compute	OVS/VLAN with SRIOV	N9K
fullon	Cisco VIC with Intel NIC	UCS C series M4/M5 computes UCS C series M5	OVS/VLAN (VIC) with SRIOV (Intel NIC)	N9K
micro	Cisco VIC	UCS C series M4 UCS C series M5	OVS/VLAN	N9K
micro	Intel NIC	UCS C series M4 UCS C series M5	OVS/VLAN	N9K
micro	Intel NIC	UCS C series M4 UCS C series M5	VPP/VLAN	N9K NCS-5500
UMHC	Cisco VIC with Intel NIC	UCS C series M4 UCS C series M5	OVS/VLAN (VIC) with SRIOV (Intel NIC)	N9K
NGENAHC	VIC for Control & Intel NIC for Data Plane	UCS C series M4	VPP/VLAN	N9K
edge	Intel NIC	Quanta D52BE-2U	OVS/VLAN with SRIOV	N9K
ceph	Intel NIC	Quanta D52BQ-2U 3UPI	N/A	N9

- fullon indicates the dedicated control, compute and ceph nodes
- micro indicates converged control, compute and ceph nodes with expandable computes.
- Hyperconverged (HC) indicates dedicated control and compute nodes, but all ceph nodes are compute nodes.
- edge indicates converged control and compute nodes with expandable computes. It communicates with Central ceph cluster for Glance Image service. Persistent storage is not supported.
- ceph indicates converged cephcontrol & cephosd nodes, with an option to add cephosd nodes for glance image services.

- The SRIOV support is applicable only for Intel NIC-based pods.
- VTF with VTC is only supported on C-series Cisco VIC.

Pod with Intel NICs

For pods with Intel NICs (X710), the networking is slightly different. You need to have atleast two NICs (4x10G) on a single server to support NIC level redundancy. Each NIC is connected to each ToR (connections explained later in this section). Since vNICs are not supported in the Intel card, bond the physical interfaces at the host and then create sub-interfaces based on the segment VLAN. Lets call the two NIC cards as NIC_1 and NIC_2 and call their four ports as A, B, C, D. Unlike Cisco VIC based pod, the traffic here is classified as follows:

1. Control plane.
2. Data plane (external, tenant and non-SRIOV provider network).
3. SRIOV (optional for provider network). If SRIOV is used, the data plane network only carries external and tenant network traffic.

Control Plane

The control plane is responsible for carrying all the control and management traffic of the cloud. The traffic that flows through control plane are:

1. Management/Provision.
2. Storage.
3. API.

The control plane interface is created by bonding the NIC_1 A port with NIC_2 A port. The bonded interface name is called as samx, indicating that it is carrying Storage, API, Management/Provision traffic (naming convention is similar to Cisco VIC pod). The underlying interfaces (physical interfaces) of the bonded interface are renamed as samx0 and samx1. samx0 belongs to NIC_1 and samx1 belongs to NIC_2. Sub interfaces are then carved out of this samx interface based on the Storage, API VLANs. The management/provision traffic will be untagged/native VLAN in order to support pxe booting.

Data Plane

The data plane is responsible for carrying all the VM data traffic. The traffic that flows through the data plane are

- Tenant
- Provider
- External

The data plane is created by bonding the NIC_1 B port with NIC_2 B port. The bonded interface name here would be pet, indicating that it is carrying Provider, External and Tenant traffic. The underlying interfaces of this bonded interface would be visible as pet0 and pet1. pet0 belongs to the NIC_1 and pet1 belongs to NIC_2.
In case of OVS/VLAN, the "pet" interface is used as it is (trunked to carry all the data VLANs) to the Openstack cloud, as all the tagging and untagging happens at the Openstack level. In case of Linux Bridge/VXLAN, there will be sub-interface for tenant VLAN to act as the VXLAN tunnel endpoint.

SRIOV

In case of Intel NIC pod, the third (and optionally the fourth) port from each NIC can be used for SRIOV traffic. This is optional and is set or unset through a setup_data.yaml parameter. Unlike the control and data plane interfaces, these interfaces are not bonded and hence there is no redundancy. Each SRIOV port can have maximum of 32 virtual functions and the number of virtual function to be created are configurable through the setup_data.yaml. The interface names of the SRIOV will show up as sriov0 and sriov1 on each host, indicating that sriov0 belongs to NIC_1 C port and sriov1 belongs to NIC_2 C port.
The following table summarizes the interface name and type of traffic for each network plane:

Network	Usage	Type of traffic	Interface name
Control Plane	To carry control/management traffic	Storage, API, Management/Provision	samx
Data Plane	To carry data traffic	Provider, External, Tenant	pet
SRIOV	To carry SRIOV traffic	SRIOV	sriov0, sriov1

The following table shows the interfaces that are present on each type of server (role based).

	Management Node	Controller Node	Compute Node	Storage Node
Installer API	+			
Control plane	+	+	+	+
Data plane		+	+	
SRIOV			+	

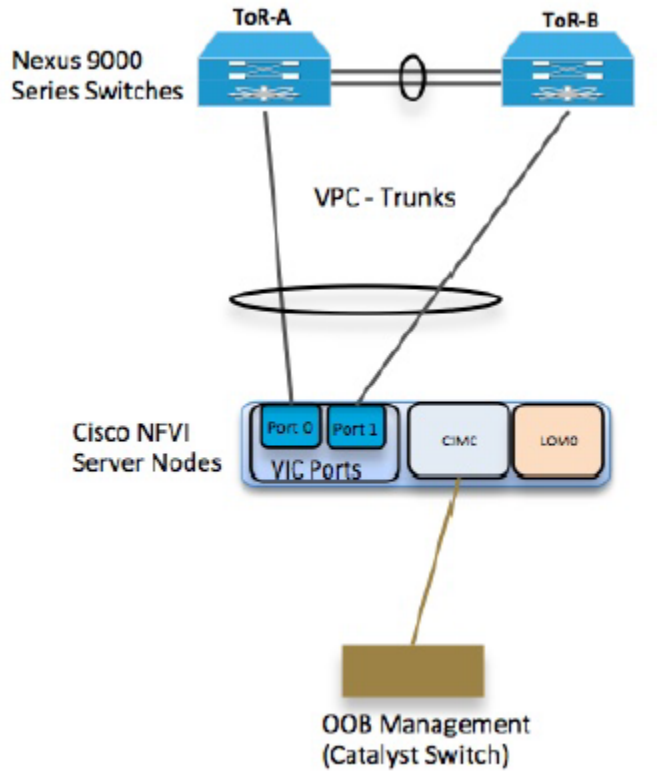
On Intel pod, all kinds of OpenStack networks are created using *physnet1* as the physnet name.

UCS C-Series Network Topologies

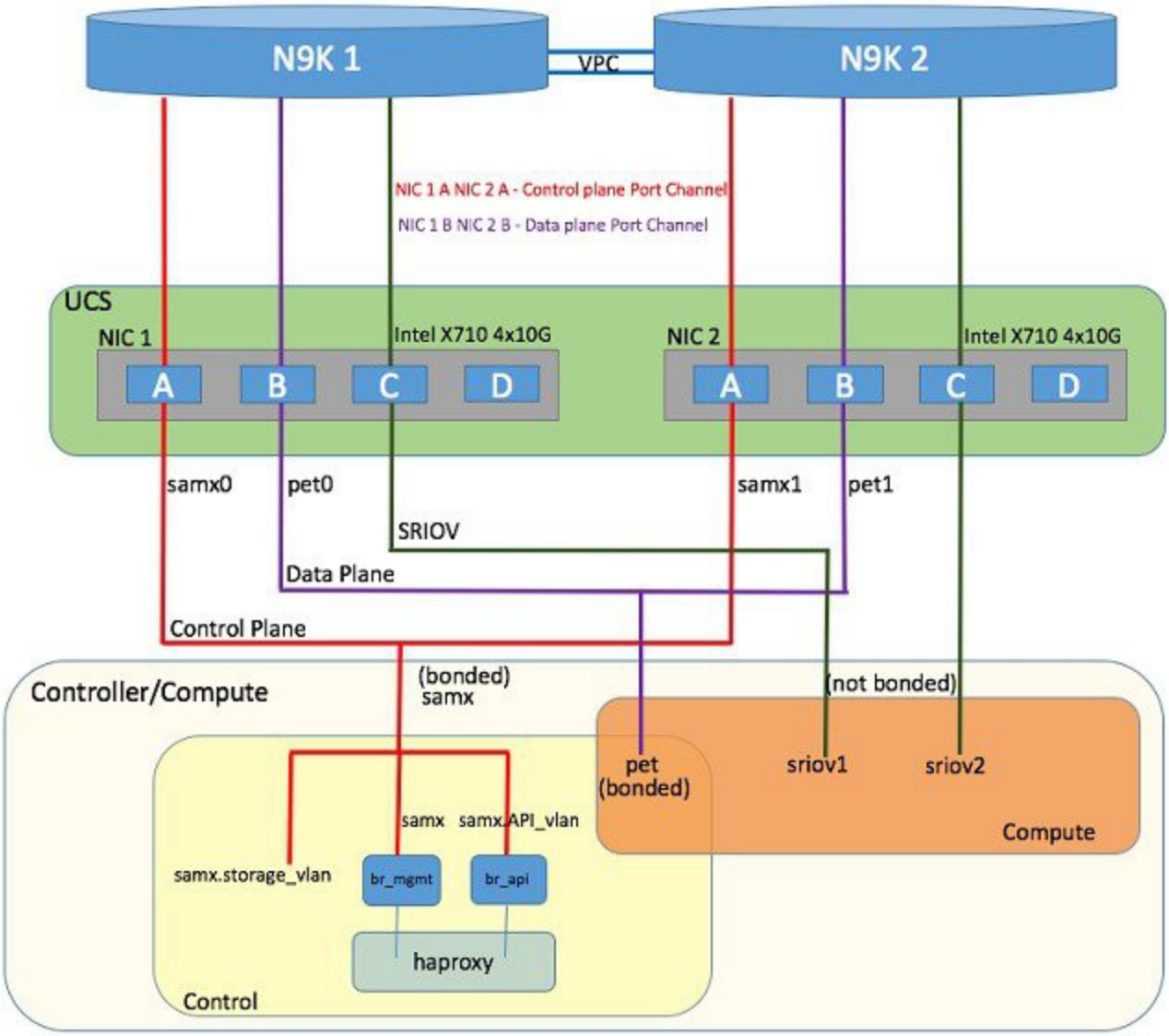
UCS C-Series Network Topologies

Cisco NFVI UCS servers are connected to the ToR switches using Cisco UCS dual-port Virtual Interface Cards (VICs). The VIC is an Enhanced Small Form-Factor Pluggable (SFP+) 10 Gigabit Ethernet and Fiber Channel over Ethernet (FCoE)-capable PCI Express (PCIe) card designed for Cisco UCS C-Series Rack Servers. Each port connects to a different ToR using a Virtual Port Channel (VPC). Each VIC is configured with multiple vNICs that correspond to specific Cisco VIM networks. The UCS Cisco IMC port is connected to an out-of-band (OOB) Cisco management switch.

The following figure shows the UCS C-series pod Cisco NFVI host to ToR topology.



For Intel NIC, a single two-port Cisco VIC in the preceding figure is replaced with two 4-port 710 Intel NIC. An extra Intel NIC is added to provide card level redundancy as shown in the figure below:



Of the four ports that are available in each NIC card, port A is used for management traffic (provision, API, storage, etc), whereas the port B is used for data plane (tenant and provider network) traffic. Port C (and optionally Port D) is dedicated for SRIOV (configured optionally based on setup_data.yaml). Sub-interfaces are carved out of the data and control plane interfaces to provide separate traffic based on specific roles. While the ports A and B from each NIC help in forming bonded interface, the ports C and D over which SRIOV traffic for provider network flows are not bonded.

You must take extreme care during pod setup, so that ports A, B and C for the Intel NIC is connected to the ToRs.

You can optionally use port D as the second pair of SRIOV ports with appropriate intent defined in the *setup_data.yaml* file. From Cisco VIM release 2.4.2 onwards, this port option is available for both M4 and M5 based systems or pods.
The following table provides the default link aggregation member pairing support for the pods based on server type:

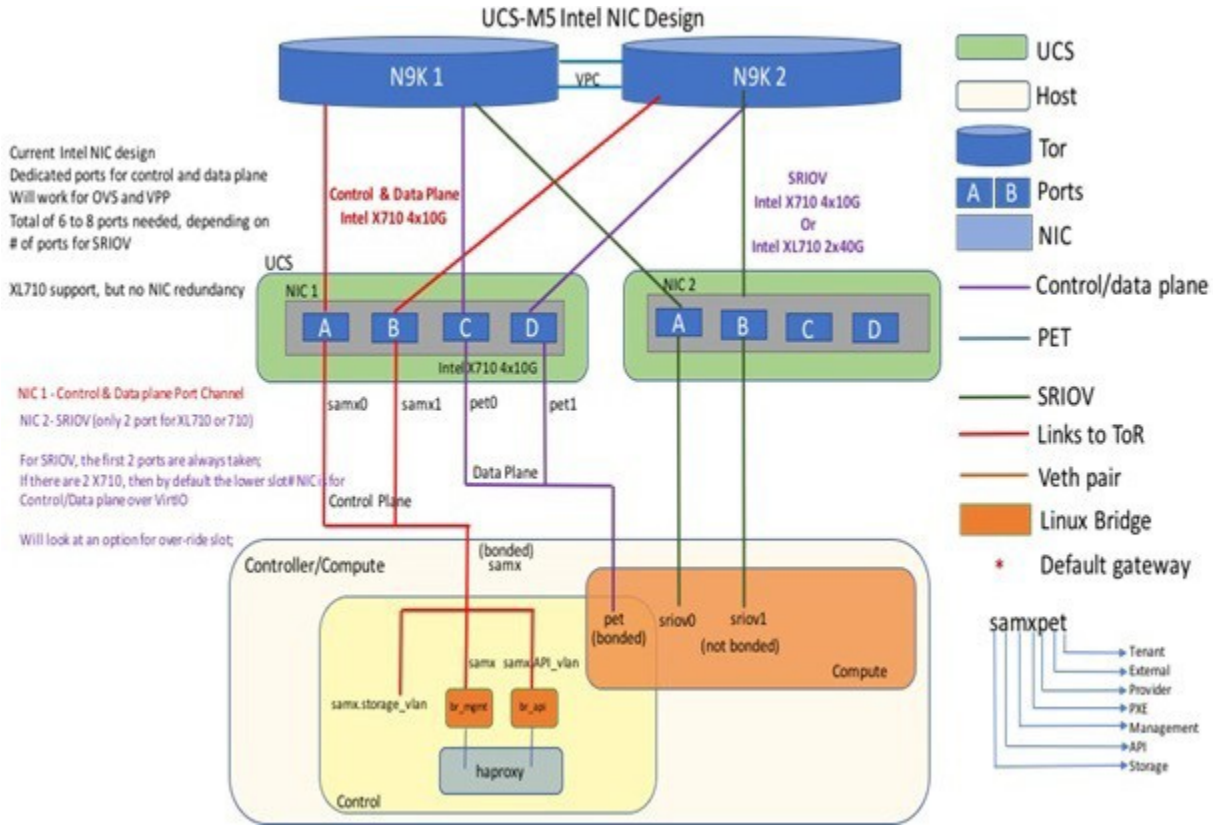
Server/POD Type	Target Functions	Default NIC Layout
M4 Intel NIC based	Control Plane	NIC-1 A + NIC-2 A
	Data Plane	NIC-1 B + NIC-2 B
	SRIOV 0/1	NIC-1 C + NIC-2 C
	SRIOV 2/3	NIC-1 D + NIC-2 D
M5 Intel NIC based	Control Plane	NIC-1 A + NIC-1 B
	Data Plane	NIC-1 C + NIC-1 D
	SRIOV 0/1	NIC-2 A + NIC-2 B
	SRIOV 2/3	NIC-2 C + NIC-2 D

⚠ In M5 pod, a NIC_LEVEL_REDUNDANCY option is available to support the M4 default option for link aggregation settings.

From Cisco VIM 2.4.2 onwards, support of M5 full on pods with two port XL-710 across control, compute and dedicated Ceph Nodes, and with NIC_LEVEL_REDUNDANCY is available. This deployment can be achieved with Cisco Nexus 9000 series or Cisco NCS 5500 as ToR. SRIOV is not supported in computes with XL-710. However, the pod can also support computes with four-port X-710, where SRIOV is over port C and D.

In Cisco VIM, computes (M4 based testbed) running a Cisco 1227 VIC, and 2 2-port Intel 520 NIC are supported. In this combination, SRIOV is running on the Intel NIC, whereas the control and data plane are carried by virtual interfaces over Cisco VIC.

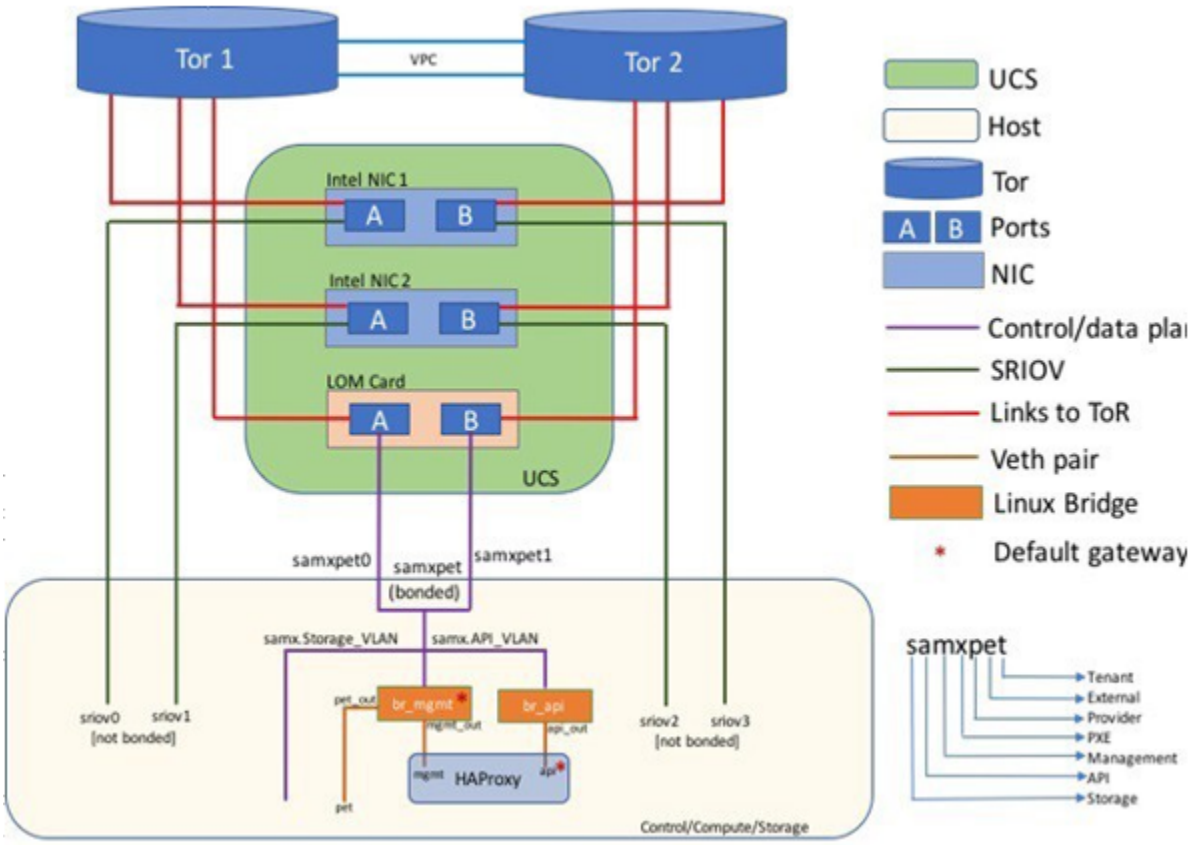
Cisco VIM 2.4 introduces the support of C220/C240 M5 servers in a micropod configuration with an option to augment the pod with additional computes (up to a max of 16). The M5 micropod environment is based on X710 for control and data plane and an additional XL710 or 2xX710 for SRIOV. The SRIOV card is optional. Once the SRIOV card is chosen, all the computes must have same number of SRIOV ports across the pod.
The following diagram depicts the server network card diagram for the UCS-M5 micropod setup.



Cisco VIM 2.4 introduces the first third-party compute. The first SKU chosen is HPE ProLiant DL360 Gen9. In Cisco VIM 2.4, the supported deployment is a full-on pod, with OVS as the mechanism driver, where the management, control, and storage nodes are based on existing Cisco UCS c220/240M4 BOM, and the compute nodes are on HPE ProLiant DL360 Gen9 hardware:

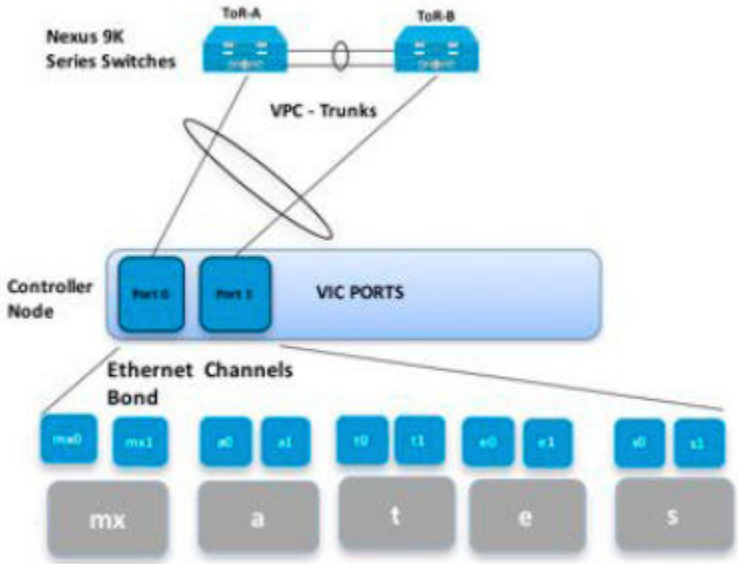
```
ProLiant DL360 Gen9 with HP Ethernet 1Gb 4-port 331i Adapter - NIC (755258-B21) 2 x E5-2695 v4 @ 2.10GHz CPU
8 x 32GB DDR4 memory (Total 256GB)
1 x Smart Array P440ar hardware RAID card with battery
2 x 1.2 TB - SAS 12GB/S 10k RPM HDD
1 x FlexLOM HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
2 x PCIe HP Ethernet 10Gb 2-port 560SFP+ Adapter
System ROM: P89 v2.40 (02/17/2017)
iLO Firmware Version: 2.54 Jun 15 2017
```

For HP Computes, the FlexLOM HP Ethernet 10Gb interface is used for management and tenant network, and the two additional HP Ethernet 10Gb 2-port 560SFP+ adapters are used for SRIOV for the provider network. Listed below is network schematic of the HP Compute node (HP DL360GEN9).

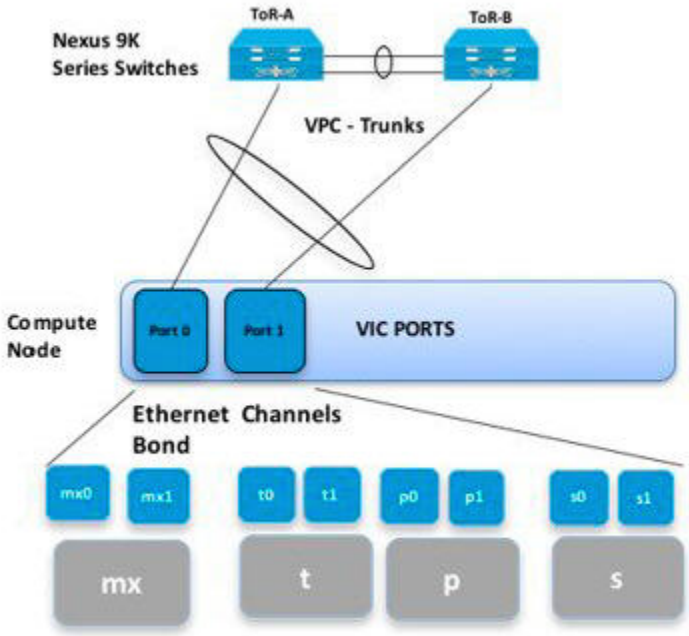


The Cisco NFVI controller node has four bonds: mx, a, t, and e. Each of them has an underlying interface that is named with the network name association and a mapped number. For example, the management and provisioning network, mx, maps to mx0 and mx1, the API network, a, to a0 and a1, and so on. The bonds map directly to the vNICs that are automatically created on the controller node when it is deployed.
Cisco VIM manages a third-party infrastructure based on Quanta servers, thereby bringing in true software abstraction. In the implementation, the supported deployment is a full-on or edge pod, with OVS as the mechanism driver. With the power limitation and rack restrictions on the edge pod, it cannot support hard-drives for the Ceph service. As the Edge pod does not need persistent storage, it is designed to communicate with a central ceph cluster for providing glance image services only.
The installation and management of the Central Ceph cluster is fully automated and it is assumed that the management network of the edge cloud is routable to that of the central Ceph cluster.
In the case of Quanta servers, the networking is similar to that of the HP computes except for the two port 25G (xxv710) Intel NICs. The 2x25GE OCP card is used for control and data plane network over virtio, and the two additional 25GE 2-port xxv710 based Intel NIC Adapters are used for SRIOV via the provider network.

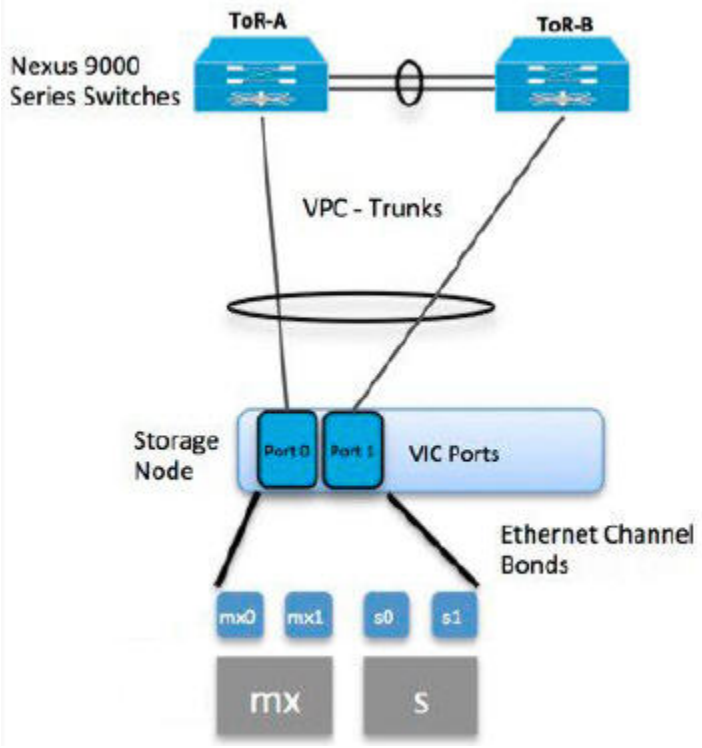
The following figure shows the controller node network-to-bond-to-vNIC interface mapping.



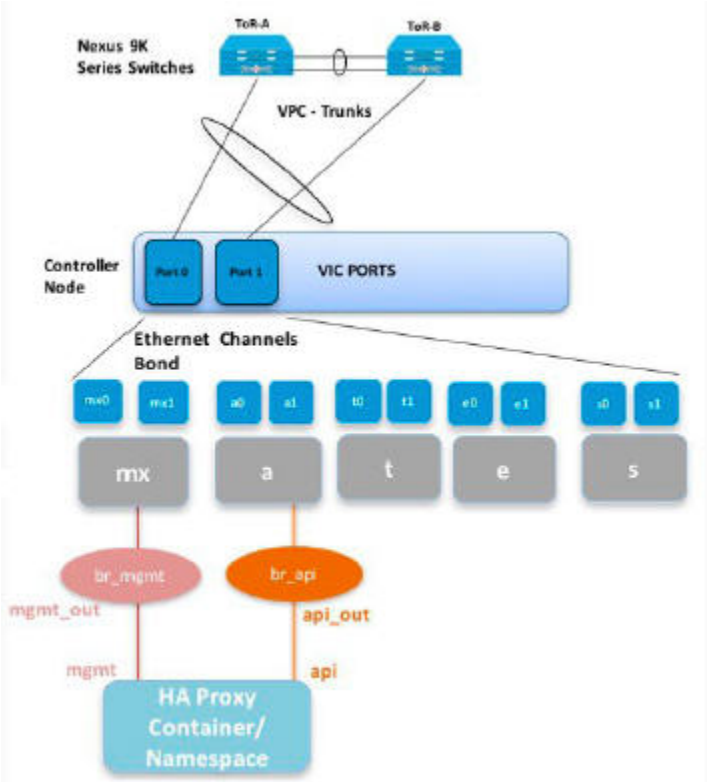
The Cisco NFVI compute node has three bonds: mx, t, and p. Each has an underlying interface that is named with the network name association and a mapped number. For example, the provider network, p, maps to p0 and p1. The bonds map directly to the vNICs that are automatically created on the compute node when it is deployed. The following figure shows the compute node network-to-bond-to-vNIC interfaces mapping.



The Cisco NFVI storage node has two bonds: mx and s. Each has an underlying interface that is named with the network name association and a mapped number. For example, the storage network, s, maps to s0 and s1. Storage nodes communicate with other storage nodes over the mx network. The storage network is only used for Ceph backend traffic. The bonds map directly to the vNICs that are automatically created on the storage node when it is deployed. The following figure shows the network-to-bond-to-vNIC interfaces mapping for Cisco NFVI storage node.



Cisco NFVI installation creates two bridges on the controller nodes and interfaces and bonds are attached to the bridges. The br_api bridge connects the API (a) interface to the HAProxy container. The HAProxy and Keepalive container has VIPs running for each OpenStack API endpoint. The br_mgmt bridge connects the Management and Provisioning (mx) interface to the HAProxy container as well.
The following figure shows the connectivity between the mx interface and the br_mgmt bridge, and the connectivity between the br_mgmt and the HAProxy container/namespace using mgmt_out and mgmt interfaces. The figure also shows the connectivity between the api interface and the br_api bridge, and the link between the br_mgmt bridge and the HAProxy container using api_out and mgmt_out interfaces.



A sample routing table is shown below, where *br_api* is the default route and *br_mgmt* is local to the pod.

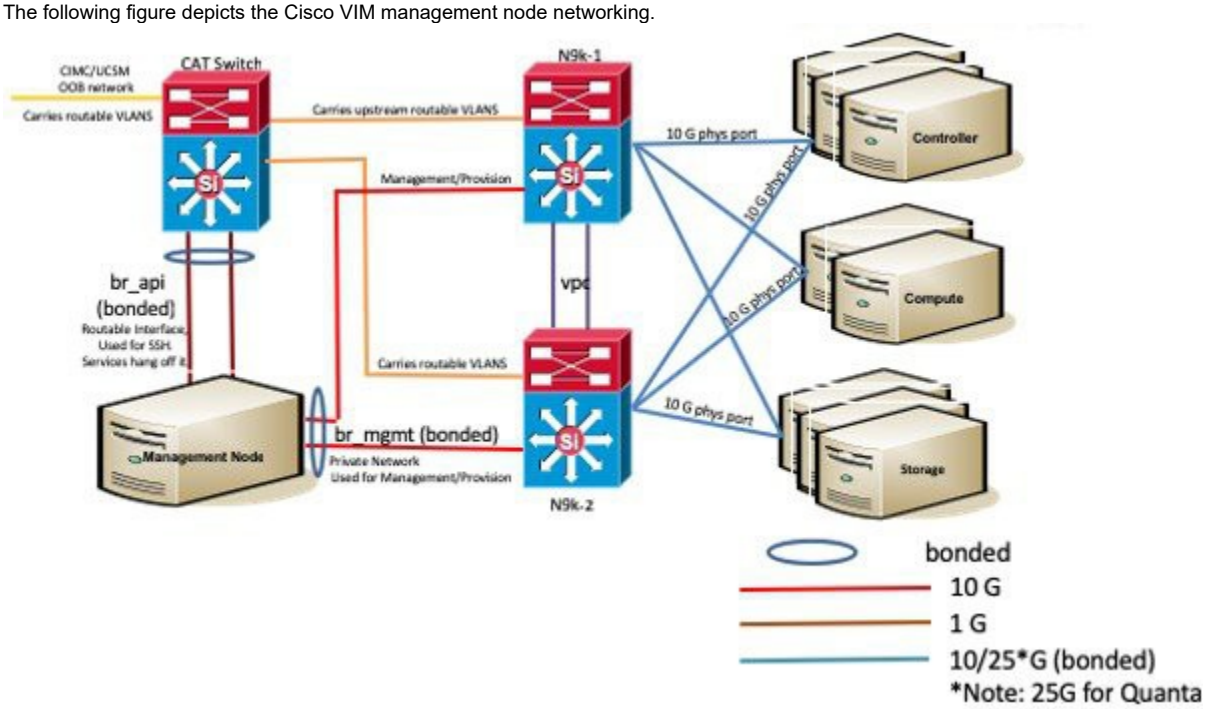
```
[root@c43-bot-mgmt ~]# ip route
default via 172.26.233.193 dev br_api proto static metric 425
172.26.233.0/25 dev br_mgmt proto kernel scope link src 172.26.233.104 metric 425
172.26.233.192/26 dev br_api proto kernel scope link src 172.26.233.230 metric 425

[root@c43-bot-mgmt ~]# ip addr show br_api
6: br_api: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
link/ether 58:ac:78:5c:91:e0 brd ff:ff:ff:ff:ff:ff
inet 172.26.233.230/26 brd 172.26.233.255 scope global br_api
valid_lft forever preferred_lft forever
inet6 fe80::2c1a:f6ff:feb4:656a/64 scope link
valid_lft forever preferred_lft forever

[root@c43-bot-mgmt ~]# ip addr show br_mgmt
7: br_mgmt: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
link/ether 58:ac:78:5c:e4:95 brd ff:ff:ff:ff:ff:ff
inet 172.26.233.104/25 brd 172.26.233.127 scope global br_mgmt
valid_lft forever preferred_lft forever
inet6 fe80::403:14ff:fef4:10c5/64 scope link
valid_lft forever preferred_lft forever
```

Management Node Networking

Management Node Networking

In Cisco VIM, the management node has an interface for API and another interface for provisioning. This is primarily done for security reasons, so that internal pod management or control plane messages (RabbitMQ, Maria DB, and so on) does not leak out, and hence reducing the attack vector to the pod. The API interface is used to access the VIM installer API and to SSH to the management node. All external services (installer API, Insight, ELK, and so on) are password-protected and hang off the API interface. The default route of the management node points to the API interface. The other interface or the provisioning interface is used to PXE boot the various nodes that constitute the OpenStack pod. Typically, the provisioning interface is a non-routable interface that is reserved for OpenStack management traffic.
In B-series pod, the networks between provisioning and the UCSM IP must be routable. You must apply proper ACL in the upstream router, so that other networks do not interfere with the provisioning network. Depending on the overall deployment, the management node acts as a jump-server to the OpenStack nodes.

The following figure depicts the Cisco VIM management node networking.



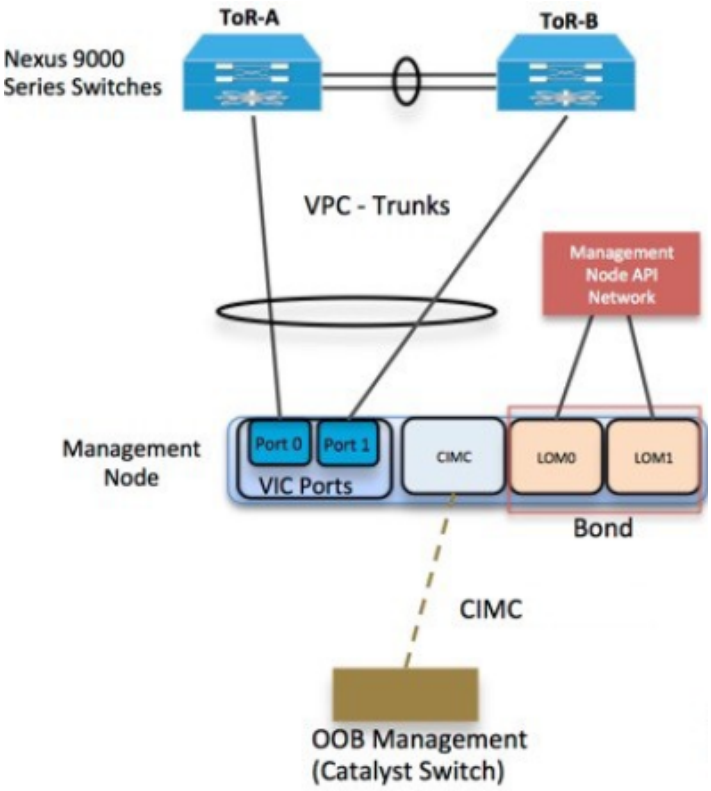
Cisco NFVI UCS C-series management node physically connects to the network. Unlike other nodes, the management node does not use multiple vNICs corresponding to specific Cisco NFVI networks. Instead, it connects to the management and API networks using two different physical connections. The management node connects to the management network using a Cisco two-port VIC or first two ports of intel X710-DA4, with each port connecting to a different ToR switch in a VPC configuration. The Cisco VIC card utilizes the default vNICs, but requires the vNICs to be in trunk mode and the default VLAN set to the management network VLAN.

The management node connects to the API network using both 1Gbps LAN On Motherboard (LOM) ports connected in a port-channel configuration. These ports can either connect to the Nexus 9000 series switch in a VPC configuration, or to an operator-managed switch, depending on how the operator wants to segment their network. The Cisco IMC port can optionally be connected to an out-of-band management Catalyst switch.

Management node services, which are required to start the other topology nodes, listen to the management network and the traffic flowing over the vNICs or NICs on that network. These services and the other management network services are unsecured. Secure management node services listen on the management node API network, and their traffic flows over the LOM ports. This service division allows tenants to utilize tighter network access control to the management network than the management node API network.

> ⚠ Connecting the Cisco IMC port to a Cisco OOB management switch is optional.

The following figure shows the Cisco NFVI management node (UCS C-series) API network connections.



For the Day 0 server automation in Cisco VIM, ensure that the reachability to:

- CIMC/ILO/BMC of the individual servers from the management node is available through the br_api network.
- Cloud API, external network (for ssh to floating IPs), and provider network from the management node is available, as the VMTP and NFVbench are typically run from the management node.

> ⚠ You can enable or disable the default behavior of the management node reachability from cloud API, external network, and provider network as part of their Day 0 configuration.

If you disable the reachability to cloud API, external, and provider network for security reasons, then:

- VMTP and NFVbench are not accessible from the management node.
- Cloud API, external network, and provider network must be properly routed as the Cisco VIM cannot automatically valid the same.

IPv6 Support

IPv6 Support on Management Network

As the number of available routable IPv4 networks is limited, Cisco VIM supports dual-stack environment. In a dual-stack environment, Cisco VIM honors all the external endpoints over IPv6, including OpenStack. The switching from IPv4 to IPv6 based environment needs a reinstallation of the entire pod. The internal networks similar to management/provision use a non-routable private IPv4 network to PXE boot the servers in a Layer 2 environment.

> ⚠ If the management node is Layer 3 adjacent to the pod made of UCS servers, the IPv4 address of the management network in the dual-stack environment is routable.

Enhancements are made so that the IPv4 address of the management network in the dual-stack environment is non-routable, when the pod is made up of Quanta servers.

As both CEPH (mon) and OpenStack control plane communication over IPv4 exists, you cannot completely remove IPv4 from the management network. However, you can run IPv4+IPv6 dual-stack in which IPv4 network can exist in a non-routable private network and IPv6 network can exist in a routable semi-private network. This satisfies the requirements of the Cisco VIM accessibility to the external services over IPv6.

In Cisco VIM, the management network supports IPv6 addresses for servers, while the management node is statically allocated from a given pool. The external services that support both IPv4 and IPv6 addresses are DNS, NTP, and AD or LDAP. You can run IPv4+IPv6 (optionally) as the cloud API endpoint. CIMC/BMC can have IPv6 addresses.

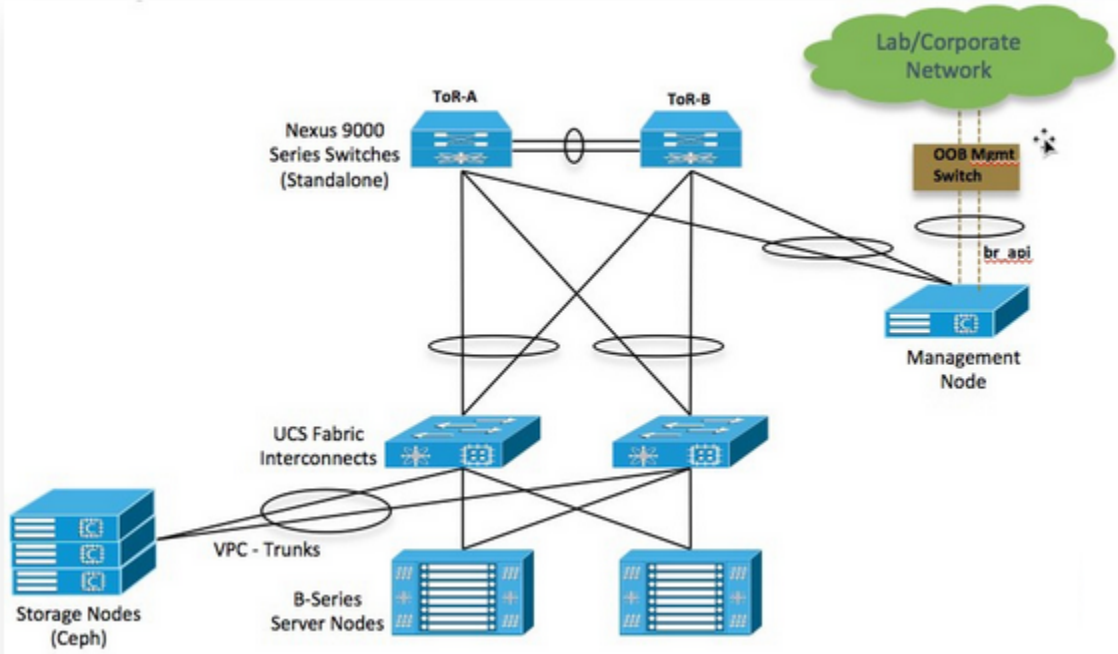
UCS C-Series/B-Series Topologies

UCS C-Series/B-Series Topologies

You can deploy Cisco NFVI using a combination of Cisco C-Series and B-Series servers. The C-series management node is connected to the Cisco Nexus 9000 Series ToRs through the Cisco VIC in a VPC configuration. The UCS Fabric Interconnects (FIs) are connected to the ToRs and the UCS B-Series blade chassis is connected to the FIs. The C-Series storage nodes are connected to the ToRs as well. For C-series implementation, see Networking Overview. For the combination of the C-Series and B-Series implementation, two exceptions are listed below:

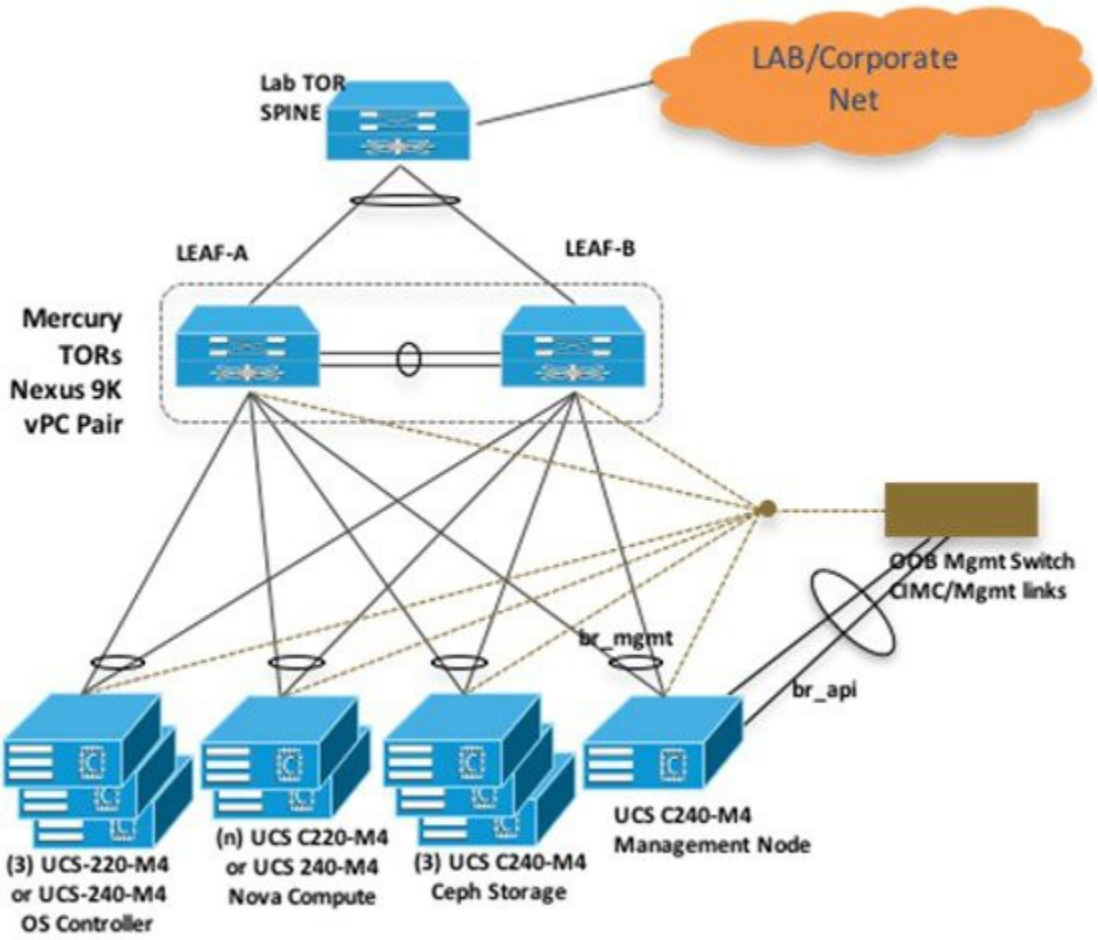
- For UCS B-Series, the Cisco UCS Manager IP address must be available to the Cisco NFVI management network. For UCS C-Series, this requirement is optional.
- The UCS Manager cluster and VIP connections are not attached to one of the Cisco NFVI network segments.

The following figure shows a high-level view of Cisco UCS C-series and B-series servers that are used in a Cisco NFVI deployment.



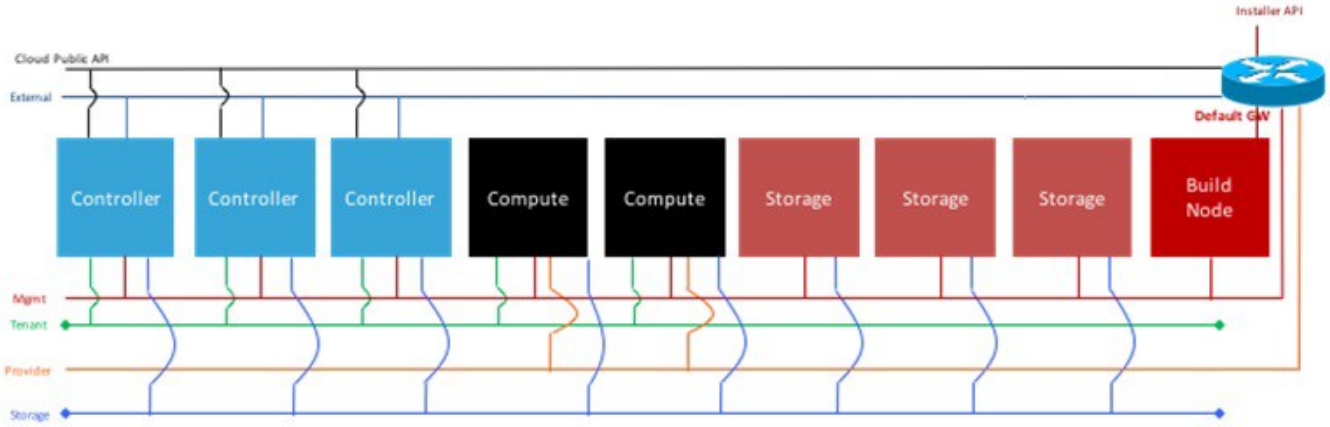
For C-Series pods, each host has a 2x10-GE Cisco network card 1227 from which the installer creates two vNICs for each network to ensure that the network topology has built-in redundancy. The provider network, if needed, is also created from the same network card. Each link of a given network type terminates to a unique Cisco Nexus 9000 switch, which acts as the ToR. The Cisco Nexus 9000s are configured in VPC mode to ensure that the network redundancy. The networking redundancy is extended to the management node, which has a redundant vNIC for the installer API and management or provisioning networks.

The following figure shows the C-Series topology.



Here, UCS 220 M4s is used as the control/compute, but it also supports UCS 240 M4s as control and compute nodes.

Cisco NFVI uses multiple networks and VLANs to isolate network segments. For UCS C-Series management and storage nodes, VLANs are trunked between the ToR switches and the Cisco VICs on the C-Series nodes. For UCS B-Series controllers and compute nodes, VLANs are trunked between the ToR switches, the UCS Fabric Interconnects, and the B-Series blades. The following figure shows the network segment layout for combined C-Series and B-Series installation. The network segments are VLANs that are trunked between the respective upstream switch/FI and the C-Series or B-Series node.



Cloud Public API – Used to access API endpoints – HAProxy front-ends the APIs – Publically Routable Space (needs very small prefix)
External – Per-tenant Neutron Routers attach 'public' interface to this segment – Publically Routable Space
Mgmt – Used for API-to-API traffic, SSH access to nodes and provisioning segment – RFC1918 space
Tenant – Used for VXLAN transit traffic (Controller/Compute nodes source VXLAN VTEPs from this network) – RFC1918 space
Provider – Used by tenants to connect instances directly to VLAN-trunked segments – Publically Routable or RFC1918 space
Storage – Used by Ceph for storage-only traffic (i.e. replication) – RFC1918 space

Installer API – Used to access services (ELK, UCSD, Installer API, etc) on Build node

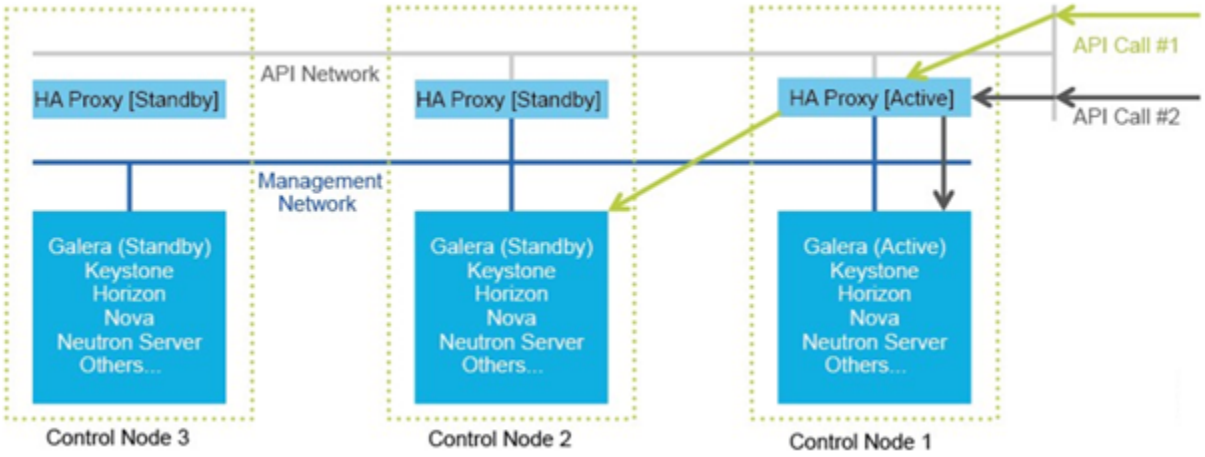
For B series, UCSM IP should be reachable from the management network

High Availability

High Availability

High availability (HA) is provided by HAProxy, a single-threaded, event-driven, non-blocking engine combining a fast I/O layer with a priority-based scheduler. HAProxy architecture is layered with bypass mechanisms at each level to ensure that the data does not reach higher levels than needed. Most processing is performed in the kernel.

The following figure shows a detailed view of Cisco NFVI controllers connecting to the API and Management and Provisioning network. It also shows how the bridges are configured and the roles of the HAProxy container and network namespace. The dedicated HAProxy container network namespace was created to avoid split default gateway problems. The namespace allows API segment ingress and egress traffic to have a different default gateway than the one configured on each controller host for non-API traffic. In the illustration, two of the three Cisco NFVI controllers have HAProxy containers and a dedicated Linux network namespace. Cisco NFVI supports three HAProxy containers.



In the figure, Control Node 1 is attached to the API network segment through the br_api bridge. The br_api bridge connects to the Linux network namespace where the HAProxy container has an interface that is mapped through the api < > api_out interface mapping. The HAProxy container has a default gateway configured that points to the upstream API Layer 3 First Hop Redundancy Protocol (FHRP) VIP. This gateway is used for the HAProxy container incoming and outgoing API traffic.

Outside traffic coming in through the API interface is routed into the API network. The traffic traverses the br_api bridge, goes into the Linux network namespace and then the API VIP (based on the IP address or port) that is listening on the HAProxy container. The HAProxy container establishes a connection with the backend API endpoint (for example, the OpenStack Horizon dashboard) and the return traffic passes through the container and back out the API network following the default gateway for the container on the API network. All other non-API traffic such as the management access over SSH to the Cisco VIM controller comes into the management or provisioning network and access the node directly. Return traffic uses the host-level default gateway that is configured on the Linux (RHEL) operating system.

If an HA event occurs in a Cisco NFVI pod, Cisco VIM automatically shuts down machines by failing over services. Examples include:

- For API servers, HAProxy automatically ensures that the other redundant control services handle requests, avoiding the shutdown/terminated/non-responding one.
- For quorum services, such as Galera, the remaining members of the quorum continue to provide service and HAProxy ensures that new requests go to the remaining processes.
- For an active/standby process such as HAProxy, the system moves the endpoint IP to a standby copy and continues to operate.

All these behaviors are automatic and do not require manual intervention. When the server is restarted, the services automatically come into service and are added to the load balancing pool, joining their quorums or are added as backup services, depending on the service type.

While manual intervention is not needed, some specific failure scenarios (for example, Mariadb, rabbit) can cause problems that require manual intervention. For example, if a complete network failure occurs, the Galera and RabbitMQ clusters can go into three-way partition. While the Cisco NFVI cluster is resilient to single-point failures, two switches failing simultaneously—something highly unlikely in long-running systems—can sometimes happen due to administrative error, in which case, manual intervention is needed.

To repair the pod, the management node must be up and running and all the nodes accessible through password-less SSH from the management node. From the *installer<tagid>* directory, execute:

```
ciscovim cluster-recovery
```

The control nodes are recovered after the network partitions are resolved. After executing this command, control nodes services come back to working state. To ensure that the Nova services are good across the compute nodes, execute the following command after sourcing */root/openstack-configs/openrc*:

```
nova service-list*
```

To check for the overall cloud status, execute the following:

```
# ciscovim
cloud-sanity create test all
```

To view the cloud-sanity results, use the following command:

```
#ciscovim cloud-sanity show result all -id
<uid of the test >
```

Storage Node Overview

Storage Node Overview

Block Storage

Cisco NFVI storage nodes utilize Ceph, an open source software for creating redundant, scalable data storage using clusters of standardized servers to store petabytes of accessible data. OpenStack Object Storage is a long-term storage system for large amounts of static data that can be retrieved, leveraged, and updated. It uses a distributed architecture with no central point of control, providing greater scalability, redundancy, and permanence. Objects are written to multiple hardware devices, with the OpenStack software responsible for ensuring data replication and integrity across the cluster. Storage clusters scale horizontally by adding new nodes. if a node fail, OpenStack replicates its content across other active storage nodes. Because Ceph uses software logic to ensure data replication and distribution across different devices, inexpensive commodity hard drives and servers can be used in lieu of more expensive equipment.

Cisco NFVI storage nodes include object storage devices (OSDs): consisting either of hard disk drives (HDDs), and/or solid state drives (SSDs). OSDs organize data into containers called objects that a user or application determines are related. The objects reside in a flat address space where they all exist at the same level and cannot be placed inside one another. Each OSD has a unique object identifier (OID) that allows the Cisco NFVI control node to retrieve it without knowing the physical location of the data it contains.

HDDs store and retrieve digital information using one or more rigid rapidly rotating disks coated with magnetic material. The disks are paired with magnetic heads arranged on a moving actuator arm, which read and write data to the disk surfaces. Data is accessed in a random-access manner; individual data blocks can be stored or retrieved in any order and not only sequentially. HDDs are a type of non-volatile memory, retaining stored data even when powered off.

SSDs are solid-state storage devices that use integrated circuit assemblies as memory to store data persistently. SSDs primarily use electronic interfaces compatible with traditional block input/output (I/O) hard disk drives, which permit simple replacements in common applications.
Cisco NFVI storage nodes are managed by the control node applications including Ceph monitoring dashboard, Glance, and Cinder. The Ceph monitoring dashboard provides a view into the overall storage node health. Glance virtualizes pools of block storage devices and provides a self-storage API to request and consume those resources. Cinder is an OpenStack block storage service designed to present storage resources to the OpenStack compute node.

In Cisco VIM, depending on the needs of the user, the number of OSDs a pod can have is between 3 and 20. From release Cisco VIM 3.0.0 onwards, you can choose to have multi-backend Ceph in the same pod, to support different I/O requirements. Currently, this is a day-0 decision. You must decide whether to start with single or multi back-end ceph, with a minimum of three nodes for each backend type. Only 2 backends (one of type HDD and another of type SSD) for each pod is supported. For details on how to use HDD or SSD based ceph, see Ceph Storage

Third Party Integration

NetApp

Cisco VIM supports NetApp devices running ONTAP 9.X or higher. NetApp devices are added as an alternate to Ceph for block storage. Cisco VIM is integrated and tested with FAS2650 SKU of NetApp, but it does not preclude Cisco VIM from working with SKUs of NetApp that are compatible FAS2650. Now, you have to choose the block storage and the hardware from Day 0. For more details, see NetApp Integration

SolidFire

In Cisco VIM, you can choose SolidFire as an option for block storage along with Ceph. In this scenario, the backend for Glance is Ceph. The Cinder block storage service manages the creation, attachment, and detachment of these volumes between a storage system, such as SolidFire and different host servers. The SolidFire cluster is pre-deployed with two networks: management and storage. It is recommended that:

- The storage network for Cisco VIM is same as that for SolidFire.
- The management network for SolidFire is reachable from Cisco VIM control nodes.

For details on how to enable SolidFire, see Enabling SolidFire

Zadara

The Zadara Virtual Private Storage Array (VPSA) is a software-defined solution, that is available as a Storage-as-a-Service with the storage servers residing in the customer premise. It is an elastic system that provides Enterprise-grade data protection and data management storage services. Cisco VIM provides Day 0 seamless integration with Zadara, and hence enables the following value add associated to it:

- Enterprise quality, resilient, highly available, and consistent performance storage for the most demanding data center application workloads.
- Consumed as a service - flexible, dynamic and billable.
- Scale out - to hundreds of storage nodes, thousands of drives, and multi-petabyte storage.
- True multi-tenancy - End-user controlled privacy and security. Separate workloads, resource allocation, and management per tenant such that each tenant truly experiences secure storage with no noisy neighbor.

- Universal storage - Supports all data services on one common infrastructure: Block, File, Object.

For details on how to enable Zadara, see Enabling Zadara

Cisco VTS Overview

Cisco Virtual Topology System (VTS) Overview

The Cisco Virtual Topology System (VTS) is a standards-based, open, overlay management and provisioning system for data center networks. It automates the data center overlay fabric provisioning for both physical and virtual workloads. It provides a network virtualization architecture and software-defined networking (SDN) framework that meets multi-tenant data center cloud service requirements.

It enables a policy-based approach for overlay provisioning. It automates network overlay provisioning and management tasks, integrates with OpenStack, and simplifies the management of heterogeneous network environments. Also, provides an embedded Cisco VTS GUI and a set of northbound Representational State Transfer (REST) APIs that is consumed by orchestration and cloud management systems.

Cisco VTS architecture has two main components namely policy plane and control plane. These perform core functions such as SDN control, resource allocation, and core management function.

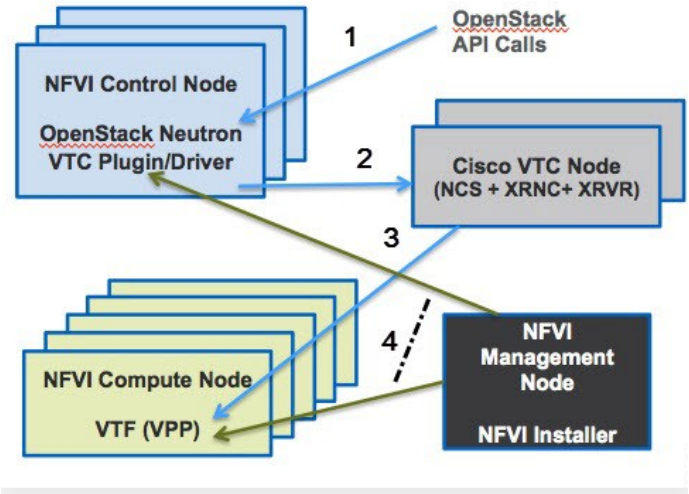
- Policy plane: Enables Cisco VTS to implement a declarative policy model that captures user intent and converts it into specific device-level constructs. Cisco VTS includes a set of modular policy constructs that can be organized into user-defined services for use cases across service provider and cloud environments. The policy constructs are exposed through REST APIs that is consumed by orchestrators and applications to express user intent, or instantiated through the Cisco VTS GUI. Policy models are exposed to system policies or service policies.
- Control plane: Serves as the SDN control subsystem that programs the various data planes including the VTFs residing on the x86 servers, hardware leafs, DCI gateways. The control plane hosts the Cisco IOS XRv Software instance that provides route peering capabilities between the DCI gateways or to a BGP route reflector. (Cisco IOS XRv is the virtualized version of Cisco IOS XR Software.) The control plane enables an MP-BGP EVPN-based control plane for VXLAN overlays originating from leafs or software VXLAN tunnel endpoints (VTEPs)

The Cisco NFVI implementation of Cisco VTS includes Virtual Topology Forwarder (VTF). VTF provides a Layer 2/Layer 3 (L2/L3) software switch that can act as a software VXLAN terminal endpoint (VTEP). VTF is a lightweight, multi-tenant software data plane designed for high-performance packet processing on x86 servers. VTF uses Vector Packet Processing (VPP). VPP is a full-featured networking stack with a software forwarding engine. VTF leverages VPP and the Intel Data Path Development Kit (DPDK) for high-performance L2, L3, and VXLAN packet forwarding.
VTF allows Cisco VTS to terminate VXLAN tunnels on host servers by using the VTF as a software VXLAN Tunnel Endpoint (VTEP). Cisco VTS also supports hybrid overlays by stitching together physical and virtual endpoints into a single VXLAN segment.

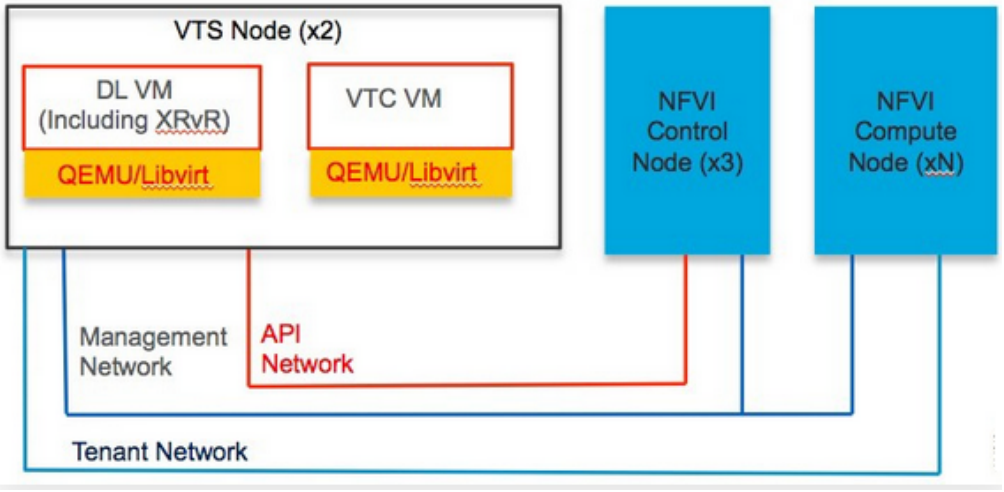
Cisco VTS is installed on separate UCS servers such that the Virtual Topology Controller plugin is installed on the control node and the VTF is installed on the compute node.

1. The OpenStack user invokes the OpenStack Neutron API.
2. Neutron uses the VTS plugin and driver to make calls to the VTC REST API.
3. VTS control components interact with the VTF agent to carry out the corresponding dataplane setup.
4. During Cisco NFVI installation, the Cisco NFVI Installer installs the OpenStack Neutron VTC plugin and driver on the Cisco NFVI controller node, and installs the VTF component (including VPP) on the Cisco NFVI compute node.

The figure below shows the architecture of Cisco VTS when installed in Cisco NFVI.



The following figure illustrates the Cisco NFVI networking after Cisco VTS is installed. The SDN controller nodes are an addition to the existing Cisco NFVI pod.



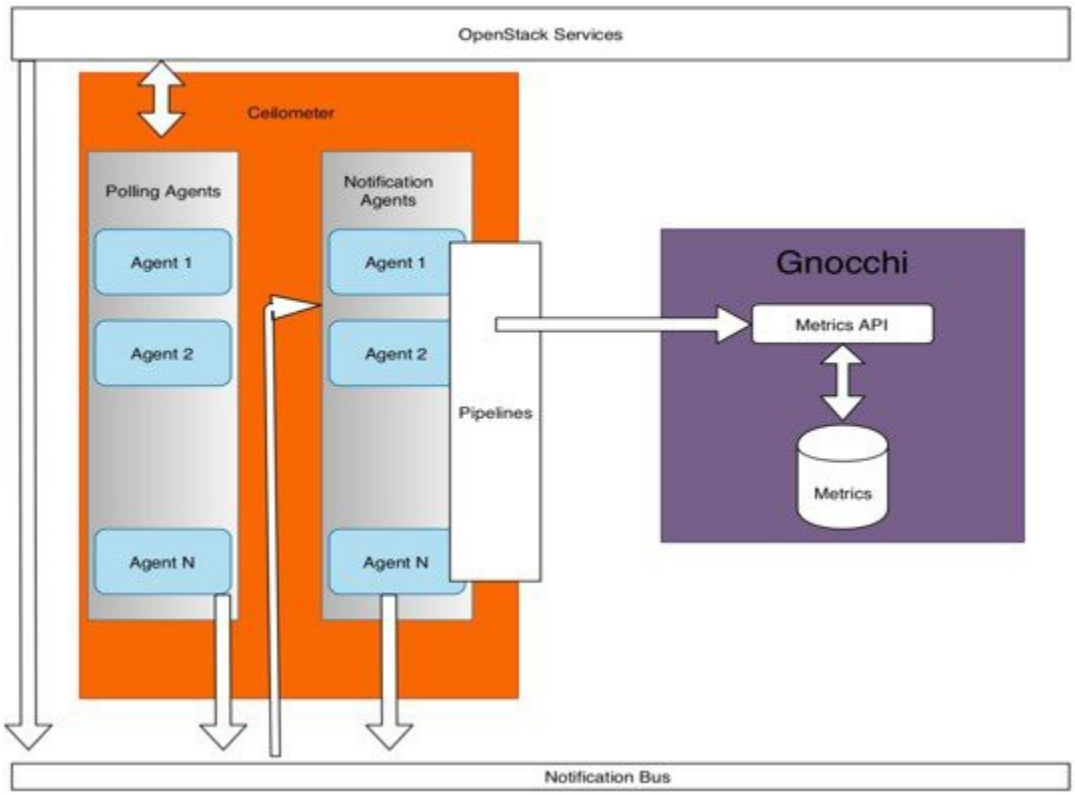
OpenStack Telemetry Service

OpenStack Telemetry Service

Overview

Cisco VIM provides telemetry services to collect meters within an OpenStack deployment. Cisco VIM Telemetry service is built on Ceilometer and Gnocchi in OpenStack Queens release. You can retrieve metrics using OpenStack CLI and REST APIs. Pods must have Ceph for persistent storage of the metrics which are collected every five minutes and retained for 48 hours. As Ceph is required for ceilometer, you can install ceilometer as part of fresh installation of the cloud, that is, ceilometer cannot be brought in as a reconfigure option. Also, the ceilometer is supported only on fullon pod.

The following figure illustrates the high-level architecture of the telemetry services.



If ceilometer is enabled in *setup_data.yaml* file, the Telemetry service in Cisco VIM collects the metrics within the OpenStack deployment.

- Once ceilometer is added as Day 0 configuration on a fullon pod, you can only deploy the pod but cannot be uninstalled.
- If ceilometer is deployed and metrics are generated, CEPH status indicates HEALTH_WARN. This is normal as ceilometer metrics pool have too many objects per placement group than average value. However, this specific warning does not block any pod management operation.

This section provides a summary of the metrics that are collected with the Cisco VIM using ceilometer/gnocchi OpenStack REST-API.

OpenStack Compute

The following metrics are collected for OpenStack Compute:

Name	Type	Unit	Resource	Origin	Note
memory	Gauge	MB	instance ID	Notification	Volume of RAM allocated to the instance

memory.usage	Gauge	MB	instance ID	Pollster	Volume of RAM used by the instance from the amount of its allocated memory
cpu	Cumulative	ns	instance ID	Pollster	CPU time used
cpu.delta	Delta	ns	instance ID	Pollster	CPU time used since previous datapoint
cpu_util	Gauge	%	instance ID	Pollster	Average CPU utilization
vcpus	Gauge	vcpu	instance ID	Notification	Number of virtual CPUs allocated to the instance
disk.read.requests	Cumulative	request	instance ID	Pollster	Number of read requests
disk.read.requests.rate	Gauge	request/s	instance ID	Pollster	Average rate of read requests
disk.write.requests	Cumulative	request	instance ID	Pollster	Number of write requests
disk.write.requests.rate	Gauge	request/s	instance ID	Pollster	Average rate of write requests
disk.read.bytes	Cumulative	B	instance ID	Pollster	Volume of reads
disk.read.bytes.rate	Gauge	B/s	instance ID	Pollster	Average rate of reads
disk.write.bytes	Cumulative	B	instance ID	Pollster	Volume of writes
disk.write.bytes.rate	Gauge	B/s	instance ID	Pollster	Average rate of writes
disk.device.read.requests	Cumulative	request	disk ID	Pollster	Number of read requests
disk.device.read.requests.rate	Gauge	request/s	disk ID	Pollster	Average rate of read requests
disk.device.write.requests	Cumulative	request	disk ID	Pollster	Number of write requests
disk.device.write.requests.rate	Gauge	request/s	disk ID	Pollster	Average rate of write requests
disk.device.read.bytes	Cumulative	B	disk ID	Pollster	Volume of reads
disk.device.read.bytes .rate	Gauge	B/s	disk ID	Pollster	Average rate of reads
disk.device.write.bytes	Cumulative	B	disk ID	Pollster	Volume of writes
disk.device.write.bytes.rate	Gauge	B/s	disk ID	Pollster	Average rate of writes
disk.root.size	Gauge	GB	instance ID	Notification	Size of root disk
disk.ephemeral.size	Gauge	GB	instance ID	Notification	Size of ephemeral disk
disk.capacity	Gauge	B	instance ID	Pollster	The amount of disk that the instance can see
disk.allocation	Gauge	B	instance ID	Pollster	The amount of disk occupied by the instance on the host machine
disk.usage	Gauge	B	instance ID	Pollster	The physical size in bytes of the image container on the host
disk.device.capacity	Gauge	B	disk ID	Pollster	The amount of disk per device that the instance can see
disk.device.allocation	Gauge	B	disk ID	Pollster	The amount of disk per device occupied by the instance on the host machine
disk.device.usage	Gauge	B	disk ID	Pollster	The physical size in bytes of the image container on the host per device
network.incoming.bytes	Cumulative	B	interface ID	Pollster	Number of incoming bytes
network.incoming.bytes.rate	Gauge	B/s	interface ID	Pollster	Average rate of incoming bytes
network.outgoing.bytes	Cumulative	B	interface ID	Pollster	Number of outgoing bytes
network.outgoing.bytes.rate	Gauge	B/s	interface ID	Pollster	Average rate of outgoing bytes
network.incoming.packets	Cumulative	packet	interface ID	Pollster	Number of incoming packets
network.incoming.packets.rate	Gauge	packet/s	interface ID	Pollster	Average rate of incoming packets
network.outgoing.packets	Cumulative	packet	interface ID	Pollster	Number of outgoing packets
network.outgoing.packets.rate	Gauge	packet/s	interface ID	Pollster	Average rate of outgoing packets
network.incoming.packets.drop	Cumulative	packet	interface ID	Pollster	Number of incoming dropped packets
network.outgoing.packets.drop	Cumulative	packet	interface ID	Pollster	Number of outgoing dropped packets
network.incoming.packets.error	Cumulative	packet	interface ID	Pollster	Number of incoming error packets
network.outgoing.packets.error	Cumulative	packet	interface ID	Pollster	Number of outgoing error packets
memory.swap.in	Cumulative	MB	interface ID	Pollster	Memory swap in
memory.swap.out	Cumulative	MB	interface ID	Pollster	Memory swap out
disk.device.read.latency	Cumulative	ns	Disk ID	Pollster	Total time read operations have taken

OpenStack Image

The following metrics are collected for OpenStack Image service:

Name	Type	Unit	Resource	Origin	Note
image.size	Gauge	B	image ID	Notification, Pollster	Size of the uploaded image
image.download	Delta	B	image ID	Notification	Image is downloaded
image.serve	Delta	B	image ID	Notification	Image is served out

OpenStack Block Storage

The following metrics are collected for OpenStack Block Storage:

Name	Type	Unit	Resource	Origin	Note
volume.size	Gauge	GB	Voulume ID	Notification	Size of the volume

Metrics Polling and Retention Policy

Cisco VIM telemetry service polls metrics every 5 minutes and retains the metrics for 48 hours.

For more details, see Heat, Ceilometer, LBaaS

NFVBench

NFVBench

Setting up NFVbench

Setting up and Using NFVbench

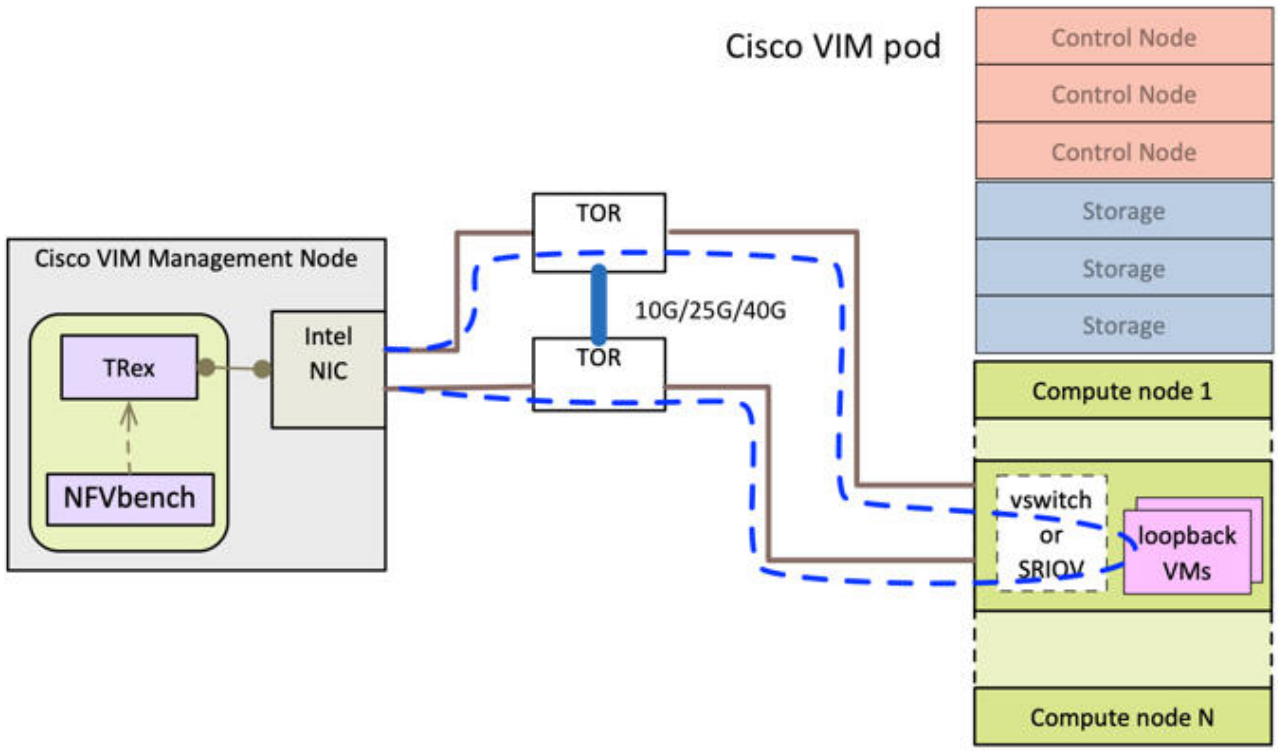
Overview

NFVbench is a built-in network benchmarking tool that provides a consistent methodology to measure the network performance of the cloud without the need to install and use dedicated traffic generators.

You can use the NFVbench to:

- Verify whether the deployed data plane is working properly and efficiently when using well-defined packet paths that are typical of NFV service chains.
- Measure the actual performance of the deployed infrastructure data plane, so that you can estimate the amount of traffic that can be sent and received by one or more VNFs.

The following figure illustrates a typical benchmark run with NFVbench:



NFVbench runs on the management node inside a container along with the TRex open source software traffic generator. The traffic generator uses a dedicated Intel NIC to send and receive traffic to the ToRs.

A typical benchmark run with NFVbench:

- Loads a test loopback VM image into Openstack using the glance API. This is done only for the first time execution of NFVbench on the pod.
- Requests Openstack to create two virtual networks, two virtual interfaces, and a VM with that loopback image using the Neutron and Nova APIs.
- Programs the traffic generator to generate UDP packets with the right L3 and L2 headers to follow the packet path outlined by the dashed blue line, once the VM is up and running in a compute node.
- Starts the traffic generation.
- Stops the traffic generation, collects the results, and presents them in a user-friendly format, at the end of the benchmark.

The traffic flows through a ToR switch to virtual switch on compute node, continues to VM representing any basic VNF in NFV deployment, and comes back in a similar way on different ports. You can compute the network performance or throughput, based on the sent and received traffic.

NFVbench supports the following Cisco VIM data plane network options:

- OVS with VLAN
- VPP virtual switch with VLAN
- VPP virtual switch with VxLAN overlay
- SRIOV

Pre-requisites

- For NFVbench running on the management node, the software traffic generator needs an extra Intel NIC X710 (2x10Gbps), XXV710 (2x25Gbps), or XL710 (2x40Gbps) with two ports connected to the ToRs.
- The NFVBENCH option must be enabled in the Cisco VIM configuration file using the following command:

```
NFVBENCH:
  enabled: true
  tor_info: {sjc04-tora-pod6: eth1/22, sjc04-torb-pod6: eth1/22}
```

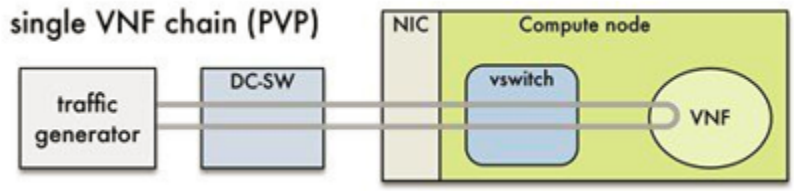
- The tor_info option must specify the interface names on the ToRs where the two Intel NIC ports reserved for NFVbench are connected.
- NFVbench can be enabled post deployment using a reconfigure operation.

Built-in packet paths

NFVbench can setup and stage one or more service chains each containing one or two VNFs .

Single VNF Chain

The default packet path is Physical - VM - Physical (PVP) and represents a typical service chain made of one VNF/VM:



The traffic generator runs within the NFVbench container on the management node. DC-SW represents the top of rack (ToR) switches. The VNF is a test VM that contains a fast L2 forwarder that can emulate a very fast VNF.

The traffic generator generates bi-directional traffic with the UDP packets generated on the two physical interfaces. The switch forwards the packets to the appropriate compute node before arriving to the virtual switch, and then to the VNF before looping back to the traffic generator on the other interface.

In the case of SRIOV, the packets bypass the virtual switch and go directly between the compute node NIC and the test VM.

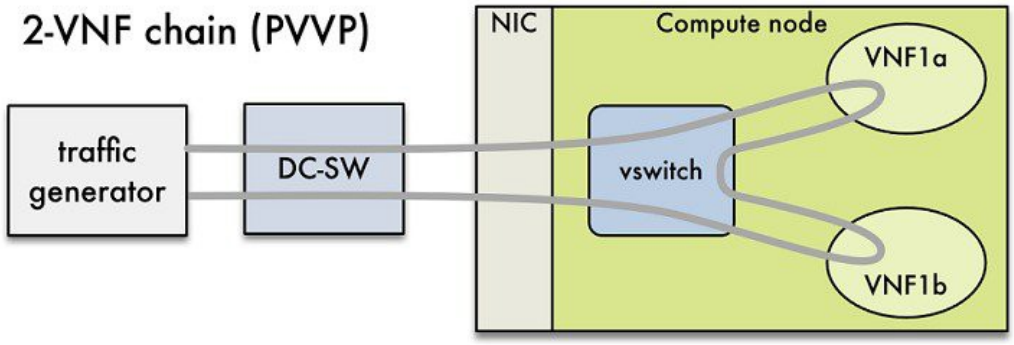
The performance of the PVP packet path provides a very good indication of the capabilities and efficiency of the NFVI data plane in the case of a single service chain made of one VNF/VM.

Two-VNF Chain

NFVbench also supports more complex service chains made of two VMs in sequence and called Physical-VM-VM-Physical (PVVP).

In a PVVP packet path, the two VMs reside on the same compute node.

The following figure illustrates packet path having two-VM chain.



NFVBench Command-Line Options and Status

You can execute most of the benchmark variants using CLI options from the shell prompt on the management node. The NFVbench command-line options are displayed using the --help option:

```
[root@mgmt1 ~]# nfvbench --help
```

Use the --status option to check the NFVbench version and see if benchmark is running:

```
[root@mgmt1 ~]# nfvbench -status
2018-12-19 20:29:49,656 INFO Version: 3.X.X
2018-12-19 20:29:49,656 INFO Status: idle
2018-12-19 20:29:49,704 INFO Discovering instances nfvbench-loop-vm...
2018-12-19 20:29:50,645 INFO Discovering flavor nfvbench.medium...
2018-12-19 20:29:50,686 INFO Discovering networks...
2018-12-19 20:29:50,828 INFO No matching NFVbench resources found
```

Using NFVbench Configuration File

More advanced use-cases require passing a yaml NFVbench configuration file. You can get the complete default NFVbench configuration file by using the *-show-default-config* option (the output of which can be redirected to a file). Navigate to the host folder mapped to the NFVbench container *(/root/nfvbench)* and copy the default NFVbench configuration by using the following command:

```
[root@mgmt1 ~]# cd /root/nfvbench
[root@mgmt1 ~]# nfvbench --show-default-config > nfvbench.cfg
```

Edit the configuration file to remove all the properties that are not changed and retain the properties that are required. For example, if the default timeout for launching the test VM is too short, you can keep the following lines in the configuration file and increase the number of retries from 100 to 200:

```
# General retry count
generic_retry_count:200
```

All other lines in the default configuration file can be removed. The NFVbench always loads the original default configuration file first before overwriting the properties that are specified in the passed configuration file.

When ready, the edited configuration file is passed to NFVbench using the -c option. Ensure that you use the container visible pathname, as this file is read from the container. The */root/nfvbench* folder on the host is mapped to the */tmp/nfvbench* folder in the container, so the configuration file stored under */root/nfvbench/<file>* must be referenced as */tmp/nfvbench/<file>* in the CLI option.

For example:

```
[root@mgmt1 ~]# nfvbench -c /tmp/nfvbench/nfvbench.cfg
```

You can use additional command line options with the -c option.

Control Plane Verification

If you are trying NFVbench for the first time, verify that the tool can stage the default packet path properly without sending any traffic. The *--no-traffic* option exercises the control plane by creating a single test service chain with one VM, but does not send any traffic.

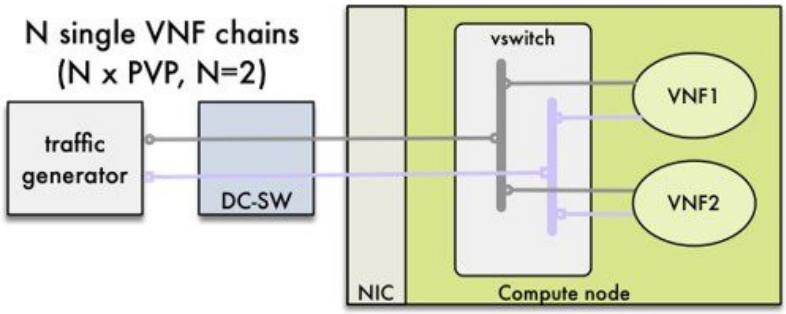
The following command stages only the default PVP packet path, but does not generate any traffic:

```
[root@mgmt1 ~]# nfvbench --no-traffic
```

Testing

Reports from NFVbench show the data measurements from every hop in the path, to detect the configuration errors or potential bottlenecks.

Advanced testing using NFVbench allows to conduct multi-chain and multi-flow testing. Multi-chain testing enables running multiple parallel independent packet paths at the same time, while the multi-flow testing performs IP ranging in packet headers within every chain. The below figure illustrates a NFVbench result test execution with two parallel chains with one VM each.



Fixed Rate Test

NFVbench offers a simple test to run traffic at a fixed rate, to verify whether each network component of packet path is working properly. It is useful for identifying bottlenecks in the test environment.
Traffic generator generates packets at a fixed rate for a specified duration. For example, you can generate a total of 10000 packets per second (which is 5000 packets per second per direction) for the default duration (60 seconds), with the default frame size of 64 bytes using the following configuration:

```
[root@mgmt1 ~]# nfvbench
```

You can specify any list of frame sizes using the -frame-size option (pass as many as desired), including IMIX.

Following is an example to run a fixed rate with IMIX and 1518 byte frames:

```
[root@mgmt1 ~]# nfvbench --rate 10kpps --frame-size IMIX --frame-size 1518
```

No Drop Rate (NDR)/Partial Drop Rate (PDR) Test

NDR/PDR test is used to determine the performance of the data plane in terms of throughput at a given drop rate using any of the standard defined packet sizes - 64B, IMIX,1518B. The NDR value represents highest throughput achieved when no packets are dropped. It allows packet drop rate of less than 0.001%. PDR represents the highest throughput achieved when only small number of packets is dropped. The packet dropped is less than 0.1% of packets sent.

NDR is always less or equal to PDR.

To calculate the NDR and PDR for your pod, run the following command:

```
[root@mgmt1 ~]# nfvbench --rate ndr_pdr
```

From the collected statistics, drop rates and latencies are computed and displayed.

Both the NDR/PDR test and fixed rate test provide a way of verifying network performance of NFV solution.

Multi-chain Test

In multi-chain test, each chain represents an independent packet path symbolizing real VNF chain. You can run multiple concurrent chains and simulate network conditions in real production environment. Results with single chain versus with multiple chains usually vary because of services competing for resources (RAM, CPU, and network).

To stage and measure multiple service chains at the same time, use *--service-chain-count* flag or shorter *-scc* version.

The following example shows how to run the fixed-rate run test with ten PVP chains:

```
[root@mgmt1 ~]# nfvbench -scc 10 --rate 100kpps
```

The following example shows how to run the NDR/PDR test with ten PVP chains:

```
[root@mgmt1 ~]# nfvbench -scc 10 --rate ndr_pdr
```

Multi-flow Test

In a multi-flow test, one flow is defined by a source and destination MAC/IP/port tuple in the generated packets. It is possible to have many flows per chain. The maximum number of flows that are supported is in the order of 1 million flows per direction. The following command runs three chains with a total of 100K flows per direction (for all chains):

```
[root@mgmt1 ~]# nfvbench -scc 3 -fc 100k
```

External Chain Test

NFVbench measures the performance of chains that are pre-staged (using any means external to NFVbench). These chains can be real VNFs with L3 routing capabilities or L2 forwarding chains.

The external chain test is used when you want to use NFVbench only for traffic generation. In this case, NFVbench sends traffic from the traffic generator and reports results without performing any Openstack staging or configuration.

Ensure that the setup is staged externally prior to running NFVbench by creating networks and VMs with a configuration that allows generated traffic to pass. You need to provide the name of the two edge Neutron networks to which the traffic generators are to be attached, during configuration, so that NFVbench can discover the associated segmentation ID (VLAN or VNI).

If the external chains support only L2 forwarding, the NFVbench configuration must specify the destination MAC to be used in each direction for each chain.

If the external chains support IPv4 routing, the NFVbench configuration must specify the public IP addresses of the service chain end points (gateway IP) that are used to discover destination MAC using ARP.

To measure performance for external chains, use the *--service-chain EXT (or -sc EXT)* option:

```
[root@mgmt1 ~]# nfvbench -sc EXT
```

NFVbench Results

You can store the detailed NFVbench results in JSON format using the below command, if you pass the *--json* option with a destination file name or the *--std-json* option with a destination folder pathname to use the standard file name generated by NFVbench.

```
[root@mgmt1 ~]# nfvbench -scc 3 -fc 10 -fs 64 --json /tmp/nfvbench/my.json
```

The above command stores the results in JSON file in */tmp/nfvbench container* directory. This file will be visible at the host level under the *~/nfvbench* directory as *~/nfvbench/my.json.*

Examples of NFVbench Result Execution

VLAN Fixed Rate

The following example shows the generation of the default frame size (64B) over 100Kpps for the default duration (60s) with the default chain type (PVP), default chain count (1) and default flow count (10k):

```
# nfvbench -rate 100kpps -fs IMIX
```

The summary of NFVbench result is shown below:

```
Date: 2018-12-19 21:26:26
NFVBench version 3.0.4.dev2
Openstack Neutron:
vSwitch: VPP
Encapsulation: VLAN
Benchmarks:
> Networks:
> Components:
> Traffic Generator:
Profile: trex-local
Tool: TRex
> Versions:
> Traffic_Generator:
build_date: Nov 13 2017
version: v2.32
built_by: hhaim
mode: STL
build_time: 10:58:17
> VPP: 18.07
> CiscoVIM: 2.4.3-15536
> Service chain:
> PVP:
> Traffic:
Profile: custom_traffic_profile
Bidirectional: True
Flow count: 10000
Service chains count: 1
Compute nodes: [u'nova:c45-compute-2']
```

The following NFVbench result execution summary table provides the drop rate measured (in this example no drops) and latency measurements in micro-seconds (time for a packet to be sent on one port and receive back on the other port).

L2 Frame Size	Drop Rate	Avg Latency (usec)	Min Latency (usec)	Max Latency (usec)
IMIX	0.0000%	28	20	330

The following NFVbench result configuration table provides the mode details for both forward and reverse directions, where:

1. Requested TX Rate is the rate that is requested in bps and pps.
2. Actual TX Rate is the actual rate achieved by the traffic generator. It can be lower than the requested rate if there is not enough CPU.
3. RX Rate is the rate of packets received.

Direction	Requested TX Rate (bps)	Actual TX Rate (bps)	RX Rate (bps)	Requested TX Rate (pps)	Actual TX Rate (pps)	RX Rate (pps)
Forward	152.7333 Mbps	152.7334 Mbps	152.7344 Mbps	50,000 pps	50,000 pps	50,000 pps
Reverse	152.7333 Mbps	152.7334 Mbps	152.7344 Mbps	50,000 pps	50,000 pps	50,000 pps
Total	305.4667 Mbps	305.4668 Mbps	305.4688 Mbps	100,000 pps	100,000 pps	100,000 pps

The forward and reverse chain packet counters and latency table shows the number of packets sent or received at different hops in the packet path, where:

- TRex.TX.p0 or p1 shows the number of packets sent from each port by the traffic generator.
- Vpp.RX.vlan.<id> shows the number of packets received on the VLAN sub-interface with VLAN id <id> in the VPP vswitch.
- Vpp.TX.veth/<id> shows the number of packets sent to the VM.
- Vpp.RX.veth/<id> shows the number of packets received from the VM.

The following table shows the forward chain packet counters and latency:

Chain	TRex.TX. p0	vpp.RX.vlan. 1547*	vpp.TX.veth /2	vpp.RX.veth /1*	vpp.TX.vlan. 1511	TRex.RX. p1*	Avg Latency	Min Latency	Max Latency
0	3,000,001	=>	=>	=>	=>	3,000,001	28 usec	20 usec	320 usec

The following table shows the reverse chain packet counters and latency:

Chain	TRex.TX.p1	vpp.RX.vlan.1511*	vpp.TX.veth/1	vpp.RX.veth/2*	vpp.TX.vlan.1547	TRex.RX.p0*	Avg Latency	Min Latency	Max Latency
0	3,000,001	=>	=>	=>	=>	3,000,001	28 usec	20 usec	330 usec

⚠ '=>' indicates that no packets are dropped. Otherwise, the value will indicate the number of packets dropped.

VLAN NDR/PDR

Use the following command to measure NDR and PDR for IMIX, with the default chain type (PVP), default chain count (1) and default flow count (10k):

```
# nfvbench -fs IMIX
```

The summary of the NFVbench result execution is shown below:

```
Date: 2018-12-20 23:11:01
NFVBench version 3.0.5.dev2
Openstack Neutron:
vSwitch: VPP
Encapsulation: VLAN
Benchmarks:
> Networks:
        > Components:
                > Traffic Generator:
                        Profile: trex-local
                        Tool: TRex
        > Versions:
                > Traffic_Generator:
                        build_date: Nov 13 2017
                        version: v2.32
                        built_by: hhaim
                        mode: STL
                        build_time: 10:58:17
        > VPP: 18.07
        > CiscoVIM: 2.3.46-17358
        > Measurement Parameters:
                NDR: 0.001
                PDR: 0.1
        > Service chain:
                > PVP:
                        > Traffic:
                                Profile: custom_traffic_profile
                                Bidirectional: True
                                Flow count: 10000
                                Service chains count: 1
                                Compute nodes: [u'nova:a22-mchester-micro-3']
```

The NFVBench result execution summary table shows the following:

- L2 frame size
- Highest throughput achieved in bps and pps below the drop rate thresholds being the sum of TX for both ports.
- Drop rate measured
- Latency measured (average, min, max)

The following table shows NFVBench result execution summary

	L2 Frame Size	Rate (fwd+rev) in Gbps	Rate (fwd+rev) in pps	Avg Drop Rate	Avg Latency (usec)	Min Latency (usec)	Max Latency (usec)
NDR	IMIX	8.5352	2,794,136	0.0000%	124	10	245
PDR	IMIX	9.5703	3,133,012	0.0680%	167	10	259

VXLAN Fixed Rate

It is applicable for platforms that support VxLAN only.

Example 1:

In this example, the default frame size of 64B is sent over 1Mpps on two chains using VxLAN with flow count of 10k:

```
# nfvbench --duration 10 -scc 2 --rate 1Mpps --vxlan
```

The summary of the NFVBench result is shown below:

```
2018-12-20 23:28:24,715 INFO --duration 10 -scc 2 --rate 1Mpps --vxlan
2018-12-20 23:28:24,716 INFO VxLAN: vlan_tagging forced to False (inner VLAN tagging must be disabled)
2018-12-20 23:28:24,716 INFO Using default VxLAN segmentation_id 5034 for middle internal network
2018-12-20 23:28:24,716 INFO Using default VxLAN segmentation_id 5017 for right internal network
2018-12-20 23:28:24,716 INFO Using default VxLAN segmentation_id 5000 for left internal network
```

Example 2:

In this example, VxLAN benchmark is run and 64B frames are sent over 100kpps for the default duration.

```
# nfvbench -rate 100kpps --vxlan
2018-12-18 19:25:31,056 INFO VxLAN: vlan_tagging forced to False (inner VLAN tagging must be disabled)
2018-12-18 19:25:31,056 INFO Using default VxLAN segmentation_id 5034 for middle internal network
2018-12-18 19:25:31,056 INFO Using default VxLAN segmentation_id 5017 for right internal network
2018-12-18 19:25:31,056 INFO Using default VxLAN segmentation_id 5000 for left internal network
```

The NFVBench result summary is as follows:

```
Date: 2018-12-18 19:26:40
NFVBench version 3.0.5.dev2
Openstack Neutron:
vSwitch: VPP
Encapsulation: VxLAN
Benchmarks:
> Networks:
        > Components:
                > Traffic Generator:
                        Profile: trex-local
                        Tool: TRex
                > Versions:
                        > Traffic_Generator:
                                build_date: Nov 13 2017
                                version: v2.32
                                built_by: hhaim
                                mode: STL
                                build_time: 10:58:17
                > VPP: 18.07
                > CiscoVIM: 2.3.46-17358
        > Service chain:
                > PVP:
                        > Traffic:
                                Profile: traffic_profile_64B
                                Bidirectional: True
                                Flow count: 10000
                                Service chains count: 1
                                Compute nodes: [u'nova:a22-mchester-micro-1']
```

The following table shows the NFVBench result summary:

L2 Frame Size	Drop Rate	Avg Latency (usec)	Min Latency (usec)	Max Latency (usec)
64	0.0000%	0	nan	0

The following table shows the NFVBench result configuration:

Direction	Requested TX Rate (bps)	Actual TX Rate (bps)	RX Rate (bps	Requested TX Rate (pps)	Actual TX Rate (pps)	RX Rate (pps)

Forward	33.6000 Mbps	33.6000 Mbps	33.6000 Mbps	50,000 pps	50,000 pps	50,000 pps
Reverse	33.6000 Mbps	33.6000 Mbps	33.6000 Mbps	50,000 pps	50,000 pps	50,000 pps
Total	67.2000 Mbps	67.2000 Mbps	67.2000 Mbps	100,000 pps	100,000 pps	100,000 pps

The following table shows forward chain packet counters and latency:

Chain	TRex.TX.p0	vpp.RX.vxlan_tunnel0	vpp.TX.veth/0	vpp.RX.veth/1	vpp.TX.vxlan_tunnel1	TRex.RX.p1
0	50,000	=>	=>	=>	=>	50,000

The following table shows reverse chain packet counters and latency:

Chain	TRex.TX.p1	vpp.RX.vxlan_tunnel1	vpp.TX.veth/1	vpp.RX.veth/0	vpp.TX.vxlan_tunnel0	TRex.RX.p0
0	50,000	=>	=>	=>	=>	50,000

Encapsulation

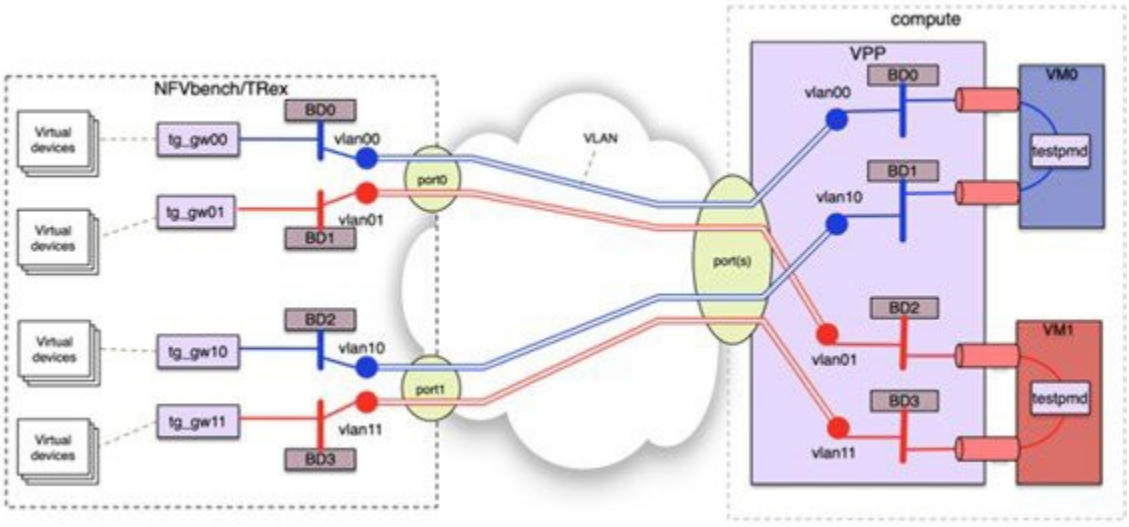
Encapsulation

NFVBench supports all networking options that can be deployed with Cisco VIM:

- OVS
- VPP with VLAN or VxLAN
- Single root input/output virtualization (SR-IOV)

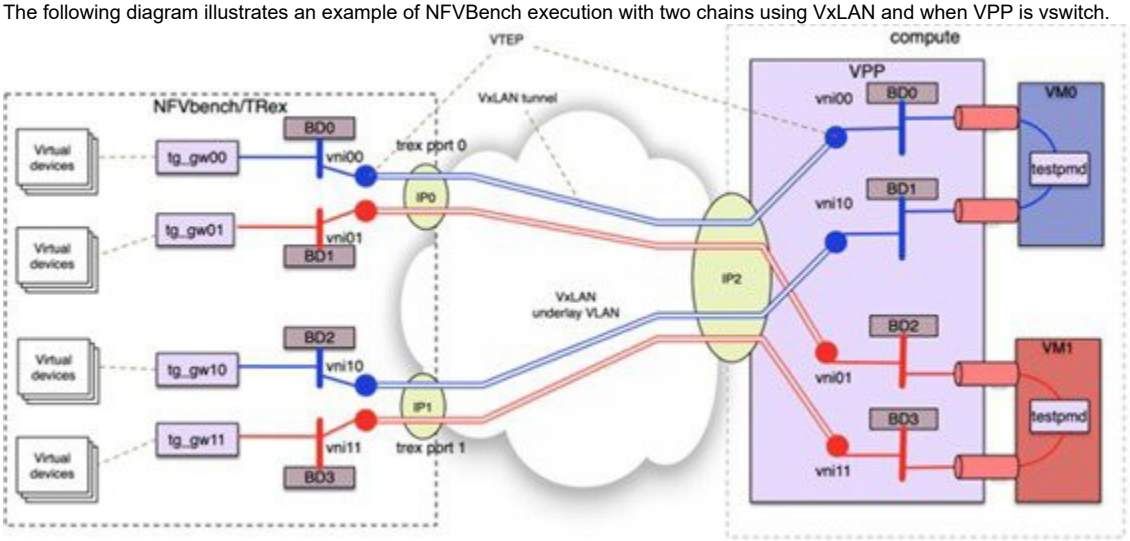
By default, NFVBench uses VLAN tagging for the generated traffic and directs the traffic to the vswitch in the target compute node (OVS or VPP).

The following diagram illustrates an example of NFVBench execution with two chains using VLAN and when VPP is vswitch.



If VxLAN is enabled, it is possible to force the use of VxLAN using the –vxlan CLI option.
The provision of custom configuration allows you to specify more VxLAN options such as specific VNIs to use. For more details, check the default configuration file.

The following diagram illustrates an example of NFVBench execution with two chains using VxLAN and when VPP is vswitch.



SR-IOV

If SR-IOV is deployed, NFVBench can support to send the traffic to the test VMs that use SR-IOV instead of vswitch.
To test SR-IOV, you must have compute nodes configured to support one or more SR-IOV interfaces (also knows as physical function (PF)) and OpenStack to support SR-IOV.
You need to know:

- The name of the physical networks associated with the SR-IOV interfaces (this is a configuration in Nova compute).
- The VLAN range to be used for the switch ports that are wired to the SR-IOV ports. Such switch ports are normally configured in trunk mode with a range of VLAN IDs enabled on that port.

For example, if two SR-IOV ports exist per compute node, two physical networks are generally configured in OpenStack with a distinct name.
The VLAN range to use is also allocated and reserved by the network administrator and in coordination with the corresponding top of rack switch port configuration.

To enable SR-IOV test, you must provide the following configuration options to NFVbench in the configuration file.
The following example instructs NFVBench to create the left and right networks of a PVP packet flow to run on two SRIOV ports named `phys_sriov0` and `phys_sriov1` using respective segmentation_id 2000 and 2001:

```
sriov: true
internal_networks:
left:
segmentation_id: 2000
physical_network: phys_sriov0
right:
segmentation_id: 2001
physical_network: phys_sriov1
```

The segmentation ID fields must be different.
In case of PVVP, the middle network must be provisioned properly. The same physical network can also be shared by the virtual networks, but with different segmentation IDs.

Cisco VIM CLI

Cisco VIM CLI

An alternate way to NFVBench CLI is to use ciscovimclient. Ciscovimclient provides an interface that is more consistent with the Cisco VIM CLI and can run remotely while the NFVBench CLI is executed on the management node.

Pass JSON configuration matching the structure of the NFVBench configuration file to start a test:

```
[root@mgmt1 ~]# ciscovim nfvbench --config '{"rate": "10kpps"}
+------------------+--------------------------------------+
| Name             | Value                                |
+------------------+--------------------------------------+
| status           | not_run                              |
| nfvbench_request | {"rate": "5kpps"}                    |
| uuid             | 0f131259-d20f-420f-840d-363bdcc26eb9 |
| created_at       | 2017-06-26T18:15:24.228637           |
+------------------+--------------------------------------+
```

Run the following command with the returned UUID to poll status:

```
[root@mgmt1 ~]# ciscovim nfvbench --stat 0f131259-d20f-420f-840d-363bdcc26eb9
+------------------+--------------------------------------+
| Name             | Value                                |
+------------------+--------------------------------------+
| status           | nfvbench_running                     |
| nfvbench_request | {"rate": "5kpps"}                    |
| uuid             | 0f131259-d20f-420f-840d-363bdcc26eb9 |
| created_at       | 2017-06-26T18:15:24.228637           |
| updated_at       | 2017-06-26T18:15:32.385080           |
+------------------+--------------------------------------+
+------------------+--------------------------------------+
| Name             | Value                                |
+------------------+--------------------------------------+
| status           | nfvbench_completed                   |
| nfvbench_request | {"rate": "5kpps"}                    |
| uuid             | 0f131259-d20f-420f-840d-363bdcc26eb9 |
| created_at       | 2017-06-26T18:15:24.228637           |
| updated_at       | 2017-06-26T18:18:32.045616           |
+------------------+--------------------------------------+
```

When the test is done, retrieve results in a JSON format:

```
[root@mgmt1 ~]# ciscovim nfvbench --json 0f131259-d20f-420f-840d-363bdcc26eb9
{"status": "PROCESSED", "message": {"date": "2017-06-26 11:15:37", ...}}
```

NFVBench REST Interface

When enabled, the NFVBench container can also take benchmark request from a local REST interface. Access is only local to the management node in the Cisco VIM (that is the REST client must run on the management node). For more details on the REST interface calls, see Cisco VIM REST API Resources.

Auto-ToR Configuration via ACI API

Auto-ToR Configuration via ACI API

While the use of ACI plugin brings in the flexibility of dynamic allocation of tenant and provider VLANs on demand, it also ties the OVS version to the ACI plugin. This leads to an extreme tight coupling of Cisco VIM and ACI.

With an APIC plugin, there are might be gaps to cover certain use-cases, for example, where there is a need to have flexibility of different access types (tagged or non-tagged) for the same VLAN but for different servers.

To address such use-case or avoid tight coupling of OVS with ACI plugin, an optional solution is available to automate the target VLANs on the right switch port based on the server role on Day 0 along with corresponding fabric access and tenant policy configurations via the ACI API.

With this option, the *setup_data* for each Cisco VIM instance is the single source for the server to switch port mappings. Also, this solution can handle switch provisioning with the correct VLANs during the addition or removal of server and provider/tenant VLAN range expansion via reconfiguration option. The solution is based on the fact that the PV (port VLAN) count in a given ACI fabric domain is under the scale limits 10000 PV/ToR and 450000 PV /Fabric. For details on ACI enablement, see Enabling ACI

NCS-5500 as ToR Option

NCS-5500 as ToR Option

Cisco VIM supports NCS-5500 as an alternate to a Nexus ToR. NCS-5500 is an IOS XR-based router which is similar to Nexus switches. You can use the 48 10/25G ports or the 6 40/100G uplink ports model to implement NCS-5500 (port-numbers depend on NCS version). Also, other SKUs of NCS-5500 are supported as long as the NCS-5500 software supports the EVLAG feature.

NCS-5500 uses the technology of bridge domain to connect to the server. The auto-ToR configuration is enabled to support NCS-5500 as ToR. NCS-5500 supports a Micropod with more computes running on Intel 710 NICs with the mechanism driver of VPP over LACP. The support is extended to include 40G /100G based NCS-5500 SKUs with splitter cables (of 4x10) connecting to the servers, which helps in increasing the server port density by four folds. For more details, see ToR Management

Disk Management

Disk Management

Cisco VIM uses the disk-maintenance tool that gives you the ability to check the status of all hard disk drives present in the running and operational mode in the following nodes:

- Management node.
- Specific or all controller servers.
- Specific or all compute servers.

The disk status such as online, offline, and rebuilding helps you to identify the disks in which slot has potentially gone bad and require to be physically replaced in the server. It can be run on servers that have either a RAID controller or an SAS pass through controller.
Once the disk is physically replaced, you can use the disk management tool to add the new disk back into the system as part of the RAID system (recommended one server at a time). For more information, see Disk and OSD Maintenance Tools.

Disk maintenance tool is useful only when one or two (in RAID6) disks is not working. Failure of more than one disk at a time sets the entire server in an irrecoverable state. Replace the server using remove and add operations through Cisco VIM. Disk management is not supported on a third-party compute due to the licensing issue with the HPE SmartArray Utility tool.

OSD Maintenance

OSD Maintenance

OSD maintenance tool gives you the ability to check the status of all OSDs and their corresponding physical hard disk drives present in the running and operational storage nodes. The status of the OSDs is reported along with the HDD mapping. It helps you to identify the status of the OSD (Up or Down) and its corresponding hard disk drive slot in the server that requires to be physically replaced. It can run on servers that have either a RAID or an SAS passthrough controller.

Once the HDD to be physically replaced is identified, the same OSD tool can be used to re-balance the ceph tree, remove the OSD from the cluster, and unmount the disk drive, in preparation for the disk removal. After the disk has been physically replaced, the tool can be used to add the new disk back into the system as part of the Ceph cluster and recreate the OSD (only one HDD/OSD at a time). It ensures to replace a bad HDD, it is not required to remove the ceph cluster from operation and then add it back through remove-storage and add-storage options in ciscovim. OSD Disk and OSD Maintenance Tools section has the relevant details.

OSD tool does not support the replacement of the internal OS drives and external journal drives, for which you still have to add or remove OSD nodes.

Power Management

Power Management of Computes for C-Series

Though many compute servers are available for Cisco VIM pods, only limited compute servers are actually used at certain times. To optimize the overall power consumption of the data center, it is required to power down the server through an API/CLI.
To prevent the cloud destabilization, ensure that you do not power off all the compute nodes and maintain at least one pod in active state.
Pod management operation(s) applies to the entire pod during update and reconfiguration of the server. Update and reconfiguration are not possible under the following circumstances:

- If one or more compute nodes are powered off.
- Computes on which VMs are running cannot be powered-off.
- Computes with All-in-one (AIO) nodes in a micro-pod cannot be powered-off through this API.

When there is a power-off, the cloud-sanity is run internally. If the cloud-sanity fails, the power-off action is aborted. For more details, see Managing Power and Reboot

Physical Cores and Reserved Memory

Physical Cores and Reserved Memory

Cisco VIM has been tuned to deliver performance from an infrastructure and VNF point of view. The following table gives the details of the physical cores (regardless of whether hyperthread is enabled or not) that the infrastructure needs. The number of cores that are reserved for the system (host system + OpenStack services) is two in all cases.

Pod Type/Node Types	Control	Storage	Compute	AIO	HC
FullOn	all	all	CPU: 2+V cores RAM: 25+Vr GB	n/a	n/a
Hyperconverged (hc)		n/a		n/a	CPU: 2+C+V cores RAM: 41+Vr GB
Micropod (aio)	n/a	n/a		CPU: Q+C+V cores RAM: 41+Vr GB	N/A
Edge-pod	Q	n/a		n/a	n/a

The following table shows the number of physical cores and RAM Reserved for Cisco VIM:

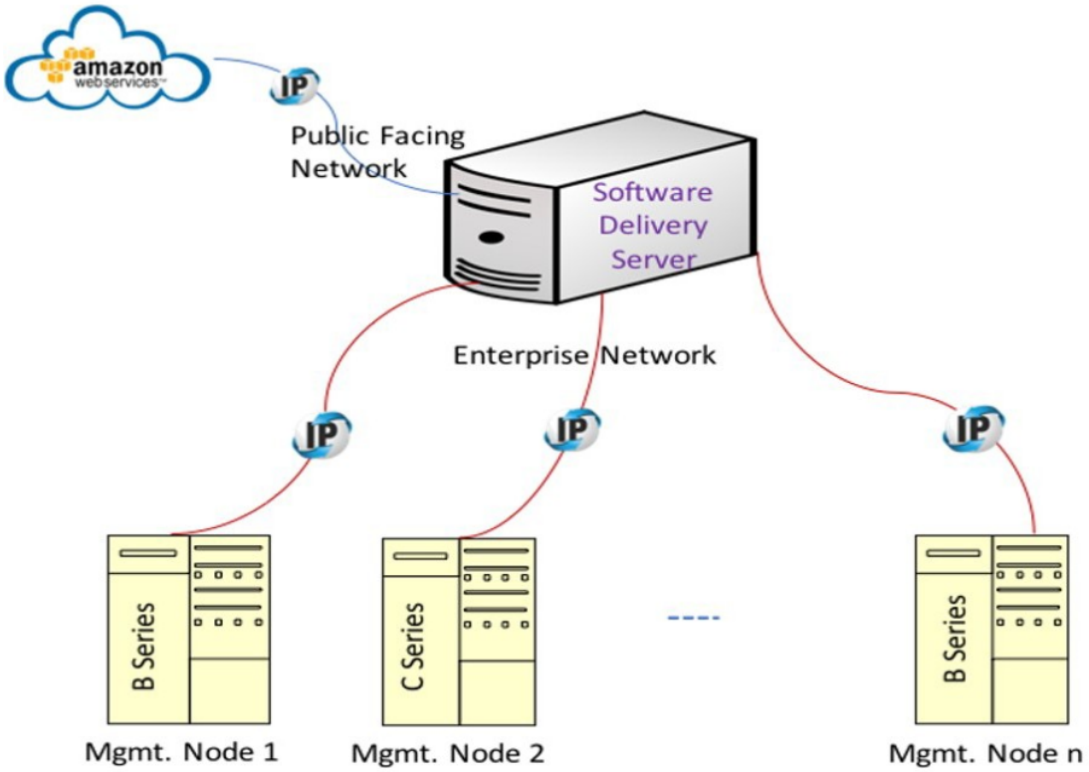
Variables	Usage	Valid range	Default
Q	Cores reserved for Control role (aio and edge)	2 to 12	2
C	Cores reserved for CEPH (aio and hc)	2 to 12	2
V	Cores reserved for VPP vswitch	2 to 6	2
Vr	RAM reserved for VPP		2GB

For OVS deployments, use V=0 and Vr=0
Some VPP deployments with high throughput requirements may require more than two VPP cores.

Software Hub

Cisco VIM Software Hub

Cisco VIM is supported in an air-gapped (disconnected mode) environment. You can use a USB or Cisco VIM Software Hub for an air-gapped install. When the number of pods is more, shipping USBs for an air-gapped install and update is not scalable. In such scenarios, we recommend that you use Cisco VIM Software Hub.
Cisco VIM Software Hub contains the Cisco VIM release artifacts such as buildnode ISO, Cisco VIM code, docker registry, and docker images. Using the management node, you can access the release artifacts from the Cisco VIM Software Hub.
You can install the artifacts available on the Cisco VIM Software Hub server through a connected or a disconnected installation procedure. For a connected installation, one end of the Cisco VIM Software Hub server is connected to the internet, while the other end is connected to the data center. The following figure shows the architecture of a connected installation.



For a disconnected installation, both interfaces are private and the artifacts are installed on the Cisco VIM Software Hub using the USB procedure. You must ensure that the ssh interface (br_api) of the management node for each Cisco VIM pod can connect to the enterprise facing interface of the Cisco VIM Software Hub server through Layer 2 or Layer 3 networking. From Cisco VIM 3.0.0 onwards, the Cisco VIM Software Hub is supported over dual-stack network. For more details on installation, see Installing Cisco VIM Software Hub

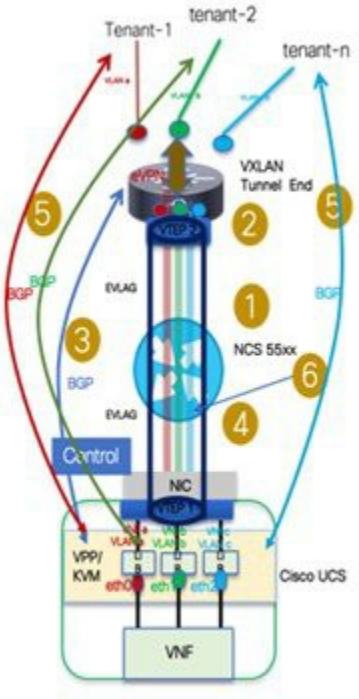
VXLAN EVPN Design

VXLAN EVPN Design

Overview

From release Cisco VIM 2.4.3 seamless connectivity from VNFs of the private cloud to the customer premise private cloud is enabled.

The architecture of the Cisco VIM Tenant L2 connectivity is shown below:

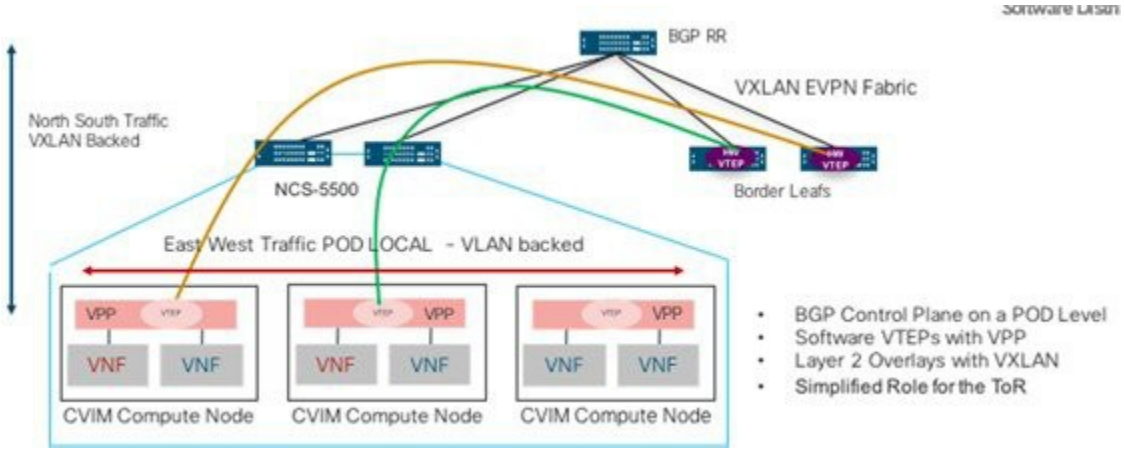


- **Segment 1: Compute to Layer 2 Aggregation (Layer 2 EVLAG)**
  - VPP will establish EVPN based EVLAG with aggregation layer
- **Segment 2: Layer 2 Aggregation switch to Fabric**
  - Fabric node will establish redundancy with aggregation layer
- **Segment 3: Infrastructure Control Plane**
  - EVPN between Compute VTEP and Remote VTEP to enable dynamic MAC learning
- **Segment 4: Infrastructure Data Plane between Compute and Tenants**
  - VXLAN will be used as a data plane for traffic transport between compute and Tenants
- **Segment 5: Overlay Control Plane Session between Private Cloud and VNF**
  - Overlay BGP session will be created between Customer private cloud and VNF
- **Segment 6: Data Traffic from/to VNF to/from Customer Private Cloud**
  - Any traffic originated from VNF or customer Private cloud will be encapsulated/decapsulated into VXLAN header
  - On Remote tunnel end, customer RI will be looked up based on received VNI in the packet
  - On Compute node VPP will determine specific VNF port based on receive VNI in the packet

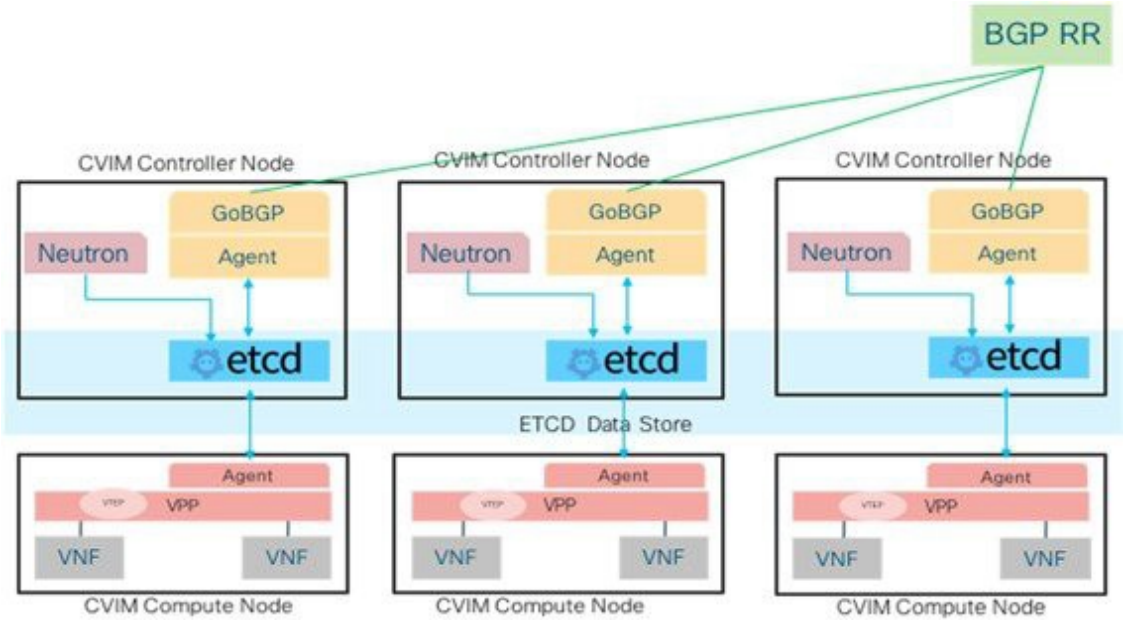
To set up Cisco VIM tenant L2 connectivity architecture, the following assumptions are made:

- OpenStack can manage VLAN allocation.
- You must manage VXLAN network and subnet for overlays, and enable OpenStack to use the EVI/VNID by creating appropriate networks /subnets in OpenStack. Cisco VIM supports VNI ranging from 1 to 65535.
- BGP configuration (peer, ASes) will be provided at the time of Cisco VIM cloud deployment through setup_data.yaml.

VXLAN tunnel is used for traffic between the VNF and customer Private cloud, while the VLAN is used for the traffic within the pod or across VNFs. EVPN is used to share L2 reachability information to the remote end, and Cisco NCS 5500 in EVLAG mode acts as a conduit for the traffic. For the VXLAN/EPVN solution to work, Cisco VIM and VXLAN tunnel peers with an external BGP route reflector to exchange IP address to Mac Binding information as shown in the below figure.

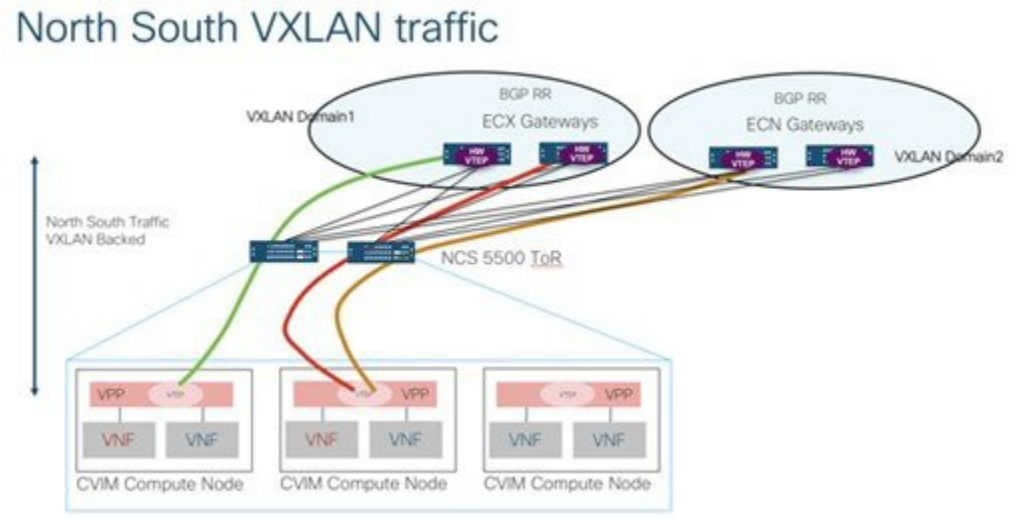


From a control plane point of view, three instances of GoBGP (in Active-Active-Active mode) run on the controller nodes to establish L3 peering with the external BGP RR for importing or exporting VxLAN routes into or from Cisco VIM respectively. The imported information is then pushed into etcd, to maintain a single source of the information within Cisco VIM.
VPP agents create and program VTEP on VPP, and also create a VXLAN tunnel interface for the VM based on the VNI information from Neutron. VPP updates VNF IP/MAC mapping in etcd, which gets exported out through EVPN to the BGP RR. The following figure shows the design of Cisco VIM VXLAN EVPN Control Plan



Multi-VXLAN EVPN Design

From release Cisco VIM 2.4.6 onwards, multiple-AS VXLAN EVPN overlay networks are supported. The following image depicts the schematic view of the multiple-AS VXLAN EVPN overlay network.



One set of VXLAN overlays manage the Cloud exchange traffic, while the other set of VXLAN overlays manage the Cloud management traffic. The multi-VXLAN (multi refers to 2) is used to conserve the number of bridge domains (BD) consumed on the Cisco NCS 5500 ToR.

From the control plane point of view, it is similar to that of a single VXLAN architecture.

The multi-VXLAN EVPN based design optionally supports a static implementation of VXLAN technology through head-end replication (HER). HER helps leverage the VXLAN technology, regardless of the hardware/software limitation in the VXLAN feature set at the remote end of the VTEP tunnel.
With the static information defined in the setup_data, VPP performs the HER to all defined remote VTEPs and updates L2FIB (MAC-IP) table based on flood and learn. If EVPN co-exists with HER, Cisco VIM treats it as if two different sets of BGP speakers exist and provides information from each speaker in the same etcd FIB table.

The only drawback of this implementation is that VPP may peform unnecessary flooding. Cisco VIM uses EVPN as the primary mechanism and HER as the fallback methodology. You can add or remove HER to or from an existing EVPN pod through Cisco VIM reconfigure option.

VPP Port Mirroring Support

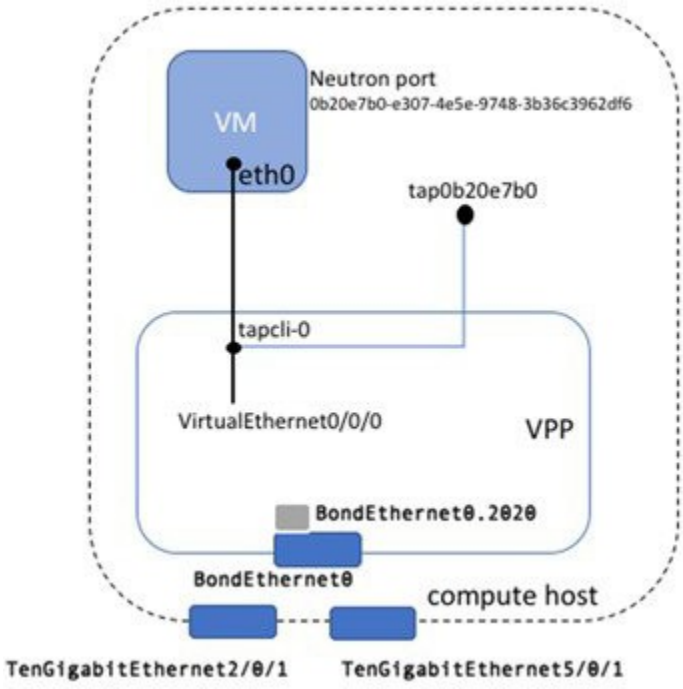
VPP Port Mirroring Support

From release Cisco VIM 2.4.3 onwards, all the network traffic between the VM and VPP is over a vhost interface which is in memory and does not use a traditional kernel side interface, when VPP is used as the vSwitch in OpenStack. The network interface is no longer on the host and available within VM, to trace packets or capture them for debugging or other administrative purposes.

Architecture

Port mirroring works by setting up the following:

1. A span port on vpp to mirror the Virtual Ethernet interface corresponding to the VMs vhost interface. This is a tap interface in VPP.
2. A tap device (tap0b20e7b0) on the compute host side is set as a kernel interface. A veth pair is created between the tap device on the VPP side (tapcli-0) and kernel side tap device (tap0b20e7b0) as shown in the below figure.



Limitations

- The port mirror feature uses tap as the interface type for the mirrored traffic. VPP may drop packets designated for this interface, under high load conditions or high traffic scenarios.
- You can only run the Port mirror CLI tools from the VPP container. This requires access to the compute node where the VM is running.
- You can only mirror the neutron ports managed by vpp-agent. This means that these have to be vhost interfaces belonging to Openstack VMs. Non Virtual Ethernet interfaces are not supported.

Segment Routing EVPN

Cisco VIM Segment Routing EVPN Design

Overview of Segment Routing EVPN

An important aspect of any Telco cloud is how the cloud is connected to the rest of the service provider network. Due to the evolution of the existing VPP-based standard VLAN and VXLAN EVPN designs, it is possible to connect Cisco VIM with an existing Segment Routing (SR) Ethernet VPN (EVPN). You can connect Cisco VIM to the SR EVPN without an additional SDN controller, by peering with EVPN route reflectors and ToR with BGP Labeled Unicast (BGP-LU). There is no contention with any controller that manages the EVPN. MPLS is used as the data plane for the SR-labelled traffic.

To connect a Cisco VIM pod to an SR EVPN, the existing VPP forwarding architecture is enhanced.

Overview of Cisco VIM VPP Architecture

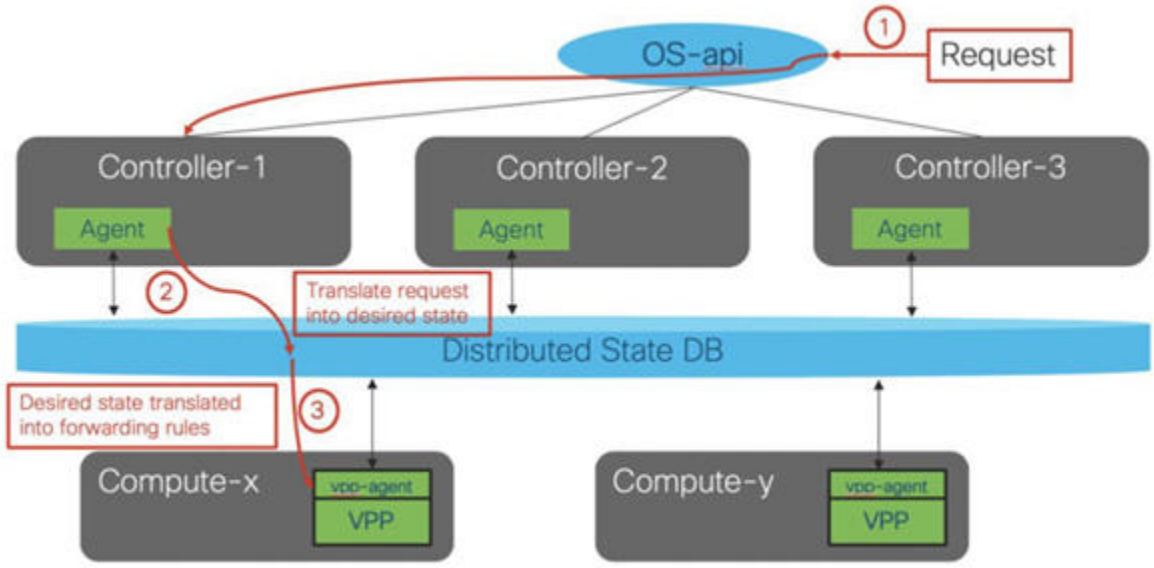
Networking-vpp is the Vector Packet Processing (VPP) based software accelerated virtual switch that is part of Cisco VIM. The architecture of networking-vpp is similar to a distributed SDN controller. However, it is not a separate controller and is integrated with Cisco VIM as a core component. Networking-vpp makes installation, updates and operational Day 2 tasks seamlessly.

Networking-vpp uses a publish and subscribe model to configure the virtual switches running on each compute node. The controllers translate any requests to the OpenStack API into the desired forwarding behavior of the VPP forwarders, and publish that information into the distributed state database. The VPP agents that run on each compute node monitor the distributed state database and program according to the desired state that is published in the distributed state database.
The controllers do not have to:

- Push configuration directly to the compute nodes.
- Validate the configuration.
- Continuously monitor the configuration of the compute nodes.

This behavior makes networking-vpp extremely efficient, resilient, and scalable. When a compute node restarts, it only needs to look at the distributed state database to check how it forwards traffic to and from the virtual machines running on this compute node and configure itself. All this is transparent to the controllers.

The figure below depicts the VPP architecture.



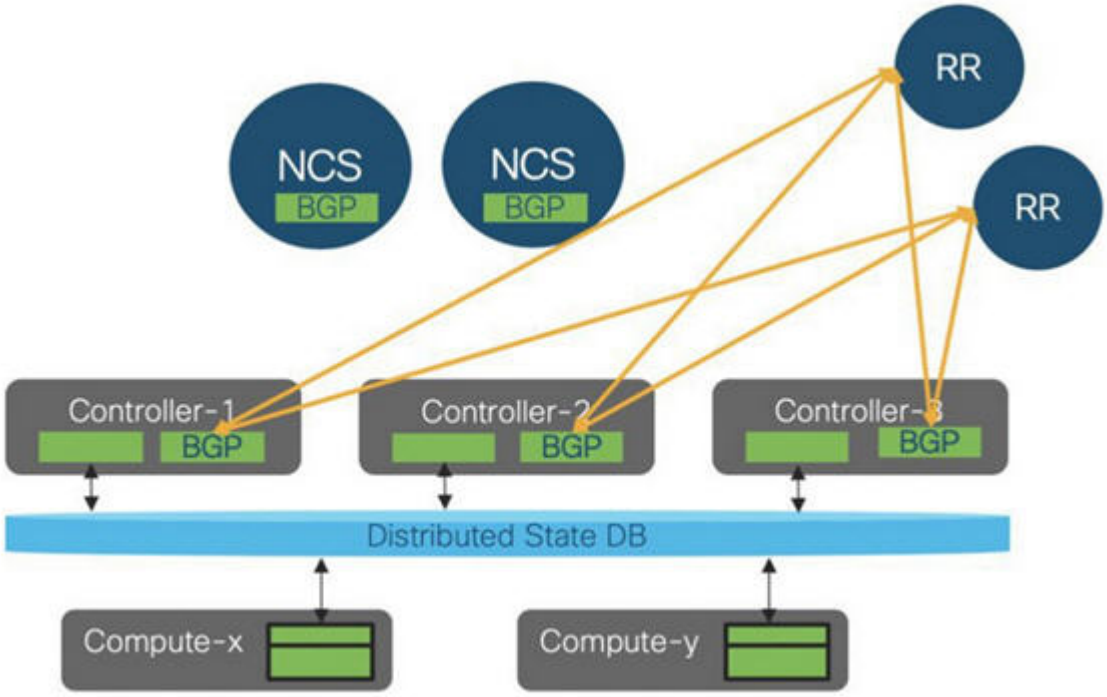
The following steps explain the figure give above:

1. The agent running on the controllers gets the incoming requests and processes the API calls that relate to the state of the network data plane forwarding.
2. The agent translates the request into the desired state of the network data plane and publishes this state into a distributed state database.
3. The vpp-agents running on the compute nodes watch the distributed state database. When they see a change relevant to the compute node, they translate the desired state and update the VPP forwarding on the compute node.

Overview of Cisco VIM SR EVPN Architecture

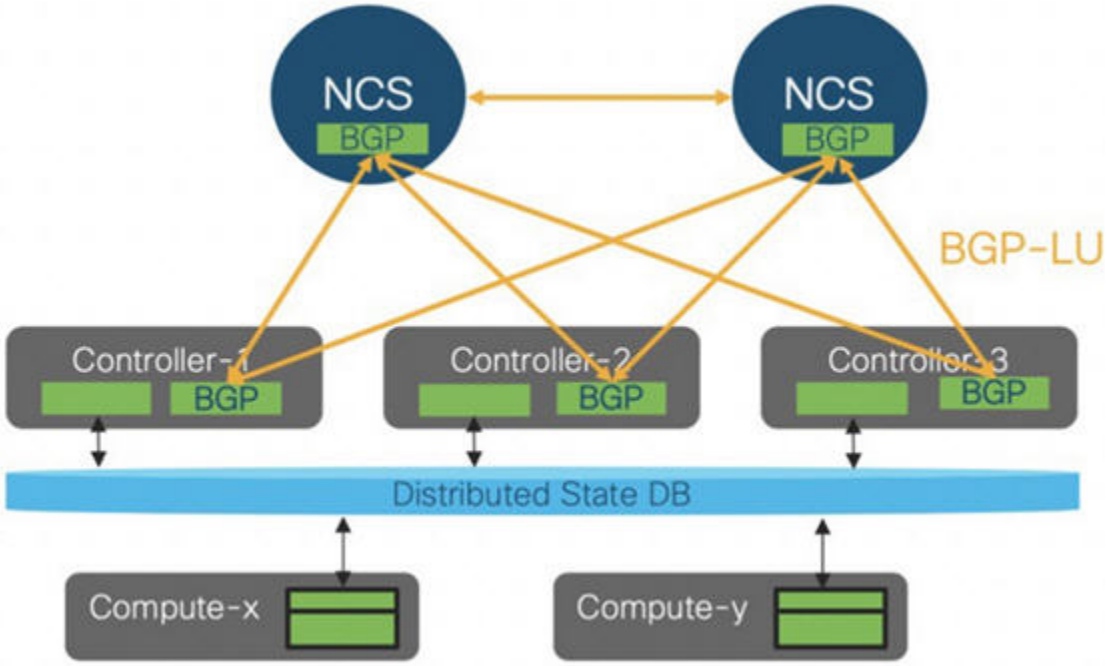
To extend the networking-vpp architecture to support Segment Routing over MPLS, Cisco VIM 3.4.1 adds several additional components.

The figure below depicts the SR EVPN RR connections.



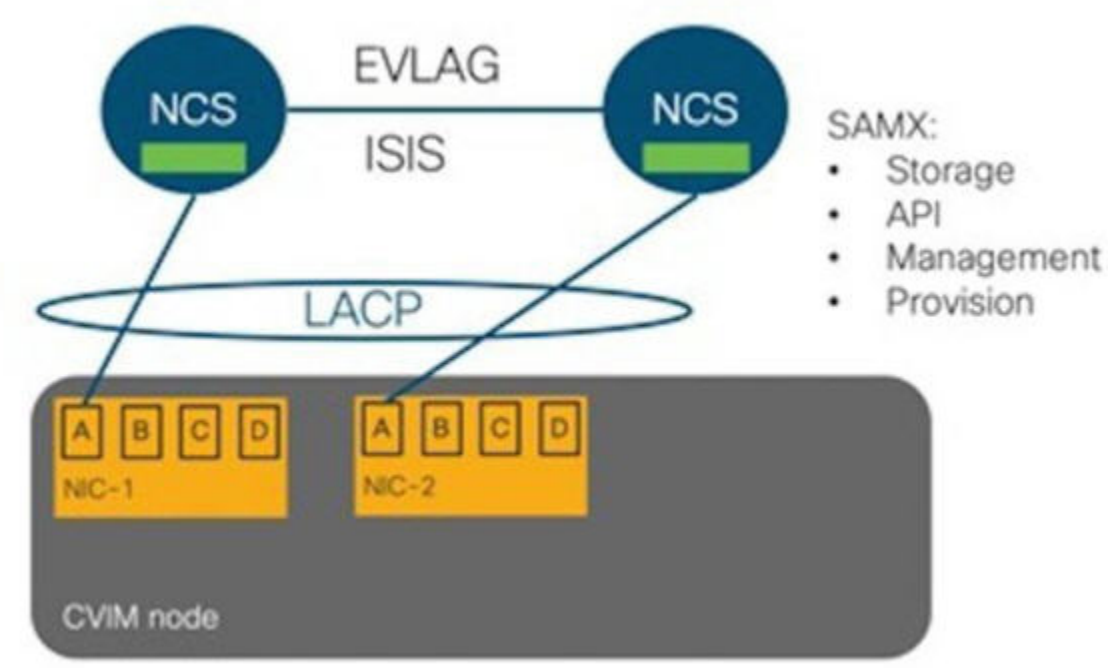
For the control plane, a BGP process runs on each of the three controller nodes. The controllers peer to the EVPN route reflectors. This peering allows the Cisco VIM pod to exchange reachability information with the EVPN. Cisco VIM does an L2 stretch with only single-homed L2 routes. The peering with the route reflectors allows Cisco VIM to exchange Type-2 routes that have MAC to IP bindings. Type-3 route updates are exchanged to handle broadcast, unknown unicast and multicast (BUM) traffic. There are unidirectional MPLS tunnels in both directions.
In addition to the BGP peering with the EVPN route reflectors, the controllers have a BGP Labeled Unicast (BGP-LU) peering with the NCS ToRs to exchange label information.

The figure below depicts the SR EVPN BGP-LU peering with the ToR.



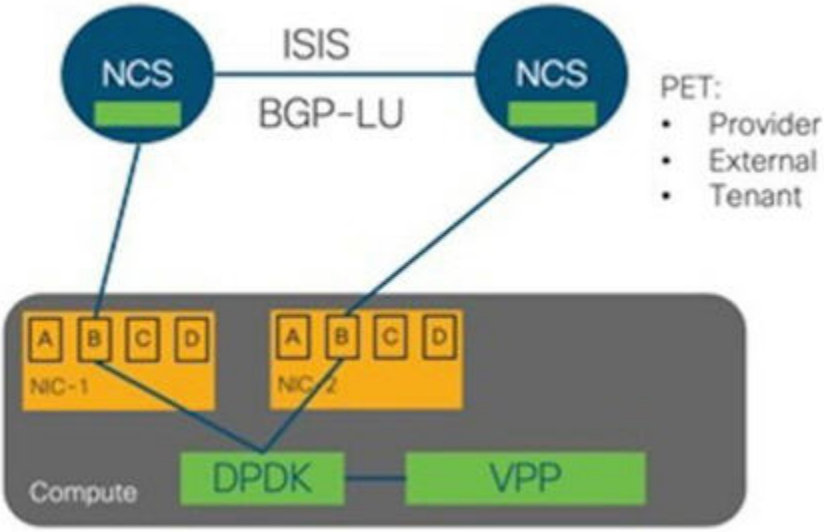
Cisco VIM does not process any SR policies coming from BGP or an SDN controller to program any explicit static or dynamic paths into VPP. BGP-LU and EVPN address family routes are processed by the BGP process running on each of the controllers. The BGP process publishes the SR policy into the distributed state database so that the VPP agents can configure VPP forwarding on the compute nodes to apply the MPLS label to the outbound traffic. The label between the compute node and the NCS ToR represents the path to node SID that identifies the VPP node. Bridge domain is identified by the Openstack Segmentation ID that is used for tenant isolation.
The data plane ports in the Cisco VIM pod are connected to the NCS with an L3 link and EVLAG provides link redundancy to the nodes. The VPP agents encapsulate the traffic leaving the compute node with an MPLS label representing the Segment Routing segment ID. The virtual machines are unaware that traffic will be sent over an SR-enabled network. For traffic arriving on the compute node from the NCS, the MPLS label represents the bridge domain, and the resulting L2 lookup determines the virtual machine to which to forward the traffic after stripping the MPLS header.

The figure below depicts the control plane port connectivity.



The control plane ports on the Cisco VIM nodes have two uplinks, one to each NCS. From the node, the two ports are bundled in a port-channel using the linux teaming driver. ISIS runs on the NCS and provides link redundancy between the two ToRs using EVLAG. The control plane ports carry any or all of the following networks: storage network to access the CEPH cluster, API network hosting the OpenStack API, Management and provision networks used at install time to provision the nodes and during Day 2 operations for management tasks.

The figure below depicts the data plane port connectivity.



The VPP backed data plane ports are configured differently. Each NIC has a port connected to one NCS. This link is a routed link with an IP address both on the NIC port in the Cisco VIM node and an IP address on the NCS port. These addresses come from a /30 subnet. ISIS runs between the NCS and BGP-LU. On the Cisco VIM nodes, ECMP load balancing occurs over the two links to the NCS. On VPP, there is a loopback interface configured that is used as the SR node SID.
Ports C and D are SR-IOV ports that give the virtual machines direct access to the NIC through the VF interfaces. These are out of scope for the SR EVPN implementation on Cisco VIM.

Container Workload

Container Workload Support

Cisco VIM supports VM, baremetal, or container-based workloads. To support the container-based workloads, Cisco VIM hosts Cisco Container Platform as an application. The orchestrator creates a common OpenStack tenant and deploys the Cisco Container Platform control plane on it. The orchestrator can also create a tenant cluster if needed.
The Kubernetes clusters deployed are multi-master clusters with three master nodes and N worker nodes. The Cisco Container Platform control plane consists of three masters and three workers. The master and worker nodes run as VMs on OpenStack.
For more information on enabling Cisco Container Platform over Cisco VIM, see Container Support

Traffic Monitoring with Open vSwitch

Traffic Monitoring with Open vSwitch

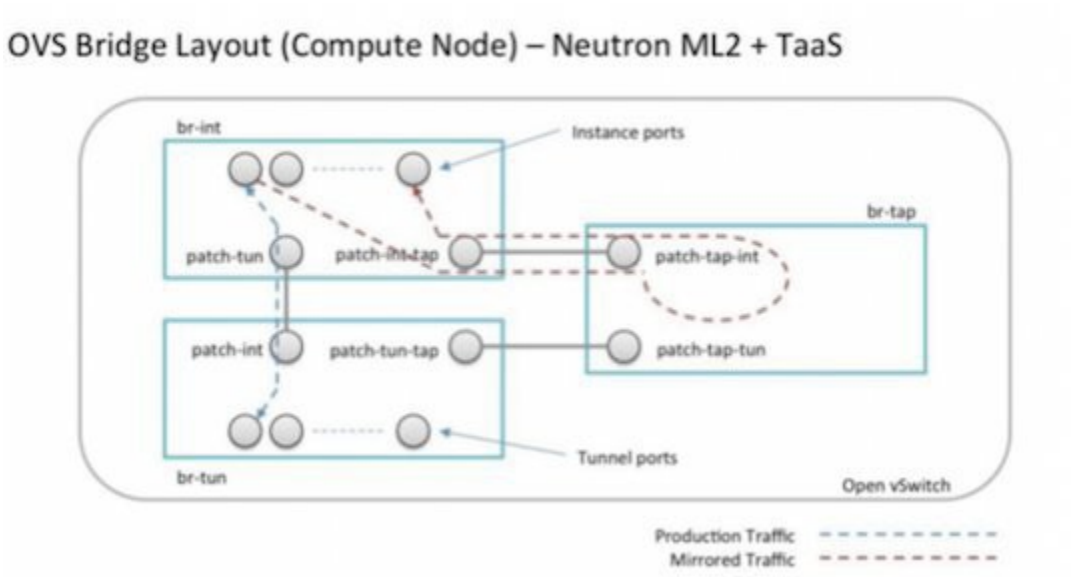
Cisco VIM supports Tap As a Server (TAAS) with Open vSwitch (OVS) as the mechanism driver.
Tap-as-a-Service (TaaS) is an extension of the OpenStack network service (Neutron). It provides remote port mirroring for tenant virtual networks. Port mirroring involves sending a copy of all packets of one port to another port.

The TAAS implementation has two parts:

1. Tap-service: Represents the neutron port that receives the mirrored traffic (mirror destination). Tap service creation mirrors the VLAN allocation from an available pool and installs flow rules into the OVS tables.
2. Tap-flow: Represents the neutron port from which the traffic needs to be mirrored (mirror source). It determines the location from where traffic should be copied and the direction to which it should be forwarded.

Tap-flow creation initiates flow rules to copy the mirror source traffic to a VLAN associated with a tap-service. All mirrored traffic is redirected from br-int to br-tap with a specific mirror VLAN number (VLAN pool is preallocated in a configuration). Depending upon the mirror destination location, traffic is redirected back to the br-int (if the destination is on the same compute) or to br-tun (if the destination is on a different compute). If traffic is redirected to br-tun it sends traffic towards the compute node where the mirror destination is located using GRE encapsulation. br-tap is an intermediate point where specific mirrored traffic is filtered towards the mirror destination.

The figure below depicts the layout for the TAAS networking diagram with OVS as the mechanism driver.



Following are the assumptions:

1. Filtering of specific traffic is not supported.
2. TaaS is used for debugging and not for mirroring production traffic as it affects OVS performance.
3. If ovs_vswitch container restarts or a compute node reloads, all tap services and tap flows have to be recreated.
4. Tap-flow and Tap-service can be created only for existing neutron ports, that is the corresponding VMs must be in running state. If the neutron ports point to a remote traffic destination, the remote ports will stay in down state.
5. Tap-flow with the same source mirror port cannot be used with different tap-services.

For information on setting up remote and local TaaS OVS, see TAAS Support.

Management Node Centralization

Management Node Centralization

Overview

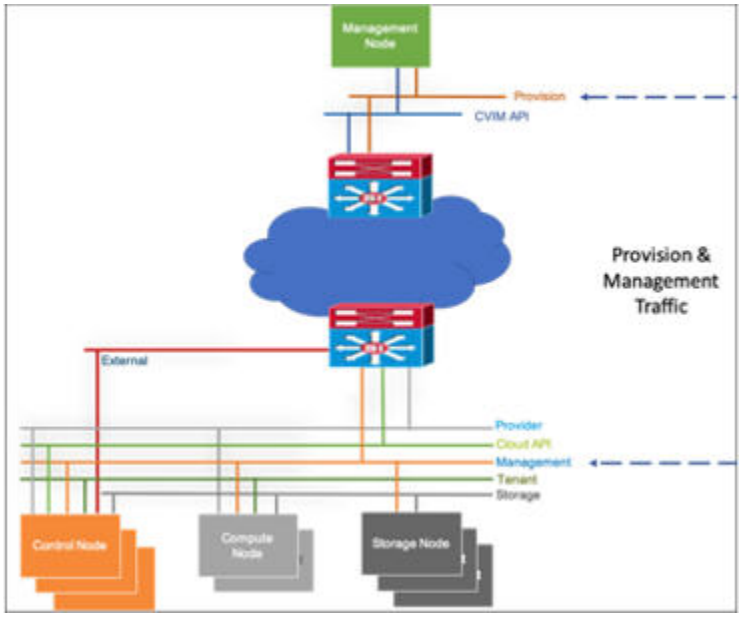
As dedicated management node is available for each pod, an additional cost of a server is involved from space, power, and capital expenditure point of view. As the cloud is moving to the edge, justifying the cost of a server on a per cloud basis becomes challenging. Hence, it is important that Cisco VIM evolves as a platform to support centralization of the management node. To support centralization, the management node is virtualized into a VM, which is then shipped as a QCOW2 image as part of the release.

Terminology Used

- Management node VM - A VM managing a pod.
- Management node - A baremetal managing a pod.
- Cisco VIM management pod - A pod hosting management node VMs. It can be a shared pod with other workloads.
- Locally managed pod - A pod that is managed by a local management node.
- Remotely managed pod - A pod that is managed remotely by a management node.

Architecture

The management node VM is Layer 3 adjacent to the pod as depicted in the figure below:



To support the architecture of management node centralization, the following prerequisites must be met:

- The cloud management network is routable from the management node VM.
- The management node VM must have access to BMC/CIMC.
- The pod servers must support remote-presence or equivalent tool, for example, VMCLI for Quanta.
- Solution uses iPXE to fetch kernel, initrd, and kickstart over httpd.

For detailed information and usage, see Centralizing Management Node

Installation

Installation

Cisco NFVI Installation Overview

Cisco NFVI Installation Overview

Cisco NFVI installation is divided into two processes:

- Preparation—Preparing the Cisco NFVI pod hardware and configuring all supporting applications including Cisco Integrated Management Controller (IMC) and Cisco UCS Manager.
- Installation—Installing the Cisco NFVI component applications such as Cisco Virtualized Infrastructure Manager (VIM), Cisco Insight (Unified Management), and Cisco Virtual Topology System (VTS) with Virtual Topology Forwarder (VTF) based on your Cisco NFVI package.

Cisco NFVI installation depends on the component applications that you install. For example, if you are installing Cisco VTS, install VTC before installing Cisco VIM or Cisco Unified Management (UM). When installing Cisco VIM UM, install the Cisco VIM management node and Insight in a sequence to complete the Cisco VIM installation through Cisco VIM UM. However, if you have Cisco VIM without other Cisco NFVI applications in your package, you can install the Cisco VIM alone in your system.
Consider the following factors before installing the Cisco NFVI components:

- **Internet Access**: Internet access is required to download the Cisco NFVI installation files from cvim-registry.com. If you do not have an Internet access to your management node, you need an alternate server with an Internet access to download the installation files to a USB stick. You can copy the installation files from USB stick to the management node.
- **Cisco NFVI Configurations**: Cisco NFVI configurations are included in the setup_data.yaml file. If you are installing Cisco VIM and not Cisco VIM Insight, you can enter the configurations directly into the setup_data.yaml file with a yaml editor. You can refer to the examples in setup_data file (for C and B-series) at the openstack-configs directory in the target install folder in the management node. For more information on Cisco NFVI data and OpenStack parameters, see OpenStack Configuration. If you are installing Cisco VIM Insight, run Cisco NFVI using Insight UI wizard. For more information, see Unified Management.

Following are the license options for installing Cisco NFVI:

- Cisco NFVI Basic—Includes Cisco Virtual Infrastructure Manager (VIM), which is an OpenStack Queens release software solution used to enhance the functionality, scale, and performance of the node.
- Cisco NFVI Standard—Includes Cisco VIM and Cisco VIM Insight. Cisco VIM Insight deploys, provisions, and manages Cisco NFVI on Cisco UCS servers.
- Cisco NFVI with third-party monitoring - Includes Cisco VIM with or without Cisco VIM Insight based on the license option chosen, with monitoring of the pod through Zenoss.
- Optional Cisco NFVI Applications—Cisco Virtual Topology System (VTS) is an optional application that can be installed with both Cisco VIM and Cisco VIM Insight. Cisco VTS is a standard-based, open software-overlay management and provisioning system. It automates the data center network fabric provisioning, for virtual and physical infrastructure.

You must perform extra manual installation procedures while installing Cisco VIM. If your package includes Cisco VIM and UM, you must do Cisco VIM manual setup and configuration procedures through the Unified management system (UM). You can manage cloud in Cisco VIM through Cisco VIM UM. Once you start managing the cloud, Cisco recommends you to continue using Cisco VIM UM for future use as well.

Installation Preparation Without Internet Access

Preparing for Installation on Servers Without Internet Access

Air-gapped Installation Approach

Approaches for Air-Gapped Installation

Listed below are the two approaches for air-gapped installation in Cisco VIM.

- Approach 1: Getting the artifacts onto USB from a staging server running CentOS/RHEL 7.6
- Approach 2: Creating a file based image on the staging server running CentOS/RHEL 7.6

For both the approaches, the staging server is connected to the docker registry.

In the first approach, you can do the installation independently post preparation of the USB. However, it involves an additional burden of shipping the physical USBs to each pod, which may be cumbersome. In the second approach of file based image, the burden associated with first approach is reduced. However, each management node must be connected to the staging server.

Prerequisites for Air-Gapped Installation

Prerequisites for Air-Gapped Installation

Prerequisites for Air-gapped Installation via USB

1. Download the Cisco NFVI installation files to a 64GB (minimum) USB 2.0 drive on a staging server with Internet access. If the management node is based on M5 or a Quanta server, you can optionally use USB 3.0 64GB to increase the installation speed significantly.
2. Copy the files to the management node.

Prerequisites for Air-gapped Installation via File-based image

1. The CentOS/RHEL 7.6 staging server (VM, laptop, or UCS server) is connected to the docker registry.
2. Each management node must be connected to this staging server.
3. Ensure that the packages truncate and parted with kpartx installed on the CentOS/RHEL 7.6 staging server.

NFVI Installation Setup via USB

NFVI Installation Setup via USB

Following procedure describes how to download the Cisco NFVI installation files onto a USB drive of the staging server with Internet access. You can use the USB to load the Cisco NFVI installation files onto the management node without Internet access.

Cisco recommends to use Virtual Network Computing (VNC), other terminal multiplexers, or similar screen sessions to complete these steps.

Before you begin

You must have a CentOS 7 staging server (VM, laptop, or UCS server) with a 64 GB USB 2.0 drive only. You can use USB 3.0 64GB if the management node is of type M5. The staging server must have wired Internet connection to download the Cisco VIM installation files onto the USB drive. Once downloaded, you can copy the installation files onto the management node from USB drive.

Downloading of the installation files (over 25 GB in size) to the USB drive might take several hours depending on the speed of your Internet connection. Ensure that you disable the CentOS to the sleep mode, for faster installation.

1. On the staging server, use yum to install the following packages:

   - PyYAML (yum install PyYAML)
   - python-requests (yum install python-requests)
   - Python 3.6 (yum install rh-python36)

   Check if python 3.6 binary is located at */opt/rh/rh-python36/root/bin/,* if not copy the python 3.6 binary to */opt/rh/rh-python36/root/bin/.*
2. Log into Cisco VIM software download site and download the *getartifacts.py* script from external registry:

```
# download the new getartifacts.py file (see example below)
curl -o getartifacts.py
https://username:password@cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/2.4.4
/getartifacts.py

# Change the permission of getartifacts.py
chmod +x getartifacts.py
```

3. Run *getartifacts.py*. The script formats the USB 2.0 drive (or USB 3.0 drive for M5/Quanta based management node) and downloads the installation files. You must provide the registry username and password, tag ID, and USB partition on the staging server.

```
./getartifacts.py -h
usage: getartifacts.py [-h] -t TAG -u USERNAME -p PASSWORD [--proxy PROXY]
                       [--retry] (-d DRIVE | -f FILE)
                       [--mgmtk8s | --argus | --insight | --sds | -U]

Script to pull container images en masse.

optional arguments:
  -h, --help            show this help message and exit
  -t TAG, --tag TAG     Installer version to pull
  -u USERNAME, --username USERNAME
                        Registry username
  -p PASSWORD, --password PASSWORD
                        Registry password
  --proxy PROXY         https_proxy if needed
  --retry               Try to complete a previous fetch
  -d DRIVE, --drive DRIVE
                        Provide usb drive path
  -f FILE, --file FILE  location of image file
  --mgmtk8s             Additionally download CVIM MON HA artifacts
  --argus               Additionally download argus artifacts
  --insight             Additionally download insight artifacts
  --sds                 Additionally download sds artifacts
  -U, --upgrade         Additionally download artifacts for upgrade from 2.4.x

This script pulls images from remote registry then copies the contents to USB
drive or image file based on the user supplied option
```

4. To identify the USB drive, execute the *lsblk* command before and after inserting the USB drive. The command displays a list of available block devices. The output data helps you to find the USB drive location. Provide the entire drive path in the *–d* option instead of any partition as shown below. Here, the tag_id refers to the Cisco VIM release version 3.4.x.

   For example:

   ```
   sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> \[--proxy proxy.example.
   com\] -
   ```

   ⚠ Ensure that you do not remove the USB drive during synchronization.

   ⚠ On executing *getartifacts.py*, the following message appears to notify bad superblock and mount failure. In this case, reformat the drive and use the *fsck* command to recover the drive: *fsck.ext4-pv/dev/sdc1* .
   stderr:mount:wrongfstype,badoption,badsuperblock on /dev/sdc1, missing codepage or helper program, or other error.

   ⚠ As the size of the artifacts is greater than 25G, it is recommended to execute this step over a wired internet connection. It takes few hours to download and populate data on the USB drive, depending on internet connectivity.

   The *getartifacts.py* script downloads the following:

   a. Core Packages

      - buildnode-K9.iso
      - buildnode-K9.qcow2
      - mercury-installer.tar.gz
      - ironic-images-K9.tar.gz
      - registry-2.6.2.tar.gz
      - docker images and manifests
      - python-docker-py-1.10.6-4.el7.noarch.rpm
      - python-docker-pycreds-1.10.6-4.el7.noarch.rpm
      - python-websocket-client-0.32.0-116.el7.noarch.rpm
      - vim_upgrade_orchestrator.py

        ⚠ For upgrade, the python-docker-py-1.10.6-4.el7.noarch.rpm, python-docker-pycreds-1.10.6-4.el7.noarch.rpm, python-websocket-client-0.32.0-116.el7.noarch.rpm, and vim_upgrade_orchestrator.py packages are required.

b. Respective checksums

- all_check_sum_file.sign.tar.gz

5. Use the following command to verify the downloaded artifacts and container images:

```
# create a directory
sudo mkdir -p /mnt/Cisco

# /dev/sdc is the USB drive, same as supplied in getartifacts.py python script

#You need to mount the partition with the steps given below:
sudo mount /dev/sdc1 /mnt/Cisco
cd /mnt/Cisco

# execute the test-usb help to look at the options
./test-usb -h

usage: ./test-usb [-h] -- Show this program to check integrity of artifacts in this USB drive/image file
                  [-a] -- Check integrity of all (core and all) artifacts in this USB drive/image File
                  [-l] -- Location of artifacts
                  [-f] -- Location of image file
                  [-U] -- test upgrade artifacts from 2.4.x to 3.4.y
# execute the verification script
./test-usb

# failures will be explicitly displayed on screen, sample success output below# sample output of ./test-
usb with 3.4.1 release
#./test-usb
           INFO: Checking the integrity of artifacts on this USB drive
           INFO: Checking artifact python-docker-py-1.10.6-4.el7.noarch.rpm
           INFO: Checking artifact python-docker-pycreds-1.10.6-4.el7.noarch.rpm
           INFO: Checking artifact python-websocket-client-0.32.0-116.el7.noarch.rpm
           INFO: Checking artifact vim_upgrade_orchestrator.py
           INFO: Checking artifact mercury-installer.tar.gz
           INFO: Checking artifact ironic-images-K9.tar.gz
                   INFO: Checking artifact buildnode-K9.iso
           INFO: Checking artifact buildnode-K9.qcow2
                   INFO: Checking artifact registry-2.6.2.tar.gz
                   INFO: Checking required layers:
           INFO: 764 layer files passed checksum.

# ./test-usb -a
           INFO: Checking the integrity of artifacts on this USB drive
           INFO: Checking artifact python-docker-py-1.10.6-4.el7.noarch.rpm
           INFO: Checking artifact python-docker-pycreds-1.10.6-4.el7.noarch.rpm
           INFO: Checking artifact python-websocket-client-0.32.0-116.el7.noarch.rpm
           INFO: Checking artifact vim_upgrade_orchestrator.py
           INFO: Checking artifact mercury-installer.tar.gz
           INFO: Checking artifact ironic-images-K9.tar.gz
                   INFO: Checking artifact buildnode-K9.iso
           INFO: Checking artifact builnode-K9.qcow2
                   INFO: Checking artifact registry-2.6.2.tar.gz
                   INFO: Checking artifact mariadb-app-K9.tar.gz
                   INFO: Checking artifact insight-K9.tar.gz
                   INFO: Checking required layers:
           INFO: 764 layer files passed checksum.
```

If the download fails, an error message is displayed.

For example:

```
# ./test-usb
INFO: Checking the integrity of this USB stick
INFO: Checking artifact buildnode-K9.iso
ERROR: Checksum for artifact buildnode-K9.iso does not match ('SHA512 (buildnode-K9.iso) =
96ec62a0932a0d69daf60acc6b8af2dc4e5eca132cd3781fc17a494592feb52a7f171eda25e59c0d326fbb09194eeda66036cbdc3
870dafe74f59cf1f2dce225'
!= 'SHA512 (buildnode-K9.iso) =
a6a9e79fa08254e720a80868555679baeea2dd8f26a0360ad47540eda831617bea0514a117b12ee5f36415b7540afa112a1c904cd
69e40d704a8f25d78867acf')
INFO: Checking artifact registry-2.3.1.tar.gz
ERROR: Artifact registry-2.3.1.tar.gz is not present
INFO: Checking required layers:
ERROR: Layer file sha256:002aa1f0fbdaea7ea25da1d906e732fe9a9b7458d45f8ef7216d1b4314e05207 has a bad
checksum
ERROR: Layer file sha256:5be3293a81773938cdb18f7174bf595fe7323fdc018c715914ad41434d995799 has a bad
checksum
ERROR: Layer file sha256:8009d9e798d9acea2d5a3005be39bcbfe77b9a928e8d6c84374768ed19c97059 has a bad
checksum
ERROR: Layer file sha256:ea55b2fc29b95d835d16d7eeac42fa82f17e985161ca94a0f61846defff1a9c8 has a bad
checksum
INFO: 544 layer files passed checksum.
```

6. To resolve download artifact failures, unmount the USB and run the *getartifacts* command again with the *--retry* option.

```
sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> --retry
```

7. Mount the USB and then run the test-usb command to validate if all the files are downloaded:

```
# /dev/sdc is the USB drive, same as supplied in get artifacts.py python script
sudo mount /dev/sda1 /mnt/Cisco
cd /mnt/Cisco
# execute the verification script
./test-usb
# In case of failures the out of the above command will explicitly display the same on the screen
```

8. When the USB integrity test is done, unmount the USB drive by running the following command:

```
sudo unmount /mnt/Cisco
```

NFVI Installation File-Based Image

NFVI Installation via File-Based Image

Installation Overview

To download Cisco VIM artifacts for disconnected installation, an image file based option is available for deployments where shipping of physical USB is not feasible for an air-gapped installation.

> **Before you begin**
>
> You must have a CentOS/RHEL 7.6 staging server (VM, laptop, or UCS server) that is connected to the docker registry. Also, each management node must be connected to this staging server.

Download the Cisco VIM artifacts to a file-based image on the staging server (running CentOS/RHEL 7.6) that is connected to the docker registry. Once the artifacts are downloaded, copy the corresponding file-based image to the management node and subsequently import the respective artifacts to the management node. You can apply the same method of importing the artifacts for an update or upgrade procedure if desired.

Assumption

- This feature is effective starting Cisco VIM 3.4.3, and can only be used for fresh installation of Cisco VIM 3.4.3 and/or update from Cisco VIM 3.4.x lineup.
- In the *setup_data.yaml,* INSTALL_MODE must be set to *disconnected.*

Prerequisites

Ensure that the packages truncate and gets parted with *kpartx* installed on the CentOS/RHEL 7.6 staging server, that is connected to the docker registry.

Procedure

Following are the steps that outline the process:

1. To download artifacts to file-based image (which is approximately 60GB in size), log into Cisco VIM software download site and download the*getartifacts.py* script from external registry onto the staging server:

```
curl -o getartifacts.py https://username:password@cvim-registry.com/mercury-releases/cvim34-rhel7-osp13
/releases/<releaseid>/getartifacts.py
# Change the permission of getartificats.py
chmod +x getartifacts.py
```

2. On the staging server, execute the *getartifacts.py* script with the *--file* option to download the correct target artifacts:

```
#./getartifacts.py -u <username> -p  <password> -t <release-tag> --file /dir/path/to/file --proxy PROXY
Example of the execution
# ./getartifacts.py -u installer -p  password -t 3.4.3 --file /var/artifacts-3-4-3.img
```

> As this process cannot be aborted in the middle, it is recommended to use either a VNC session/screen/KVM or serial console.

For upgrade from 2.4.x (x = 15, 16, 17, or 18) to 3.4.3, the above command gets appended with *-U* or *--upgrade:*

```
#./getartifacts.py -u <username> -p  <password> -t <release-tag> --file /dir/path/to/file --proxy PROXY -
U
```

⚠ To download additional target artifacts, check the help option of getartifacts.py,

3. On the staging server, verify the integrity and consistency of the downloaded artifacts in the file-based image:

```
 # curl -o mercury-installer.tar.gz https://username:password@cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/<releaseid>/mercury-installer.tar.gz
 # tar --no-same-owner -xvzf mercury-installer.tar.gz
 # cd installer-3.4.3/tools/
 # ./test-usb -f /var/artifacts-3-4-3.img
```

4. Copy the file-based image */var/artifacts-3-4-3.img* from the staging server to */var/* of the target management node:

```
 # scp /var/artifacts-3-4-3.img root@<management-node-ip>:/var/

Repeat the test-usb on the management node (from the installer-xxx/tools work space) for consistency check
# cd installer-3.4.3/tools/
# ./test-usb -f /var/artifacts-3-4-3.img
Execution Snippet:
/test-usb -f /var/artifacts.img
INFO: Checking the integrity of artifacts on this Image file
INFO: Checking artifact python-docker-py-1.10.6-4.el7.noarch.rpm
INFO: Checking artifact python-docker-pycreds-1.10.6-4.el7.noarch.rpm
INFO: Checking artifact python-websocket-client-0.32.0-116.el7.noarch.rpm
INFO: Checking artifact vim_upgrade_orchestrator.py
INFO: Checking artifact mercury-installer-internal.tar.gz
INFO: Checking artifact ironic-images-internal.tar.gz
INFO: Checking artifact buildnode-internal-24641.iso
INFO: Checking artifact registry-2.6.2-internal-24641.tar.gz
INFO: Checking artifact buildnode-internal-24641.qcow2
INFO: Checking required layers:
INFO: 782 layer files passed checksum
```

5. To import the artifacts onto the management node., execute *import_artifacts.sh* with *-f* option on the management node, and provide the location of the file-based image:

```
# cd /root/installer-3.4.3/tools/
#  ./import_artifacts.sh -f /var/artifacts-3-4-3.img
#  ./import_artifacts.sh -h
import_artifacts.sh  : Program to import artifacts from USB
---------------------------------
usage: ./import_artifacts.sh
-s              : Specify this flag is importing on SDS server
-f              : Specify this flag along with image file location as a argument to import artifacts
-h              : To display this help
```

Preparing for Cisco NFVI Installation

Preparing for Cisco NFVI Installation

Cisco NFVI Hardware Installation

Cisco NFVI Hardware Installation

Switch on the Cisco UCS C-Series or B-Series hardware, before you install the Cisco VIM. Depending upon the pod type, you need to set up the CIMC connection or UCSM IP ahead of time.The following table lists the UCS hardware options and network connectivity protocol used with virtual extensible LAN (VXLAN) over a Linux bridge, VLAN over OVS or VLAN over VPP. If Cisco VTS, an optional Cisco NFVI application, is installed, Virtual Topology Forwarder (VTF) is used with VXLAN for tenants and VLANs for providers on C-Series pods.

UCS Pod Type	Compute and Controller Node	Storage Node	Network Connectivity Protocol
Rack Type	UCS C220/240 M4/M5	UCS C240 M4 (SFF) with two internal SSDs	OVS/VLAN or VPP/VLAN (only on intel NIC) or ACI /VLAN
Rack Type	Controller: UCS C220/240 Compute: HP DL360 Gen9 Quanta servers for Fullon or Edge pod	UCS C240 M4 (SFF) with two internal SSDs	OVS/VLAN
C-Series with Cisco VTS	UCS C220/240 M4	UCS C240 M4 (SFF) with two internal SSDs	For tenants: VTF with VXLAN. For providers: VLAN
C-Series Micropod	• UCS 240 M4/M5 with 12 HDD and 2 external SSDs. Pod can be expanded to 16 computes. Each compute contains 2x1.2 TB HDD or • UCS 220 M4/M5 with 6 HDD and 1 external SSDs. Pod can be expanded to 16 computes. Each compute contains 2x1.2 TB HDD. ⚠ Refer to the BOM for SSD based install for M5. M5 BOM is based on Intel X710 for control and data plane and XL710 for SRIOV. For exact BOM details, reach out to Cisco VIM product marketing.	Not applicable as it is integrated with Compute and Controller.	OVS/VLAN or VPP/VLAN (on intel NIC).
C-Series Hyperconverged	UCS 240 M4/M5.	UCS C240 M4/M5 (SFF) with 10 HDD and two external SSDs, acts as compute node	OVS/VLAN
B-Series	UCS B200 M4.	UCS C240 M4 (SFF) with two internal SSDs.	OVS/VLAN.

The storage nodes boot off two internal SSDs. It also has four external SSDs for journaling, which gives a 1:5 SSD-to-disk ratio (assuming a chassis filled with 20 spinning disks). Each C-Series pod has either a dual-port 10 GE Cisco vNIC 1227 card or dual-port/quad-port Intel X 710 card. UCS B-Series blade servers only support Cisco 1340 and 1380 NICs.

⚠ For more information on Cisco vNICs, see LAN and SAN Connectivity for a Cisco UCS Blade.

Cisco VIM has a Micropod (based on UCS-M4/M5 hardware) which works on Cisco VIC 1227 or Intel NIC 710, with OVS/VLAN or VPP/VLAN (for Intel NIC only) as the virtual network protocol. The Micropod supports with a small, functional, but redundant cloud with capability of adding standalone computes (maximum of 16) to an existing pod.

Cisco VIM supports M4/M5-based Micropod on a VIC/NIC system with OVS, to extend the SRIOV support on a 2x2-port Intel 520 or 2x40G XL710 NIC card. The same pod can be extended to include M5 computes having 40G Cisco VIC with an option to have 2x40G XL710 intel NIC as SRIOV.

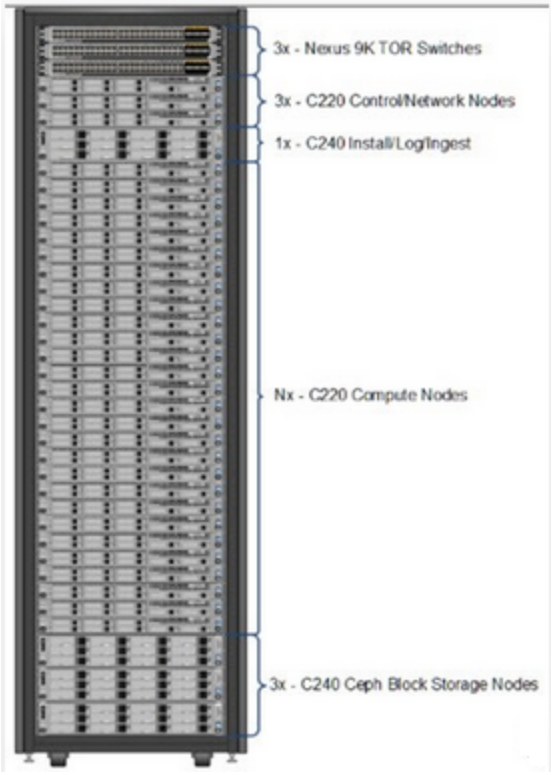
⚠ M5 can only use 2x40G XL710 for SRIOV.

The M5-based Micropod is based on Intel NIC 710 and supports SRIOV over XL710, with OVS/VLAN or VPP/VLAN as the virtual network protocol. From release Cisco VIM 2.4.2 onwards, 40G M5-based Micropod is supported on a VIC (40G)/NIC (2-XL710 for SRIOV) system.

In addition, the Cisco Nexus 9372 or 93180YC, or 9396PX is also available to serve the Cisco NFVI ToR function.
After verifying that you have required Cisco UCS servers, blades and Nexus 93xx, install the hardware following procedures at the following links:

- Cisco UCS C220 M4 Server Installation and Service Guide
- Cisco UCS C240 M4 Server Installation and Service Guide
- Cisco UCS B200 Blade Server and Installation Note
- Cisco Nexus 93180YC,9396PX, 9372PS and 9372PX-E NX-OS Mode Switches Hardware Installation

The figure below shows C-Series Cisco NFVI pod. Although the figure shows a full complement of UCS C220 compute nodes, the number of compute nodes vary depending on the implementation requirements. The UCS C220 control and compute nodes can be replaced with UCS 240 series. However, in that case the number of computes fitting in one chassis system is reduced by half. The following figure shows the Cisco NFVI C-series pod.



⚠ The combination of UCS-220 and UCS-240 within the compute and control nodes is not supported.

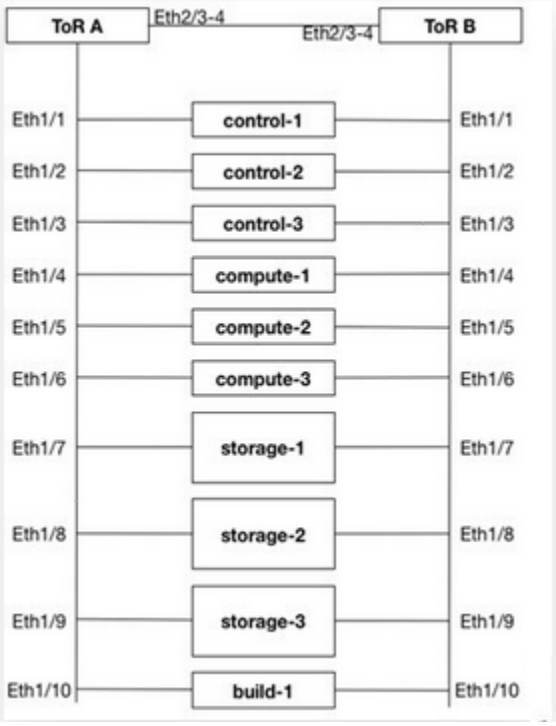
For more information on wiring schematic of various pod configuration, see Wiring Diagrams.

ToR Switch Configuration for C-Series Pods

ToR Switch Configuration for C-Series Pods

During installation, the Cisco VIM installer creates vNICs on each of the two physical interfaces and creates a bond for the UCS C-Series pod. Before this, manually configure the ToR switches to create a vPC with the two interfaces connected to each server. Use identical Cisco Nexus 9372, 93180YC, or 9396PX switches for the ToRs. Cisco recommends you to use the N9K ToR software versions for setup: 7.0(3)I4(6), 7.0(3)I6(1), 9.3(2). For information on the wiring details for each pod type on a C-series-based installation, see Wiring Diagrams.

Complete the following steps to create a vPC on a pair of Cisco Nexus ToR switches. The steps use the following topology as an example. Modify the configuration as per your environment. The following figure shows a sample ToR configuration.



Cisco VIM optionally supports the auto-configuration of ToR for N9K series only. If auto-configuration of ToR is enabled, you can skip the following steps:

1. Change the vPC domain ID for your configuration. The vPC domain ID can be a unique number. The IP address on the other switch mgmt0 port is used for the keepalive IP. Change it to the IP used for your network.

   For the preceding example, the following is the configuration:

   ```
   ToR-A (mgmt0 is 172.18.116.185)
   feature vpc
   vpc domain 116
   peer-keepalive destination 172.18.116.186
   ToR-B (mgmt0 is 172.18.116.186)
   feature vpc
   vpc domain 116
   peer-keepalive destination 172.18.116.185
   ```

   Because both switches are cabled identically, the remaining configuration is identical on both switches. In this example, topology Eth2/3 and Eth2 /4 are connected to each other and combined into a port channel that functions as the vPC peer link.

   ```
   feature lacp
   interface Ethernet2/3-4
   channel-group 116 mode active
   interface port-channel116
   switchport mode trunk
   vpc peer-link
   ```

2. For each VLAN type, (mgmt_vlan, tenant_vlan_range, storage, api, external, provider), execute the following on each ToR:

```
vlan <vlan_type> no shut
```

3. Configure all the interfaces that are connected to the servers as the members of the port channels. In the example, only ten interfaces are shown. But you must configure all interfaces that are connected to the server.

   ⚠ If interfaces have configuration from previous deployments, you can remove them by entering default interface Eth1/1-10, then no interface Po1-10.

   a. For deployment with any mechanism driver on Cisco VIC:

      There is no configuration differences among different roles (controllers/computes/storages). The same configuration applies to all interfaces.

      ```
      interface Ethernet 1/1
      channel-group 1 mode active
      interface Ethernet 1/2
      channel-group 2 mode active
      interface Ethernet 1/3
      channel-group 3 mode active
      interface Ethernet 1/4
      channel-group 4 mode active
      interface Ethernet 1/5
      channel-group 5 mode active
      interface Ethernet 1/6
      channel-group 6 mode active
      interface Ethernet 1/7
      channel-group 7 mode active
      interface Ethernet 1/8
      channel-group 8 mode active
      interface Ethernet 1/9
      channel-group 9 mode active
      interface Ethernet 1/10
      channel-group 10 mode active
      ```

   b. For deployment with OVS/VPP with VLAN on Intel NIC:

      The interface configuration is the same as the Cisco VIC as shown in the above section. However, the number of switch interfaces that are configured is more in the case of Intel NIC as it has dedicated control and data physical ports. For SRIOV switch port, no port channel is configured and the participating VLAN can be in trunk mode. In the case of pod-based on Quanta servers or HPE as computes, configure the control and data plane VLANs in trunk mode on the switch ports connected to the OCP and LOM cards, respectively.

4. Configure the port-channel interface as vPC and trunk all VLANs. For Intel NIC, you must configure native VLAN and set it to mgmt VLAN on the control ports so that PXE boot does not fail. Skip to listen or learn in spanning tree transitions, and ensure that you do not suspend the ports if LACP packets are not received. Also, configure it with a large MTU of 9216 to avoid Ceph installation failure. The last configuration allows you to start the servers before the bonding is set up.

   ```
   interface port-channel1-9
   shutdown
   spanning-tree port type edge trunk
   spanning-tree bpdufilter enable
   switchport mode trunk
   switchport trunk native vlan mgmt_vlan for the control ports when Intel NIC is used
   switchport trunk allowed vlan <mgmt_vlan, tenant_vlan_range, storage, api, external, provider>
   no lacp suspend-individual
   mtu 9216
   vpc <1-9>
   no shutdown
   ```

5. Identify the port-channel interface that connects to the management node on the ToR:

```
shutdown
spanning-tree port type edge trunk
switchport mode trunk
switchport trunk allowed vlan <mgmt_vlan>
no lacp suspend-individual
vpc 10
no shutdown
```

6. Check the port-channel summary status. The ports connected to the neighbor switch have to be in (P) state. Before the server installation, the server facing interfaces must be in (I) state. After installation, they have to be in (P) state, which means they are up and in port-channel mode.

```
gen-leaf-1# show port-channel summary
Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port- Type Protocol Member Ports
Channel
--------------------------------------------------------------------------------
1 Po1(SD) Eth LACP Eth1/1(I)
2 Po2(SD) Eth LACP Eth1/2(I)
3 Po3(SD) Eth LACP Eth1/3(I)
4 Po4(SD) Eth LACP Eth1/4(I)
5 Po5(SD) Eth LACP Eth1/5(I)
6 Po6(SD) Eth LACP Eth1/6(I)
7 Po7(SD) Eth LACP Eth1/7(I)
8 Po8(SD) Eth LACP Eth1/8(I)
9 Po9(SD) Eth LACP Eth1/9(I)
10 Po10(SD) Eth LACP Eth1/10(I)
116 Po116(SD) Eth LACP Eth1/116(I)
```

7. Enable automatic Cisco NX-OS errdisable state recovery:

```
errdisable recovery cause link-flap
errdisable recovery interval 30
```

Cisco NX-OS places links that flap repeatedly into errdisable state to prevent spanning tree convergence problems caused by non-functioning of hardware. During the Cisco VIM installation, the server occasionally triggers the link flap threshold, so enabling automatic recovery from this error is recommended.

```
errdisable recovery cause link-flap
errdisable recovery interval 30
```

8. If you are installing Cisco Virtual Topology Systems, an optional Cisco NFVI application, enable jumbo packets and configure 9216 MTU on the port-channel or Ethernet interfaces. For example:

```
Port channel:
interface port-channel10
switchport mode trunk
switchport trunk allowed vlan 80,323,680,860,2680,3122-3250
mtu 9216
vpc 10
Ethernet:
interface Ethernet1/25
switchport mode trunk
switchport trunk allowed vlan 80,323,680,860,2680,3122-3250
mtu 9216
```

ToR Switch Configuration for UCS B-Series Pods

Configuring ToR Switches for UCS B-Series Pods

Complete the following steps to create a vPC on a pair of Cisco Nexus ToR switches for a UCS B-Series pod. The steps are similar to configuring ToR switches for C-Series pods, with some differences. Here, the two ToR switches are Storm-tor-1 (mgmt0 is 172.18.116.185) and Storm-tor-2 (mgmt0 is 172.18.116.186). Modify the configuration as applicable to your environment.

1. Change the vPC domain ID for your configuration. The vPC domain ID can be any unique number. The IP address on the other switch mgmt0 port is used for the keepalive IP. Change it to the IP used for your network.

```
Storm-tor-1 (mgmt0 is 172.18.116.185).
 feature vpc vpc domain 116
 peer-keepalive destination 172.18.116.186
 for each vlan_type (mgmt_vlan, tenant_vlan_range, storage, api, external, provider); # execute the
following for each vlan
 vlan <vlan_type> no shut
 vrf context management
 ip route 0.0.0.0/0 172.18.116.1
 interface mgmt0
 vrf member management
 ip address 172.18.116.185/24

 Storm-tor-2 (mgmt0 is 172.18.116.186).
 feature vpc vpc domain 116
 peer-keepalive destination 172.18.116.185
 for each vlan_type (mgmt_vlan, tenant_vlan_range, storage, api, external, provider); # execute the
following for each vlan
 vlan <vlan_type> no shut
 vrf context management
 ip route 0.0.0.0/0 172.18.116.1
 interface mgmt0
 vrf member management
 ip address 172.18.116.186/24
```

2. As both switches are cabled identically, the rest of the settings are identical on both the switches. Configure all the interfaces that are connected to the fabric interconnects for VPC.

```
 feature lacp
 interface port-channel1
 description "to fabric interconnect 1" switchport mode trunk
 vpc 1
 interface port-channel2
 description "to fabric interconnect 2" switchport mode trunk
 vpc 2
 interface Ethernet1/43
 description "to fabric interconnect 1" switchport mode trunk
 channel-group 1 mode active interface Ethernet1/44
 description "to fabric interconnect 2" switchport mode trunk
 channel-group 2 mode active
```

3. Create the port-channel interface on the ToR that connects to the management node:

```
 interface port-channel3
 description "to management node" spanning-tree port type edge trunk switchport mode trunk
 switchport trunk allowed vlan <mgmt_vlan> no lacp suspend-individual
 vpc 3
 interface Ethernet1/2
 description "to management node" switchport mode trunk
 channel-group 3 mode active
```

4. To enable multicast traffic for Cisco VIM, change the Nexus 9000 configuration including enabling the PIM routing and OSPF:

```
 feature ospf feature pim
 feature interface-vlan feature hsrp
 ip pim rp-address 192.1.1.1 group-list 224.0.0.0/4 ip pim ssm range 232.0.0.0/8
 ip pim anycast-rp 192.1.1.1 192.168.100.1
 ip pim anycast-rp 192.1.1.1 192.168.100.2
 interface Ethernet1/18
 description "Mcast Sender Example"
 switchport trunk allowed vlan <provider/tenant vlan id>
 interface loopback7
 ip address 192.1.1.1/32
 ip router ospf 777 area 0.0.0.0 ip pim sparse-mode
 router ospf 777
 router-id 1.1.1.1
 area 0.0.0.0 default-cost 10
 interface Vlan<provider/tenant vlan id> no shutdown
 ip address <IP address/mask> no ip ospf passive-interface ip router ospf 777 area 0.0.0.0 ip pim sparse-
mode
 hsrp 101
 priority 11
 ip <provider/tenant gateway address>

 Storm-tor-1
 interface loopback0
 ip address 192.168.100.1/32
 ip router ospf 777 area 0.0.0.0 ip pim sparse-mode

 Storm-tor-2
 interface loopback0
 ip address 192.168.100.2/32
 ip router ospf 777 area 0.0.0.0 ip pim sparse-mode
```

5. If Cisco VIM implementation has extensive multicast traffic, prioritize the multicast traffic by setting up the following service classes on the ToR switches and enabling the media QoS profile. Fore more details, see ToR Management. The Nexus 9000 configuration is as follows:

```
 class-map type qos match-all class-silver match cos 2
 class-map type qos match-all class-bronze match cos 1
 policy-map type qos system-level-qos class class-silver
 set qos-group 3 class class-bronze
 set qos-group 2
 class-map type queuing class-silver match qos-group 3
 class-map type queuing class-bronze match qos-group 2
 policy-map type queuing Uplink-out_policy class type queuing class-silver
 bandwidth percent 60 priority
 class type queuing class-bronze bandwidth percent 30
 class type queuing class-default bandwidth percent 10
 class-map type network-qos class-silver match qos-group 3
 class-map type network-qos class-bronze match qos-group 2
 policy-map type network-qos system-level-net-qos class type network-qos class-silver
 set cos 2
 mtu 9126
 multicast-optimize
 class type network-qos class-bronze set cos 1
 mtu 9126
 class type network-qos class-default mtu 9126
 system qos

 service-policy type queuing input fcoe-default-in-policy service-policy
 type queuing output Uplink-out_policy service-policy type qos input
system-level-qos
 service-policy type network-qos system-level-net-qos
```

6. Enable jumbo frames for each ToR port-channel that connects to the Fabric Interconnects:

```
interface port-channel<number>
mtu 9216
```

⚠ Ensure that you enable jumbo frames in the *setup_data.yaml* file as given below:

```
# Jumbo MTU functionality.
# ENABLE_JUMBO_FRAMES: True
```

Preparing Cisco IMC and Cisco UCS Manager

Preparing Cisco IMC and Cisco UCS Manager

Cisco NFVI requires specific Cisco Integrated Management Controller (IMC) and Cisco UCS Manager firmware versions and parameters. The Cisco VIM bare metal installation uses the Cisco IMC credentials to access the Cisco IMC interface which is used to delete and create vNICS and to create bonds. Complete the following steps to verify if Cisco IMC and UCS Manager are ready for Cisco NFVI installation:

1. Verify that each Cisco UCS server uses Cisco IMC firmware version of either 2.0 series (2.0(13i) or greater preferably 2.0(13n)) or 3.0 series (use 3.0.3(f) or later). You can download the latest Cisco IMC ISO image from the Cisco Software Download site. For upgrade procedures, see the Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide.
2. For UCS B-Series pods, verify that the Cisco UCS Manager version is one of the following: 2.2(5a), 2.2(5b), 2.2(6c), 2.2(6e), 3.1(c).
3. For UCS C-Series pods, verify the following Cisco IMC information is added: IP address, username, and password.
4. For UCS B-Series pods, verify the following UCS Manager information is added: username, password, IP address, and resource prefix. The resource prefix maximum length is 6. The provisioning network and the UCS Manager IP address must be connected.
5. Verify that no legacy DHCP/Cobbler/PXE servers are connected to your UCS servers. If so, disconnect or disable the interface connected to legacy DHCP, Cobbler, or PXE server. Also, delete the system from the legacy cobbler server.
6. Verify if Cisco IMC has NTP enabled and is set to the same NTP server and time zone as the operating system.

Management Node on UCS C-series (M4/M5)

Installing Management Node on UCS C-series (M4/M5)

This procedure installs RHEL with the following modifications:

- Hard disk drives are setup in RAID 6 configuration with one spare HDD for eight HDDs deployment, two spare HDDs for 9 to 16 HDDs deployment, or four spare HDDs for 17 to 24 HDDs deployment.
- Networking: Two bridge interfaces are created; one for the installer API (br_api off the LOM interfaces) and the other for provisioning (br_mgmt off the Cisco VIC on the MLOM or off a X710 based Intel NIC depending on the BOM). Each bridge interface has underlying interfaces bonded together with 802.3ad. Provision interfaces are 10/40 GE interfaces (either off Cisco VICs or X710 Intel NIC (first 2 ports of Intel NIC)). API interfaces are 1/10 GE LOMs based on the BOM. For using NFVbench, you require another NIC card constituting off 2xIntel 520, or 2xIntel 710XL, or 4xIntel710 X. For management node BOM (Intel NIC based), ensure that you place the NIC for NFVbench at a slot higher than that of the br_mgmt based Intel NIC.
- The installer code is placed in /root/.
- SELinux is enabled on the management node for security.

Before you Begin

Verify that the Cisco NFVI management node where you plan to install the Red Hat for Enterprise Linux (RHEL) operating system is a Cisco UCS C240 M4/M5 Small Form Factor (SFF) with 8, 16, or 24 hard disk drives (HDDs). In addition, the management node must be connected to your enterprise NTP and DNS servers. If your management node server does not meet these requirements, do not continue until you install a qualified UCS C240 server. Also, verify that the pod has MRAID card.

1. Log into the **CIMC GUI** of Cisco NFVI management node.
2. Follow steps in Configuring the Server Boot Order to set the boot order to boot from local HDD.
3. Follow steps in Cisco UCS Configure BIOS Parameters to set the following advanced BIOS settings:

   For management node based on UCS M4 boxes, set the following for BIOS parameters:

   ```
   PCI ROM CLP—Disabled
   PCH SATA Mode—AHCI
   All Onboard LOM Ports—Enabled
   LOM Port 1 OptionROM—Disabled
   LOM Port 2 OptionROM—Disabled
   All PCIe Slots OptionROM—Enabled
   PCIe Slot:1 OptionROM—Enabled

   PCIe Slot:2 OptionROM—Enabled
   PCIe Slot: MLOM OptionROM—Disabled
   PCIe Slot:HBA OptionROM—Enabled
   PCIe Slot:FrontPcie1 OptionROM—Enabled
   PCIe Slot:MLOM Link Speed—GEN3
   PCIe Slot:Riser1 Link Speed—GEN3
   PCIe Slot:Riser2 Link Speed—GEN3
   MLOM OptionROM—Enabled
   ```

   For management node based on UCS M5 boxes, set the following for BIOS Parameters:

   ```
   All Onboard LOM Ports—Enabled
   LOM Port 1 OptionROM—Disabled
   LOM Port 2 OptionROM—Disabled
   PCIe Slot:1 OptionROM—Enabled
   PCIe Slot:2 OptionROM—Enabled
   MLOM OptionROM—Enabled
   MRAID OptionROM—Enabled
   ```

   Other parameters must be set to default.
4. Click **Save Changes**.
5. Add the management node vNICs to the provisioning VLAN to provide the management node with access to the provisioning network:

   a. In the CIMC navigation area, click the **Server** tab and select **Inventory**.
   b. In the main window, click the **Cisco VIC Adapters > General Tab**, and then click **Reset to Default** tab.

   Delete any additional vNICs configured on the UCS server beyond the two default ones.

6. Download the ISO on a local server that can serve HTTP and use CIMC GUI to mount the ISO under *Cisco IMC Mapped vMedia*.

7. In CIMC, launch the KVM console.
8. Mount the Cisco VIM Build node ISO image as a virtual DVD.
9. Reboot the UCS server, then press **F6** to enter the boot menu.
10. Select the CIMC mapped DVD to boot the Cisco VIM Build node ISO image provided with the install artifacts.
11. From the boot menu, select **Install Cisco VIM Management Node**. By default, it is selected after the timeout.
12. At the prompt, enter the required parameter values to install the management node as a UM node only or not:

    - Mode selection — Select the mode that the management node needs to serve. Enter 1 for standard management node, 2 for UM node, or 3 for Software Distribution System (SDS) node
    - Hostname—Enter the management node hostname. The hostname length must be 32 or fewer characters.
    - Select **Yes** to Install as Unified Management only when required. Migration from one to another is not supported.
    - API IPv4 address—Enter the management node API IPv4 address in CIDR (Classless Inter-Domain Routing) format. For example, 172.29.86.62/26.
    - API Gateway IPv4 address—Enter the API network default gateway IPv4 address.
    - MGMT IPv4 address—Enter the management node MGMT IPv4 address in CIDR format. For example, 10.30.118.69/26

      ⚠ The MGMT IPv4 entry is not required if the management node is installed as unified management node only.

    - Prompt to enable static IPv6 address configuration—Enter **Yes** to continue input similar IPv6 address configuration for API and MGMT network, or **No** to skip if IPv6 is not needed.
    - API IPv6 address—Enter the management node API IPv6 address in CIDR (Classless Inter-Domain Routing) format. For example, 2001:c5c0:1234:5678:1001::5/8.
    - Gateway IPv6 address—Enter the API network default gateway IPv6 address.
    - MGMT IPv6 address—Enter the management node MGMT IPv6 address in CIDR format. For example, 2001:c5c0:1234:5678:1002::5/80
    - DNS server—Enter the DNS server IPv4 address or IPv6 address if static IPv6 address is enabled.
    - Option for Teaming Driver for Link Aggregation <Yes/No> — Select **Yes** if Nexus switch is ToR, and **No** if Cisco NCS 5500 is ToR.
    - Option for setting MGMT's Link Aggregation to active-active (802.3ad) mode <Yes|No> — Enter **Yes** for active-active mode or **No** for active-backup mode. Most commonly, the Active-active mode is the recommended mode. The active-backup mode is recommended only when CIMC is in in-band shared mode without using the dedicated CIMC mgmt port.

After you enter the management node IP addresses, the Installation options menu appears with several options. Fill in the options as listed below (option 8 and 2) and leave the other fields as it is. If you are unable to start the installation, enter **r** to refresh the Installation menu.

1. From the Installation menu, select option **8** to enter the root password.
2. From the Installation menu, select option **2** to enter the time zone.
3. Under the Timezone settings, select the option **1**, as option **2** is not supported.
4. Enter the number corresponding to your time zone.
5. Enter the number for your region.
6. Choose the city and then confirm the time zone settings.

   ⚠ NTP server IP must not be entered at the time of setting the time zone.

7. After confirming your time zone settings, enter **b** to start the installation.
8. After the installation is complete, press **Return** to reboot the server.
9. After the reboot, check the management node clock using the Linux *date* command to ensure that the TLS certificates are valid, for example:

```
#date
 Mon Aug 22 05:36:39 PDT 2016
 To set date:
 #date -s '2016-08-21 22:40:00'
 Sun Aug 21 22:40:00 PDT 2016
 To check for date:
 #date
 Sun Aug 21 22:40:02 PDT 2016
```

Management Node on Quanta Servers

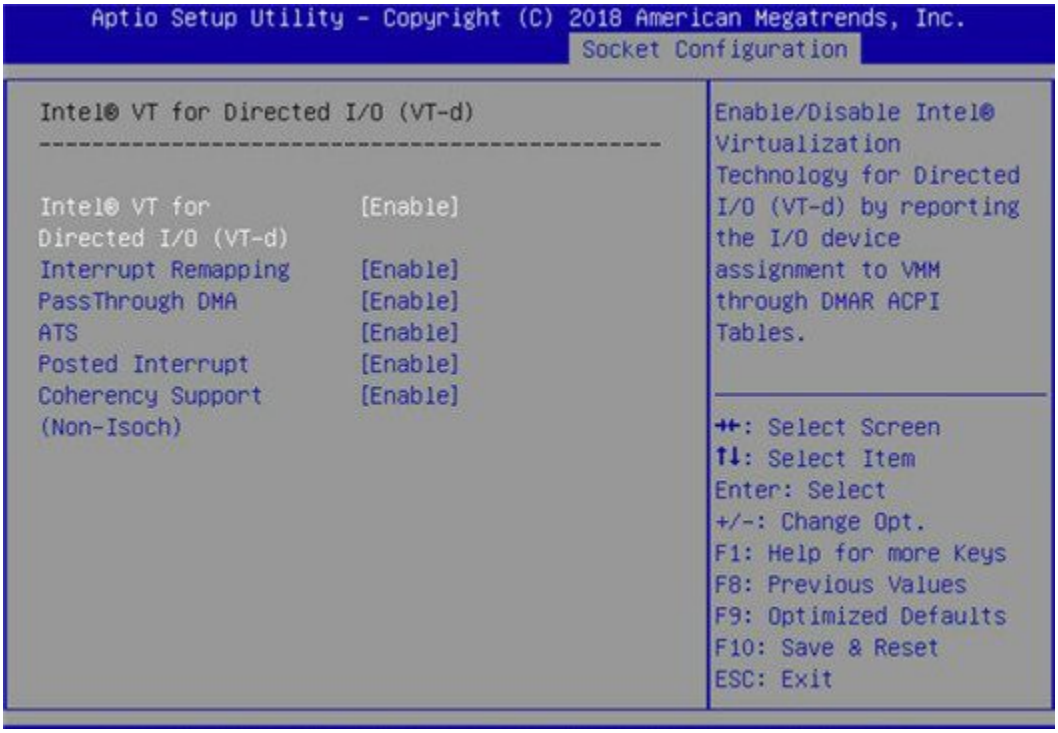
Installing Management Node on Quanta Servers

Most of the settings in the server remain default.

> To run NFVbench, you must enable the Intel VT for Directed I/O (VT-d) on the Management node.

To enable the Intel VT for Directed I/O, navigate to the following path:

BIOS Setup > Socket Configuration > IIO Configuration > Intel VT for Directed I/O (VT-d) > Intel VT for Directed I/O (VT-d) > Enable



To enable NFVbench on a Quanta management node:

- Reboot the MGMT node, press F2 or DEL to enter BIOS:
- Choose **Socket Configuration > IIO Configuration > Intel(R) VT for Directed I/O (VT-d)**.
- Set **Intel(R) VT for Directed I/O (VT-d)** to Enable
- Press F10 to save and exit.

> From Cisco VIM 3.4.0 onwards, the remote installation of a management node is possible to alleviate manual bootstrapping of the management node. For more information, see Remote Installation of Management Node.

Cisco VIM Software Hub

Installing Cisco VIM Software Hub

Cisco VIM Software Hub alleviates the need for Cisco VIM management nodes to have internet connectivity and helps to remove the logistics of shipping USBs to multiple pods across the enterprise for software installation or update of the cloud.

Cisco VIM Software Hub is also referred as Software Delivery Server, therefore you might encounter references to SDS in the configuration files, directory paths, and automation outputs.

Prerequisites for Cisco VIM Software Hub Nodes

- Ensure that the Cisco VIM management nodes have connectivity to the Cisco VIM Software hub.
- Ensure that the Cisco VIM Software Hub node where you want to install the *buildnode.iso* file is Cisco VIM SDS BOM compliant
- Ensure that the Cisco VIM Software Hub node is connected to the enterprise NTP and DNS servers.
- Ensure that the Cisco VIM Software Hub node has a hardware MRAID and a cache card.

Prerequisites for Cisco VIM Software Hub Server

1. TLS certificate (For production environment)
   On the Cisco VIM Software Hub server, configure a secure registry so that the pods can obtain the container images over TLS. You need to provide a certificate signed by a trusted third-party CA authority and the **CommonName** in the certificate must match the Cisco VIM Software Hub Registry FQDN name. The *sds_setup_data.yaml* file has 3 fields:

   - SSL_CERT_FILE: Path of x509 certificate obtained from a trusted CA authority
   - SSL_CERT_KEY_FILE: Path of private key obtained from a trusted CA authority
   - SSL_CERT_CHAIN_FILE: Path of a single ssl cert chain file. The trusted CA authority might provide you the x509 cert for your domain, intermediate x509 cert, and root CA cert.
     You need to create a single SSL cert chain file using the commands below:

     ```
     cat <x509 domain cert> >> ssl_chain_file.cer
     cat <intermediate ca cert> >> ssl_chain_file.cer # cat <root ca cert> >> ssl_chain_file.cer
     ```

2. Self-signed certificate (For internal use)

   We recommend that you use a trusted CA-signed certificate when a Cisco VIM Software Hub node is used in a production environment. For internal testing and POC, Cisco supports Cisco VIM Software Hub node with a self-signed certificate.
   Follow the below steps to generate the self-signed certificate:

   ```
   # openssl genrsa -des3 -out https_reverse_proxy.key 2048
   # openssl req -new -key https_reverse_proxy.key -out https_reverse_proxy.csr
   # cp https_reverse_proxy.key https_reverse_proxy.key.org
   # openssl rsa -in https_reverse_proxy.key.org -out https_reverse_proxy.key
   # openssl x509 -req -days 365 -in https_reverse_proxy.csr -signkey
   https_reverse_proxy.key -out https_reverse_proxy.cer
   ```

   Generate the certificate with the same FQDN as specified in the sds_setup_data.yaml. Populate the SSL_CERT_FILE, SSL_CERT_KEY_FILE and SSL_CERT_CHAIN_FILE in sds_setup_data.yaml. In case of a self-signed certificate, use the same x509 certificate for both cert file and cert chain file. You need to manually trust the self-signed certificate. The operator needs to execute the commands below on both Cisco VIM Software Hub server and Cisco VIM pod management node:

   ```
   # cp <x509 cert> /etc/pki/ca-trust/source/anchors/ca.crt
   # update-ca-trust extract
   ```

   For docker registry to work with self-signed certificates, execute the commands below on the SDS server:

```
# mkdir /etc/docker/certs.d/<fqdn>
# cp <x509 cert> /etc/docker/certs.d/<fqdn>/ca.crt
```

3. DNS server:

   Ensure that the DNS server can reach the pods and the Cisco VIM Software Hub server. The DNS server must be able to resolve the Cisco VIM Software Hub Registry FQDN. If the enterprise does not have a unified DNS, then you need to populate the */etc/hosts* file with FQDN after provisioning a node using the ISO archive file.

Installing Cisco VIM Software Hub Node

The steps to install a Cisco VIM Software Hub node are similar to the steps in Management Node on UCS C-series (M4/M5). The only difference being, in Step 11 of the task, you need to choose the option to configure the server as a Cisco VIM Software Hub server. In the subsequent prompts, you can enter information such as the hostname, ipv4 or ipv6 addresses for br_public and br_private interfaces, and gateway addresses, similar to the Management Node on UCS C-series (M4/M5).

The node is installed with RHEL 7.6 with the following modifications:

- Hard disk drives are set up in RAID 6 configuration with two spare HDDs for a 16 HDDs deployment or four spare HDDs for a 24 HDDs deployment.
- Two bridge interfaces are created, namely, br_public and br_private. In case of a connected Cisco VIM Software Hub server, the br_public interface is connected to the internet. The br_private interface is local to your datacenter. The management node for every Cisco VIM pod must be reachable to the br_private interface of Cisco VIM Software Hub server through the br_api interface. Each bridge interface has underlying interfaces bonded together with 802.3ad. For the Cisco VIM Software Hub, the private interfaces are over 10/25 GE Cisco VICs/ Intel NIC, while the public interfaces are 1 GE LOMs.
- Security_Enhanced Linux (SELinux) is enabled on the management node for security.

The Cisco VIM Software Hub code consists of packages with installer code. After provisioning the server with ISO, the installer code is placed in the following path:

```
/root/cvim_sds-<tag>
```

Setting up Cisco VIM Software Hub for Cisco VIM Artifact Distribution

You must configure a *sds_setup_data.yaml* file for each installer workspace.

1. Copy the example file from the *openstack-configs* directory and save it as *sds_setup_data.yaml*.
2. If you want to install a release tag on a Cisco VIM Software Hub server, update the fields in the *sds_setup_data.yaml* file as required.

```
## Configuration File:
# This file is used as an inventory file to setup CVIM SDS (software delivery server).
############################################################
# User Defined Configuration File.
# Information in this file is specific to the SDS setup.
############################################################
SSL_CERT_FILE: <abs_location_for_cert_path of x509 certificate>
SSL_CERT_KEY_FILE: <abs_location_for_cert_priv_key of x509 certificate>
SSL_CERT_CHAIN_FILE: <abs_location_for_cert_chain_file of x509 certificate>
############################################################
Cisco Virtualized Infrastructure Manager Installation Guide, 3.0.0
94
Preparing for Cisco NFVI Installation
Installing Cisco VIM Software Hub Node
# Registry credentials to access the CVIM registry (Cisco Supplied)
############################################################
CVIM_REGISTRY_NAME: <satellite.fqdn.com>          # optional, needed to download artifacts from another
SDS server; FQDN of the source SDS server

CVIM_REGISTRY_USERNAME: <username>
CVIM_REGISTRY_PASSWORD: <password>

NETWORKING:
## Max. NTP servers = 4, min of 1
ntp_servers: <ntp.server1.fqdn.com, ntp.server2.fqdn.com >
or
ntp_servers: [ipv6_address, 'ipv4_address'] # "," separated IPv4 or IPv6 address info
http_proxy_server: <proxy.domain.com:8080> # optional, needed if the pod is behind a proxy
https_proxy_server: <proxy.domain.com:8080> # optional, needed if the pod is behind a proxy
SDS_REGISTRY_NAME: <satellite.fqdn.com> #SDS registry name needs to resolve to valid IP
SDS_REGISTRY_USERNAME: <username>
SDS_REGISTRY_PASSWORD: <password>
# (Optional)SDS users who can only pull images from SDS docker registry
SDS_READ_ONLY_USERS:
- username: <user1>
password: <password1>
- username: <user2>
password: <password2>
```

3. Save the *sds_setup_data.yaml* file in the following path:

```
openstack-configs
directory under /root/cvim_sds-<tag>
```

Installing Cisco VIM Software Hub in Connected Mode

In the connected mode, the Cisco VIM Software Hub server having a publicly routable IP address can connect to the cvim-registry or to another Cisco VIM Software Hub server having the target artifacts and the registry. When the Cisco VIM Software Hub server is initially configured with the ISO, Cisco VIM Software Hub workspace of that release is pre-installed in the /*root*/ directory.

1. Download the *mercury-installer.tar.gz* file of the release that you want.
2. Unzip the zip file manually and rename the unzipped file as *cvim_sds-<release>*.
3. Perform the following steps:

   a) Place a valid TLS certificate in the directory:

   ```
   /root/cvim_sds-<tag>/openstack-configs
   ```

   b) Update the fields of the Cisco VIM Software Hub setup data file and save it in the following directory:

   ```
   /root/cvim_sds-<tag> openstack-configs
   ```

4. To install the release on the Cisco VIM Software Hub server, navigate to the following directory on the Cisco VIM Software Hub server:

```
/root/cvim_sds-<target-tag>
```

5. Run the following command:

```
# cd to /root/cvim_sds-<target-tag>
# ./sds_runner/runner.py
```

The command validates the Cisco VIM Software Hub node hardware, the contents of the *sds_setup_data.yaml* file, and the validity of the TLS certificate, and then obtains the artifacts from the external Cisco VIM release registry and populates the Cisco VIM Software Hub server.

Installing Cisco VIM Software Hub in Air-Gapped Mode

Cisco VIM Software Hub is installed in the air-gapped mode when the Cisco VIM Software Hub server in the datacenter does not have internet connectivity. You can use the USB drive to load the installation files on the Cisco VIM Software Hub node. The installation files are over 25 GB in size. Downloading them to the USB drive may take several hours depending on the speed of your internet connection.

Before you begin

- Ensure that you have set up a CentOS 7 staging server (VM, laptop, or UCS server) with a 64 GB USB 2.0 drive.
- Ensure that you have internet, preferably a wired connection, to download the Cisco VIM installation files, which you want to load onto the USB drive.
- Ensure that you have disabled the CentOS sleep mode.

1. On the staging server, use yum to install the following packages:
   a) PyYAML

   b) python-requests

   c) Python 3.6 (rh-python36))

   Check if python 3.6 binary is located at */opt/rh/rh-python36/root/bin/*, if not copy the python 3.6 binary to */opt/rh/rh-python36/root/bin/.*
2. Access the Cisco VIM software download web site using a web browser.
3. Log in with the credentials provided by your account representative and download the *getartifacts.py* script from the external registry.

```
# download the new getartifacts.py file
curl -o getartifacts.py
https://username:password@cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/<3.4.x>
/getartifacts.py
# Change the permission of getartificats.py
chmod +x getartifacts.py
```

4. Run the *getartifacts.py* script. The script formats the USB 2.0 drive (or USB 3.0 drive for M5-based management node) and downloads the installation files. You must provide the registry username and password, tag ID, and USB partition on the staging server.

```
./getartifacts.py -h
usage: getartifacts.py [-h] -t TAG -u USERNAME -p PASSWORD [--proxy PROXY]
                       [--retry] (-d DRIVE | -f FILE)
                       [--mgmtk8s | --argus | --insight | --sds | -U]

Script to pull container images en masse.

optional arguments:
  -h, --help            show this help message and exit
  -t TAG, --tag TAG     Installer version to pull
  -u USERNAME, --username USERNAME
                        Registry username
  -p PASSWORD, --password PASSWORD
                        Registry password
  --proxy PROXY         https_proxy if needed
  --retry               Try to complete a previous fetch
  -d DRIVE, --drive DRIVE
                        Provide usb drive path
  -f FILE, --file FILE  location of image file
  --mgmtk8s             Additionally download CVIM MON HA artifacts
  --argus               Additionally download argus artifacts
  --insight             Additionally download insight artifacts
  --sds                 Additionally download sds artifacts
  -U, --upgrade         Additionally download artifacts for upgrade from 2.4.x

This script pulls images from remote registry then copies the contents to USB
drive or image file based on the user supplied option
```

The *getartifacts.py* script gets the images from the remote registry and copies the contents to the USB drive.

5. To identify the USB drive, execute the *lsblk* command before and after inserting the USB drive. The command displays a list of available block devices. You can use the output data to find the location of the USB drive. You must provide the entire drive path in the –d option instead of any partition.
   For example:

   ```
   sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> --sds [--proxy proxy.
   example.com]
   ```

   For file-based image, follow the example below:

   ```
   sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -f /var/<artifacts-x-y-z.img> --sds [--
   proxy proxy.example.com]
   ```

6. Verify the integrity of the downloaded artifacts and container images.

```
# create a directory sudo mkdir -p /mnt/Cisco
# /dev/sdc is the USB drive, same as supplied in getartifacts.py python script sudo mount /dev/sdc1
/mnt/Cisco
cd /mnt/Cisco
# execute the test-usb help to look at the options
./test-usb -h

usage: ./test-usb [-h] -- Show this program to check integrity of artifacts in this USB drive/image file
                  [-a] -- Check integrity of all (core and all) artifacts in this USB drive/image File
                  [-l] -- Location of artifacts
                  [-f] -- Location of image file
                  [-U] -- test upgrade artifacts from 2.4.x to 3.4.y
# execute the verification script
./test-usb
# failures will be explicitly displayed on screen, sample success output below
# sample output of ./test-usb execution with 3.0.0 release
#./test-usb
INFO: Checking the integrity of this USB drive
INFO: Checking artifact buildnode-K9.iso
INFO: Checking artifact registry-3.0.0.tar.gz
INFO: Checking the integrity of this USB drive
INFO: Checking artifact buildnode-K9.iso
INFO: Checking artifact registry-3.0.0.tar.gz
INFO: Checking artifact mariadb-app-K9.tar.gz
INFO: Checking artifact haproxy-K9.tar.gz
INFO: Checking artifact insight-K9.tar.gz
Node
INFO: Checking required layers:
INFO: 548 layer files passed checksum.
If a failure occurs, an error message is displayed. For example:
# ./test-usb
INFO: Checking the integrity of this USB drive
INFO: Checking artifact buildnode-K9.iso
ERROR: Checksum for artifact buildnode-K9.iso does not match ('SHA512 (buildnode-K9.iso) =
96ec62a0932a0d69daf60acc6b8af2dc4e5eca132cd3781fc17a494592feb52a7f171eda25e59c0d326fbb09194eeda66036cbdc3
870dafe74f59cf1f2dce225'
!= 'SHA512 (buildnode-K9.iso) =
a6a9e79fa08254e720a80868555679baeea2dd8f26a0360ad47540eda831617bea0514a117b12ee5f36415b7540afa112a1c904cd
69e40d704a8f25d78867acf')
INFO: Checking artifact registry-3.4.2.tar.gz
ERROR: Artifact registry-3.4.2.tar.gz is not present INFO: Checking required layers:
ERROR: Layer file sha256:002aa1f0fbdaea7ea25da1d906e732fe9a9b7458d45f8ef7216d1b4314e05207 has a bad
checksum
ERROR: Layer file sha256:5be3293a81773938cdb18f7174bf595fe7323fdc018c715914ad41434d995799 has a bad
checksum
ERROR: Layer file sha256:8009d9e798d9acea2d5a3005be39bcbfe77b9a928e8d6c84374768ed19c97059 has a bad
checksum
Cisco Virtualized Infrastructure Manager Installation Guide, 3.4.x
97
Preparing for Cisco NFVI Installation
Installing Cisco VIM Software Hub in Air-Gapped Mode
ERROR: Layer file sha256:ea55b2fc29b95d835d16d7eeac42fa82f17e985161ca94a0f61846defff1a9c8 has a bad
checksum
INFO: 544 layer files passed checksum.
```

7. To resolve failure in downloading artifacts, unmount the USB and run the *getartifacts* command again with the *--retry* option.

```
sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> --sds --retry
```

8. Mount the USB and then run the *test-usb* command to validate if all the files are downloaded.

```
# /dev/sdc is the USB drive, same as supplied in getartifacts.py python script
sudo mount /dev/sda1 /mnt/Cisco
cd /mnt/Cisco
```

9. Execute the verification script:

```
# ./test-usb
# In case of failures the out of the command displays a message indicating the same on the screen
```

   For file-based image, execute the following script:

```
# ./test-usb -f /var/<artifacts-x-y-z.img>
# In case of failures, the output of the command displays a message indicating the same on the screen
```

10. When the USB integrity test is complete, unmount the USB using the below command:

```
sudo umount /mnt/Cisco
```

11. After the artifacts of a target release are saved on the USB, you must unplug the USB from the staging server, connect it to the Cisco VIM Software Hub server, and then perform the following steps on the Cisco VIM Software Hub server:

    a. Provision your Cisco VIM Software Hub server with the build node ISO of that release and then connect the USB to the Cisco VIM Software Hub server.
    b. To copy the contents of the USB to the Cisco VIM Software Hub server, navigate to the */root/cvim_sds-<tag>* directory, and then execute the import artifacts command:

```
# cd ~/cvim_sds-<tag>/tools
# ./import_artifacts.sh -s
```

       To copy the contents of the file-based image to the Cisco VIM Software Hub server, navigate to the */root/cvim_sds-<tag>* directory, and then execute the import artifacts command:

```
# cd ~/cvim_sds-<tag>/tools
# ./import_artifacts.sh -s -f /var/<artifacts-x-y-z.img>
```

    c. Place a valid TLS certificate in */root/cvim_sds-<tag>/openstack-configs* directory.
    d. Configure the Cisco VIM Software Hub setup data file with all the fields and placed the file in the */root/cvim_sds-<tag>/openstack-configs* directory.
    e. Install the release on the Cisco VIM Software Hub server.
    f. Navigate to the *cvim_sds* directory on the Cisco VIM Software Hub server and execute the following command:

```
# cd /root/cvim_sds-<tag>
# ./sds_runner/runner.py
Usage: runner.py [options]
Runner
Options:
-h, --help show this help message and exit
-l, --list_steps List steps
-s SKIP_STEPS, --skip_steps=SKIP_STEPS
Comma separated list of steps to skip. eg -s 2,3
-p PERFORM_STEPS, --perform=PERFORM_STEPS
-y, --yes Yes option to skip steps without prompt
```

Installing Pod from Cisco VIM Software Hub Server

When you want to install a Cisco VIM pod using the artifacts obtained from the Cisco VIM Software Hub server, you need to provide an additional parameter in *setup_data.yaml.* Ensure that the release artifacts are pre-installed on the Cisco VIM Software Hub server and that the *setup_data.yaml* file is populated with the pod details. Provide the registry FQDN name for install through Cisco VIM Software Hub. For example, your domain.com.

```
REGISTRY_NAME: '<registry_name>' # Mandatory Parameter.
```

Cisco VIM pod *setup_data.yaml* requires the REGISTRY_USERNAME and REGISTRY_PASSWORD to connect to the docker registry and fetch docker images. To fetch the docker images from Cisco VIM Software Hub node, provide the user credentials available in the SDS_READ_ONLY_USERS section of *sds_setup_data.yaml.* The details of an admin user with read/write access to docker registry are provided in SDS_REGISTRY_USERNAME and SDS_REGISTRY_PASSWORD field. So, it is recommended to have a read-only user on Cisco VIM pod.

The Cisco VIM management node must have connectivity to the organization's DNS server to resolve the Cisco VIM Software Hub server domain.

The Cisco VIM management node must have connectivity to the organization's DNS server to resolve the Cisco VIM Software Hub server domain.

Supported Day 2 Operations

The following Day 2 operations are supported on the Cisco VIM Software Hub server:

1. Reconfiguration of Cisco VIM Software Hub TLS certificate and Cisco VIM Software Hub registry credentials.
2. Cisco VIM Software Hub server backup and restore.
3. Execution of registry cleanup script.
4. Manual update of few packages in the maintenance window.

UCS C-Series Pod

Setting Up UCS C-Series Pod

Procedure

After you install the RHEL OS on the management node, perform the following steps to set up the Cisco UCS C-Series servers:

1. Log into CIMC GUI of Cisco NFVI management node**.**
2. Follow steps in Configuring the Server Boot Order to set the boot order to boot from Local HDD.
3. Follow steps in Configure BIOS Parameters to set the LOM, HBA, and PCIe slots to the following settings:

   For servers based on UCS M4 boxes, set the following for BIOS parameters:

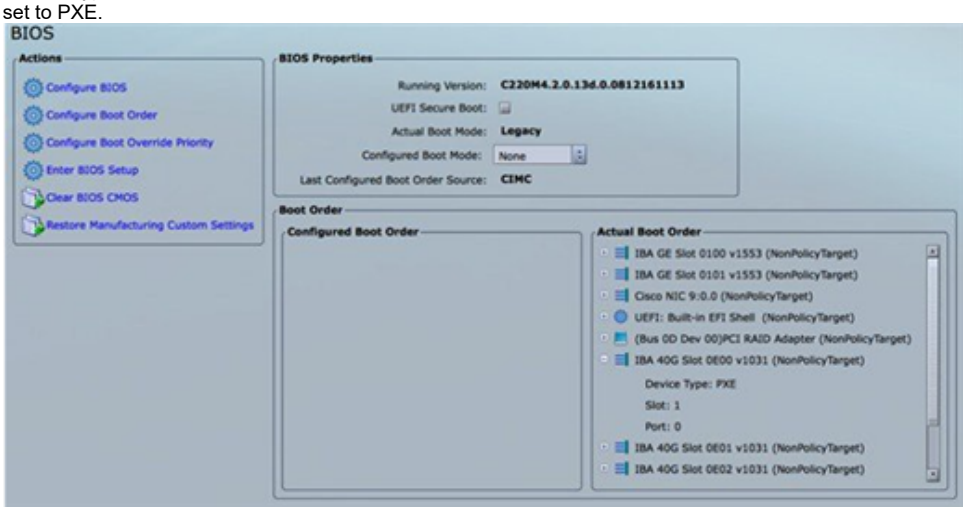
   - CDN Support for VIC—Disabled
   - PCI ROM CLP—Disabled
   - PCH SATA Mode—AHCI
   - All Onboard LOM Ports—Enabled
   - LOM Port 1 OptionROM—Disabled
   - LOM Port 2 OptionROM—Disabled
   - All PCIe Slots OptionROM—Enabled
   - PCIe Slot:1 OptionROM—Enabled
   - PCIe Slot:2 OptionROM—Enabled
   - PCIe Slot: MLOM OptionROM—Enabled
   - PCIe Slot:HBA OptionROM—Enabled
   - PCIe Slot:N1 OptionROM—Enabled
   - PCIe Slot:N2 OptionROM—Enabled
   - PCIe Slot:HBA Link Speed—GEN3

   For servers based on UCS M5 boxes, set the following for BIOS parameters:

   - All Onboard LOM Ports—Enabled
   - LOM Port 1 OptionROM—Disabled
   - LOM Port 2 OptionROM—Disabled
   - PCIe Slot:1 OptionROM—Enabled
   - PCIe Slot:2 OptionROM—Enabled
   - MLOM OptionROM—Enabled
   - MRAID OptionROM—Enabled

   Other parameters must be set to their default values.
4. To setup C-series pod with Intel 710 NIC:

   a. Each C-series server must have two 4-port Intel 710 NIC cards.
   b. Connect the ports A, B, and C for each Intel 710 NIC card to the respective ToR.
   c. Enable the PCI slot with Intel NIC cards through the BIOS setting (**BIOS > Configure BIOS > Advanced > LOM and PCI Slot Configuration > All PCIe Slots OptionROM**-Enabled and enable respective slots).
   d. Identify the slots by checking the slot-id information under the **Network-Adapter** tab listed under the Inventory link on the **CIMC** pane.
   e. All the Intel NIC ports must be indicated in the BIOS summary page under the **Actual Boot Order** pane, as IBA 40G Slot xyza with Device Type is
   set to PXE.



For UCS M5, look for **IBA 40G Slot** under the **BIOS Properties**

If the boot order for the Intel NICs is not listed as above, enable the PXE boot setting for each UCS-C M4 series server by using either Intel's BootUtil tool on a pre-installed Linux system or boot a special ISO image. This is time consuming especially on a large pod with many nodes. Hence, an automated tool is developed to help with this painstaking process.

> ⚠ From release Cisco VIM 3.4.0, the above context is applicable only to UCS M4 series servers, as UCS-M5 is based on UEFI for boot.

While the pxe-boot tool simplifies the job of flashing the intel NIC cards, the restrictions of COSI compliance prevent us from shipping third-party utility (from CIMC 4.0 onwards). Administrators must download the PREBOOT.exe file from Intel website: https://downloadcenter.intel.com/download/27539/Ethernet-Intel-Ethernet-Connections-Boot-Utility-Preboot-Images-and-EFI-Drivers

Version: 22.10

Date: 12/7/2017

OS Independent

Language: English

Size: 16.54 MB

MD5: ace485e8a3ef9039212f52b636ce48e3

PREBOOT.EXE

Ensure that there is unrestricted network access from Cisco VIM Management node to UCS-C series server's CIMC over following ports:

- TCP/2400 - serial-over-lan (SOL)
- TCP/22 - XMLAPI

Ensure that there is unrestricted network access from UCS-C series server's CIMC to Cisco VIM Management node's API interface over following port:

- TCP/80 - HTTP

This utility updates only the Intel PXE configuration and not the card's firmware or Option ROM.

Utility Details

Two scripts available in the Cisco VIM Installer's tools directory are:

- create-bootutil-img.sh
- intel-bootutil-update.py

Usage

```
[root@cologne-mgmt tools]# ./create-bootutil-img.sh
Usage: ./create-bootutil-img.sh <PREBOOT.exe file> <output image name>
```

You can download PREBOOT.exe file from :

https://downloadcenter.intel.com/download/27862/Ethernet-Intel-Ethernet-Connections-Boot-Utility-Preboot-Images-and-EFI-Drivers

Version: 22.1

Date: 12/07/2017

OS Independent

Language: English

Size: 16.54 MB

MD5: ace485e8a3ef9039212f52b636ce48e3

PREBOOT.EXE

To toggle Intel PXE configuration on UCS C-series, use the script below:

```
[root@cologne-mgmt tools]# ./intel-bootutil-update.py -h
usage: intel-bootutil-update.py [-h] [--hosts HOSTS]
[--exclude-hosts EXCLUDE_HOSTS] [-v] [-y]
--setupfile SETUPFILE --bootutil-image
BOOTUTIL_IMAGE --port {0,1,2,3} --state
{enable,disable}
```

Details of the optional arguments for the *intel-bootutil-update.py* script are given below:

Optional Arguments	Description
-h --help	Displays the help with details of each argument of the script.
--hosts HOSTS	Displays the list of servers for PXE configuration from the *setup_data.yaml* file.
--exclude-hosts EXCLUDE_HOSTS	Displays the list of servers to be excluded for PXE configuration from the *setup_data.yaml* file.
-v, --verbose	Enables verbose output.
--setupfile SETUPFILE	Specifies the *setup_data.yaml* file location.
--bootutil-image BOOTUTIL_IMAGE	Specifies the BootUtil image location.
--port {0,1,2,3} port #	Specifies the port to be enabled.
--state {enable,disable}	Enables or disables the PXE configuration.

Example to enable all port A:

```
/intel-bootutil-update.py --setupfile /root/openstack-configs/setup_data.yaml
--bootutil-image /root/bootutil.img --port 0 --state enable
```

Example to enable all port A and B:

```
./intel-bootutil-update.py --setupfile /root/openstack-configs/setup_data.yaml
--bootutil-image /root/bootutil.img --port 0 --port 1 --state enable
```

Example to disable all port C:

```
./intel-bootutil-update.py --setupfile /root/openstack-configs/setup_data.yaml
--bootutil-image /root/bootutil.img --port 2 --state disable
```

Workflow:

Multiple scripts are required as Intel's PREBOOT.exe utility is not packaged with Cisco VIM for COSI compliance:

1. Download PREBOOT.exe version (listed above) from Intel's website.
2. Go to Cisco VIM Installer's tools directory.
3. Run *create-bootutil.img* script to create a CIMC-KVM mountable USB image.
4. Run *intel-bootutil-update.py* script to configure Intel NIC for enabling or disabling PXE.

Utility Examples:

```
[root@cologne-mgmt installer]# cd tools
[root@cologne-mgmt tools]#
[root@cologne-mgmt tools]# ./create-bootutil-img.sh

Usage: ./create-bootutil-img.sh <PREBOOT.exe file> <output image name>


[root@cologne-mgmt tools]#
[root@cologne-mgmt tools]# ./create-bootutil-img.sh /root/PREBOOT.exe /root/bootutil.img
...
Unmounting temporary mount point /tmp/tmp_bootutil.img
Cleaning up temporary workspaces
Successfully created image file with BOOTUTIL64E.EFI
-rw-r--r--. 1 root root 5.0M Jul 20 17:52 /root/bootutil.img

[root@cologne-mgmt tools]#
[root@cologne-mgmt tools]# ./intel-bootutil-update.py --setupfile /root/openstack-configs/setup_data.yaml --
bootutil-image /root/bootutil.img --port 0 --state enable

All servers will be rebooted as part of PXE configuration, would you like to continue? <y|n> y
2018-07-18 18:34:36,697 INFO Enabling temporary HTTP server hosting BootUtil.img on 172.29.86.10
2018-07-18 18:34:36,790 INFO Successfully enabled temporary HTTP server hosting BootUtil.img on 172.29.86.10
...
2018-07-18 18:40:28,711 INFO Disabling temporary HTTP server hosting BootUtil.img on 172.29.86.10
2018-07-18 18:40:28,810 INFO Successfully disabled temporary HTTP server hosting BootUtil.img on 172.29.86.10
Server(s) successfully updated PXE configuration:
cologne-control-1,cologne-control-3,cologne-control-2,cologne-compute-1,cologne-compute-2,cologne-storage-1,
cologne-storage-3,cologne-storage-2
[root@cologne-mgmt tools]#
```

UCS B-Series Pod

Setting Up UCS B-Series Pod

After you install the RHEL OS on the management node, complete the following steps to configure a Cisco NFVI B-Series pod:

1. Log in to Cisco UCS Manager, connect to the console of both fabrics and execute the following commands:

```
# connect local-mgmt
# erase config*
All UCS configurations are erased and system starts to reboot. Are you sure? (yes/no): yes
Removing all the configuration. Please wait....
```

2. Go through the management connection and clustering wizards to configure Fabric A and Fabric B:

   a. Fabric Interconnect A

```
# connect local-mgmt
# erase config
Enter the configuration method. (console/gui) console
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin":
Confirm the password for "admin":
Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes
Enter the switch fabric (A/B) []: A
Enter the system name: skull-fabric
Physical Switch Mgmt0 IPv4 address : 10.30.119.58
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 10.30.119.1
Cluster IPv4 address : 10.30.119.60
Configure the DNS Server IPv4 address? (yes/no) [n]: y
DNS IPv4 address : 172.29.74.154
Configure the default domain name? (yes/no) [n]: y
Default domain name : ctocllab.cisco.com
Join centralized management environment (UCS Central)? (yes/no) [n]: n
Following configurations are applied:
Switch Fabric=A
System Name=skull-fabric
Enforced Strong Password=no
Physical Switch Mgmt0 IP Address=10.30.119.58
Physical Switch Mgmt0 IP Netmask=255.255.255.0
Default Gateway=10.30.119.1
DNS Server=172.29.74.154
Domain Name=ctocllab.cisco.com
Cluster Enabled=yes
Cluster IP Address=10.30.119.60
NOTE: Cluster IP is configured only after both Fabric Interconnects are initialized
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait..
```

   b. Fabric Interconnect B:

```
Enter the configuration method. (console/gui) ? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect is
added
to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric interconnect:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IP Address: 10.30.119.58
Peer Fabric interconnect Mgmt0 IP Netmask: 255.255.255.0
Cluster IP address : 10.30.119.60
Physical Switch Mgmt0 IPv4 address : 10.30.119.59
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.
```

3. Configure the NTP:
    a. In UCS Manager navigation area, click **Admin** tab.
    b. In the Filter drop-down list, choose **Time ZoneManagement**.
    c. In the main window under Actions, click **Add NTP Server**.
    d. In the Add NTP Server dialog box, enter the NTP hostname or IP address, then click **OK**.
4. Follow instructions in the Configuring Server Ports with the Internal Fabric Manager section of Cisco UCS Manager GUI Configuration Guide and configure the Fabric Interconnect A and Fabric Interconnect B uplinks to the Cisco NFVI ToR switches as **Uplink Ports**, **Server Ports**, and **Port C hannels**.
5. Configure the downlinks to the B-Series server chassis as **Server Ports**.
6. Acknowledge all chassis.

Out-of-Band Management Switch

Configuring Out-of-Band Management Switch

For Cisco VIM installer API and SSH bonded interface, use 1-GB Intel NICs that connect the Cisco NFVI management node and Cisco Catalyst switch. Following is a sample configuration for creating a port channel on a Catalyst switch. Modify the configuration for your environment:

```
interface GigabitEthernet0/39
channel-group 2 mode active speed 1000


interface GigabitEthernet0/40
channel-group 2 mode active speed 1000


interface Port-channel2 switchport
access vlan 165 switchport mode access
```

Third-Party Compute (HP DL 360 Gen9)

Support of Third-Party Compute (HP DL 360 Gen9)

Cisco VIM manages all aspects of the cloud through full automation, with no manual intervention beyond the initial infrastructure setup. To extend this approach to third-party computes, specifically HP DL360 Gen9, distribute the HP SmartArray Utility Tools as part of the platform offering.
To support third-party computes, perform the following steps:

1. Download the **ssacli** tool directly from HPE's website and place the RPM file in **/root/installer-<tagid>/openstack-configs/** directory.

   Cisco VIM supports ssacli-3.10-3.0.x86_64.rpm.

2. Location and checksum of the target RPM is: https://downloads.linux.hpe.com/SDR/repo/spp-gen9/RHEL/7/x86_64/2017.07.1/ssacli-3.10-3.0.x86_64.rpm SHA1 checksum: 51ef08cd972c8e65b6f904fd683bed8e40fce377

Remote Installation of Management Node

Installing the Management Node Remotely

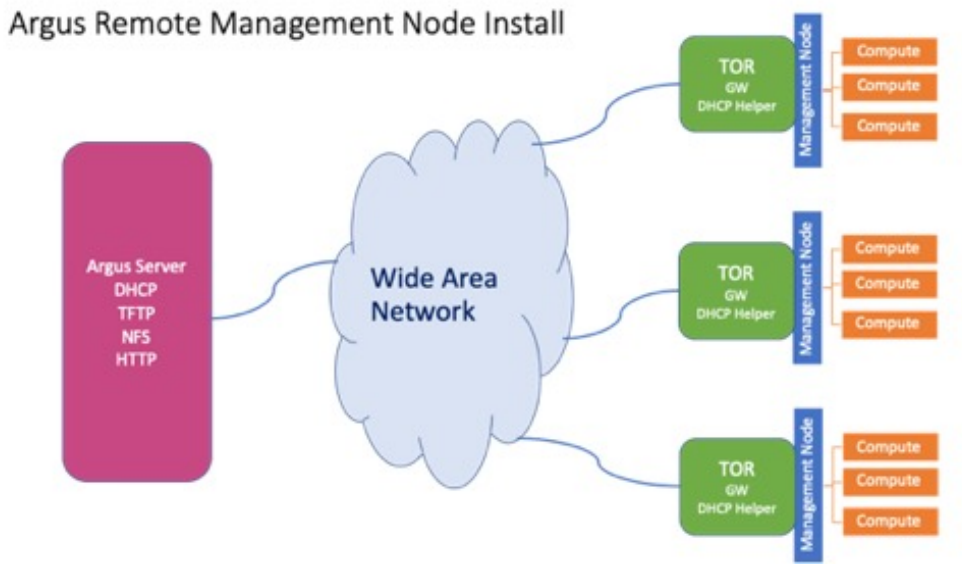
Overview

Overview of Remote Installation of Management Node

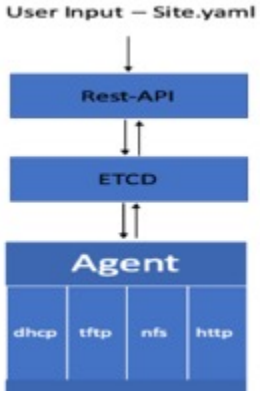
Cisco VIM fully automates the installation operation of the cloud. In releases prior to Cisco VIM 3.4.1, the management node installation was always manual. Using this feature, the management node, referred to as Cisco VIM Baremetal Manager is automatically installed over a Layer 3 network to accelerate the Cisco VIM installation process.

> ⚠ The term Cisco VIM Baremetal Manager and Remote Install of Management Node (RIMN) are used interchangeably.

Remote Installation of Management Node (RIMN) software is deployed on the RIMN deployment node from where one or more management nodes are installed. Cisco VIM Baremetal Manager or RIMN supports the remote installation of servers across WAN or LAN with either IPv4 or IPv6 connectivity. You can install Cisco VIM Baremetal Manager on the Cisco VIM Baremetal Manager deployment node by using air-gapped installation. After you install the RIMN software on its management node, you must define an input file for bare-metal config (in YAML format) and use Cisco VIM Baremetal Manager CLI or Rest API to deploy the user-specified ISO into the target platform (as depicted in the figure below):



RIMN solution is built based on the interaction of several components as depicted below:



- Rest-API and CLI: Pushes the received input data into Etcd datastore.
- Etcd datastore: Stores any stateful data related to sites, jobs, and flavor or policies used in the deployment.
- Agent: Golang-based services that installs the servers based on user config, and includes a controller with multiple services (TFTP, DHCP, HTTP, NFS)

Cisco VIM Baremetal Manager software is designed to be stateful, micro-service based, and easy to use.

Hardware Requirements

Hardware Requirements for RIMN

RIMN Cisco VIM Baremetal Manager solution consists of two hardware components:

1. Cisco VIM Baremetal Manager deployment server

   Cisco VIM Baremetal Manager service is deployed on the deployment server. It can be deployed on the standard Cisco VIM Management node BOM, which is based on UCS-C or Quanta hardware.
2. Servers to be deployed

   These are actual hardware to pxe-boot, install and configure that can include a number of clusters and a number of servers in each cluster. Cisco VIM Management node BOM (UCS-C M5, M4 and/or Quanta servers) are supported target servers. Supported firmware versions are Major =4.0 and Minor >= 1a.

From a component point of view, a typical Cisco VIM Management node BOM includes:

1. 8, 16 or 24 1.2 TB hard disks: Required to install the OS.
2. Intel 1G NIC (br_api) for PXE and 10/25/40G VIC or Intel NIC (for br_mgmt) NICs: Supports configuration of multiple bridges, and other minimum requirements to satisfy the server workload.
3. API availability for remote server management:

   a. Quanta: Redfish
   b. UCS-C: Redfish with UCS-C XML-API
4. Enabled pxeboot in UEFI mode for the chosen NIC (1g Intel NIC: br_api) for the target servers.

Network Requirements

Network Infrastructure Requirements for RIMN

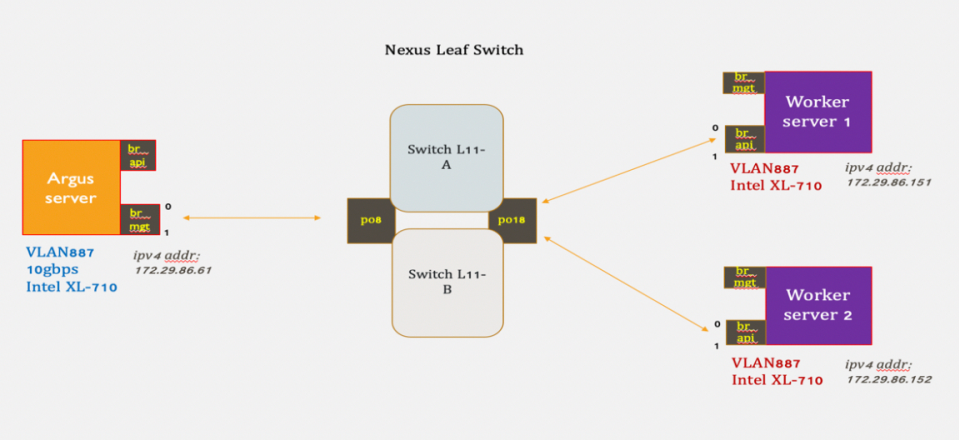
To install RIMN or Cisco VIM Baremetal Manager pxe-boots target nodes over layer 2 or layer 3 networks, the conditions for the solution feasibility are given below:

- The Cisco VIM Baremetal Manager server needs to have access to the remote management API interface (Redfish for Quanta, Redfish with XML-API for UCS-C) of the target nodes.
- The Cisco VIM Baremetal Manager server services (agent, including agent, TFTP, DHCP, HTTP, NFS ports) need to be reachable over a layer 2 or layer 3 IPv4 and IPv6 network from the target nodes.
- For layer 3-based installation, you must configure DHCP forwarder in the intermediate routing infrastructure so that the installed nodes can DHCP query the Cisco VIM Baremetal Manager server from its own network across WAN.
- For Edge deployment across WAN, DHCP Helper is configured on the network gateway of the management node API network to point out the Cisco VIM Baremetal Manager Agent IP for the DHCP server.
- WAN latencies for less than 500 milliseconds needs a successful install within a reasonable time period (< 30 mins). The higher the latency, the slower the installation and chances for installation failure.

Below are examples of topologies deployed with Cisco VIM Baremetal Manager on bare-metal servers over layer 2 and layer 3 networks respectively.

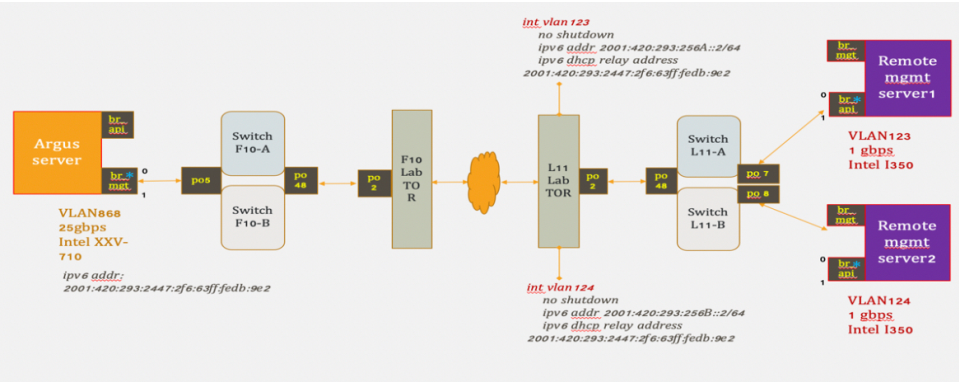
1. Target Server connected to RIMN over layer 2 and IPv4 network

   Here, the Cisco VIM Baremetal Manager server with agent running on br_mgmt using address 172.29.86.61 is pxe-booting two worker nodes on VLAN 887 on ip-address 172.29.86.151 and 172.29.86.152.



2. Target server connected to RIMN over Layer 3 IPv6 network

   Here, the Cisco VIM Baremetal Manager server with agent running on br_mgmt on address is pxe-booting two remote worker nodes on VLAN 123 and VLAN124 across WAN. DHCP forwarder is configured on VLAN 123 and 124 to forward DHCP request to the Cisco VIM Baremetal Manager server IP.



In either case, 1 or 2, a port-channel configured for installed server pxe-boot interface (for example po18 in case 1) looks like:

```
interface port-channel18
switchport access vlan 887
spanning-tree port type edge
no lacp suspend-individual
vpc 18
```

The following network ports are open on the Cisco VIM Baremetal Manager deployment server:

Network	Type	Port	Protocol	Application
Argus RMI API network	TCP	8141	HTTP	Cisco VIM Baremetal Manager REST-API
Argus RMI management network	TCP	24601	HTTP	Agent Asset Server
CVIM Management node API network	TCP	2049	NFS	Agent NFS Server
	UDP	67	DHCP4	Agent DHCPserver ipv4
	UDP	547	DHPCP6	Agent DHCP server ipv6
	UDP	69	TFTP	Agent tftp server

Workflow

Workflow for RIMN

The workflow for RIMN on Argus has the following steps:

1. Install the Cisco VIM Baremetal Manager management node server with the ISO.
2. Create the Cisco VIM Baremetal Manager setup data.
3. Bootstrap the Cisco VIM Baremetal Manager management server.
4. Import target ISO files and fetch the associated flavors.
5. Create baremetal files with flavor and target server details.
6. Deploy the target server.

RIMN REST API

Cisco VIM Baremetal Manager REST API

You can use the Cisco VIM Baremetal Manager REST API to manage RIMN. Cisco VIM Baremetal Manager provides a Representational State Transfer (REST) API that is used to deploy, expand, and manage RIMN.
The REST APIs perform the following actions:

- Provide a logical grouping of management nodes in the form of site, cluster, and nodes for better management of nodes globally.

```
site
`-- clusters
|-- cluster_0
|   `-- servers
|       |-- node_0.0
|       | .
|       | .
|       `-- node_0.n
| .
| .
|-- cluster_n
|   `-- servers
|       |-- node_n.0
|       | .
```

- Deploy a Cisco VIM Baremetal Manager site, cluster, and node
- Add cluster to the deployed site
- Delete cluster from the deployed site
- Add nodes to the deployed cluster
- Delete nodes from a deployed cluster
- Jobs to track deployment of site, cluster, and node

The Cisco VIM Baremetal Manager API security is provided by the Secure Sockets Layer (SSL) included on the Apache web server. The Flask-Restplus-based web application runs the Rest API server. The Flask REST API server requires a username and password to authorize the REST API server requests. Apache handles the authorization process to access the Flask web application. You can access API server on the br_api interface on port 8141. Authentication is enabled by default in the web service.

You can access the API endpoints of a version (v1 now) using the following URL format: https://<management_node_api_ip>:8141/v1

By default, basic authentication is enabled for the API endpoints in the management node. You can find the authentication credentials in the following file in the management node:
/opt/cisco/argus/rest_api/client_config.json

A sample configuration in the client_config.json file is given below:

```
{
"REST_API_URL": "https://172.22.191.134:8141",
"REST_API_USERNAME": "admin",
 "REST_API_PASSWORD": "8675d63674ff686e8688",
 "PODTYPE": "rmi"
}
```

Cisco VIM Baremetal Manager REST API is a Flask-Restplus-based web application that comes with Swagger integration. Swagger is built around OpenAPI specification that helps to design, build, document, and consume REST-APIs.

The REST-API resources along with their expected payloads and responses are documented by Swagger.

Server Installation

Installing RIMN Management Node On Servers

Installing Cisco VIM Baremetal Manager Management Node On UCS C-Series Server

The steps to install a Cisco VIM Baremetal Manager management node are similar to the steps in Management Node on UCS C-series (M4/M5). However, there are two major differences that are listed below:

In Step 11, choose the option to configure the server as a CVIM Baremetal node (Option 5).
Management (br_mgmt) interface must be routable as it serves as a host to the Cisco VIM Baremetal Manager Agent.
The routing ability of the API (br_api) interface depends on your choice. If the intention is to expose Cisco VIM Baremetal Manager REST API externally, br_api must be routable.

> ⚠ The default gateway in Cisco VIM Baremetal manager management node is through br_mgmt and not through br_api.

In the subsequent prompts, you can enter information such as the hostname, IPv4 or IPv6 addresses for br_api and br_mgmt interfaces and gateway addresses. Ensure you conform to the point 2 mentioned above while providing inputs), as per the procedure given in Management Node on UCS C-series (M4/M5).
The node is installed with RHEL with the following modifications:

- Security_Enhanced Linux (SELinux) is enabled on the management node for security.
- The Cisco VIM Baremetal code consists of packages with installer code. After provisioning the server with ISO, the installer code is placed in the following path:

```
/root/cvim_bm-<tag>
```

Installing Cisco VIM Baremetal Manager Management Node on Quanta Servers

For Quanta-based system, the CDC management node (CDC SKU1) is used as the Cisco VIM Baremetal manager management node. Please leave the settings in the quanta to its default.
The bootstrap procedure on the management node sets up Cisco VIM Baremetal manager/RIMN with its components REST API, CLI, Agent, and ETCD along with the needed data containers. It prepares the Cisco VIM Baremetal manager server for the actual site deployment.

Preparing Cisco VIM Baremetal Manager Management Node from Cisco VIM Software Hub Server

When you want to install the Cisco VIM Baremetal Manager node using the artifacts obtained from the Cisco VIM Software Hub server, you need to provide an additional parameter in the *setup_data.yaml* file. Ensure that the release artifacts are pre-installed on the Cisco VIM Software Hub server and that the *setup_data.yaml* file is populated with the pod details. Provide the registry FQDN name to enable installation through Cisco VIM Software Hub.

For example, your.domain.com.

```
REGISTRY_NAME: '<registry_name>' # Mandatory Parameter.
```

Cisco VIM Baremetal Manager node's *setup_data.yaml* requires the REGISTRY_USERNAME and REGISTRY_PASSWORD to connect to the docker registry and fetch docker images.

To fetch the docker images from Cisco VIM Software Hub node, provide the user credentials available in the SDS_READ_ONLY_USERS section of *sds_setup_data.yaml*. The details of an admin user with read or write access to docker registry are provided in SDS_REGISTRY_USERNAME and SDS_REGISTRY_PASSWORD field. Hence, ensure that you have a read-only user on Cisco VIM pod.

Argus Management Node

Preparing Argus Management Node for Air-gapped Install

If the Argus management node does not have internet access, use the prepared USB stick and complete the following steps:
To prepare the USB stick with Argus artifacts, see Preparing to Install Cisco NFVI on Management Nodes Without Internet Access

> ⚠ The only change in the *getartifacts* command is that --argus needs to be added to both download and retry commands.

1. Insert the USB stick into the management node drive after you install it with *buildnode.iso* having Cisco VIM Baremetal option.
2. Run the *import_artifacts.sh* script to copy all artifacts onto the management node, for example:

```
# cd ~/Cisco VIM_bm-<tag_id>/tools
# ./import_artifacts.sh
```

The installation artifacts are copied to */var/cisco/artifacts/* on the management node. Once the artifacts are available in the management node, the Argus server can be set up irrespective of the install mode (connected or disconnected).

RIMN Setup File

Creating RIMN Setup File

To create the RIMN *setup_data.yaml* file, perform the following steps:

```
#  cd Cisco VIM_bm-<tag-id>
#  cp openstack-configs/setup_data.yaml.Argus.EXAMPLE /root/openstack-configs/setup_data.yaml
```

You must change this example format as per your pod and use case. Argus also supports Cisco VIM Software hub (SDS) based installation. The setup data of Argus has multiple sections. Listed below are the snippets of the common section of the Argus *setup_data.yaml:*

```
setup_data.yaml
#############################################################################
#                      !! ARGUS SETUP CONFIGURATIONS !!                     #
#                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~                     #
# User Defined Configuration File
# Information in this file is specific to the user setup


#############################################################################
#                           REGISTRY INFORMATION                            #
#############################################################################
# Mandatory parameters
# Can be reconfigured, to point to SDS and back
REGISTRY_USERNAME: '<username>'
REGISTRY_PASSWORD: '<password>'

# Mandatory Parameter when SDS is enabled.
# Not required when SDS is not enabled.
# Example registry FQDN name [your.domain.com]
# Can be reconfigured, to point to SDS and back
REGISTRY_NAME: '<registry_name>'

#############################################################################
#                            INSTALLATION MODE                              #
#############################################################################
# Optional parameter
# Valid options:
#  a) connected (default): Node has connectivity to https://cvim-registry.com
#
#  b) disconnected: Node had NO connectivity to https://cvim-registry.com
#     Refer to CISCO VIM Install Guide for details on disconnected install
#     Chapter 5: Installing Management Node Remotely
#     Section: Preparing the Argus Management Node in an Air-gapped Install
INSTALL_MODE: connected

#############################################################################
#                             POD INFORMATION                               #
#############################################################################
# Mandatory parameter, must be set to 'rmi' (only option for now)
# rmi -> Remote Management Install
PODTYPE: 'rmi'

#############################################################################
#                           NETWORKING INFORMATION                          #
#############################################################################
# Optional, valid options are 'v4' (default) and 'v6'.
# This parameter determines whether the CVIM pods going to be deployed via
# RMI the will use IPv6 or IPv4 addresses.
# Mixing IPv4 and IPv6 (CVIM pods) is not supported for now.
DHCP_MODE: 'v4'

# Optional, needed if the pod is behind a proxy
# Name of the proxy server without 'https://'
# Not required for INSTALL_MODE: disconnected
https_proxy_server: '<proxy.domain.com:8080>'
#############################################################################
```

RIMN Server Setup

Setting up RIMN Management Server

1. Set up the Cisco VIM Baremetal Manager management server infrastructure including the REST-API and CLI.

```
# cd ~/Cisco VIM_bm-<tag-id>;
# ./argus/argus_runner.py --list
** ARGUS **
* CISCO'S BAREMETAL ORCHESTRATOR *
==================================
+--------------------+--------------+
| Operations | Operation ID |
+--------------------+--------------+
| INPUT_VALIDATION | 1 |
| BOOTSTRAP_INFRA | 2 |
+--------------------+--------------+
# ./argus/argus_runner.py -p 1,2
Perform steps ['1']. Continue (Y/N) y
```

2. Perform hardware validations to check if the deployment node is Cisco compliant BOM and validations on user-passed *setup_data.yaml.*
3. Run Ansible playbooks and deploy docker containers namely argus_rest_api_<tag-id>, argus_agent_<tag_id>, argus_etcd_<tag_id>, and CISCO VIM data containers.
4. Install a CLI to Argus Baremetal REST-API.

Target Server Deployment

Deploying Target Servers over Layer 2 and Layer 3

You can deploy the remote servers after the Cisco VIM Baremetal Manager or RIMN server installation.

Cisco VIM Baremetal Manager CLI Helper

```
# argus -h

usage: argus [-h] [--json] [--debug] <subcommand> ...
Command-line interface to the Argus Baremetal Installer

positional arguments:
<subcommand>
baremetal   Perform baremetal operations
job              Perform job operations
flavor            Perform flavor operations iso Perform ISO operations

optional arguments:

-h, --help    show this help message and exit
--json        Get output in json format
--debug       Print debugging output
-y,--yes     Option to skip steps without prompt
```

Import ISOs to Argus

You must download the Cisco-provided ISO file to the Argus management node before starting the server deployment. The ISO file creates a unique flavor for Cisco VIM Baremetal Manager Agent that is then used to decide the base of networking, boot, and OS for new servers.

```
# argus iso -h

usage: argus iso [-h] -a action [-f config_file] [-n name]

optional arguments:
-h,--help              show this help message and exit
-a action              list    - List all ISOs
                                show    -  Show ISO details
                                import -   Import an ISO on the management node
                                delete -   Delete ISO
-f config_file Path of an ISO file
-n name         ISO name

# argus iso -a import -f buildnode-internal-18173.iso -n my_argus-iso

+--------+--------+-------------------+
| Action | Status |      Flavor       |
+--------+--------+-------------------+
| Import |  PASS  | my_argus-iso-18173|
+--------+--------+-------------------+
```

The above command can be used multiple times to import different ISO files. Verify the ISO and the corresponding flavor:

```
# argus iso -a list
List of Isos:
+--------+--------------+
| SL.NO. |     Isos     |
+--------+--------------+
| 1      | my_argus-iso |
+--------+--------------+
# argus iso -a show -n master_20928

ISO Details:
+------------------------------+--------------------+
|          File Name           |       Flavor       |
+------------------------------+--------------------+
| buildnode-internal-18173.iso | my_argus-iso-18173 |
+------------------------------+--------------------+
```

The ISO import creates flavors that define the nature of the server. A flavor is specifically tied to the ISO file imported. You can verify the flavors that are created from the ISO import operations explained above:

```
# argus flavor -a list
List of Flavors:
+--------+--------------------+
| SL.NO. |     Flavors        |
+--------+--------------------+
| 1      | my_argus-iso-18173 |
+--------+--------------------+

[root@argus-mgmt ~]# argus flavor -a show -n my_argus-iso-18173

Flavor Details:
+-------------------+-------------------+-----------------+---------------+------------------+-----------+
|        Name       |      Workflow     |  OS Policies    | Disk Policies | Network Policies | Boot Mode |
+-------------------+-------------------+-----------------+---------------+------------------+-----------+
| my_argus-iso-18173| my_argus-iso-18173| huge-pages-1g   |   disk-sriov  |    management    |    uefi   |
|                   |                   |                 |               |       api        |           |
+-------------------+-------------------+-----------------+---------------+------------------+-----------+
```

The above-mentioned created flavors must be used in the *site/cluster/node* configuration during server deployment.

```
* Flavor can be defined either in common or server level, as a single flavor can be used with multiple severs
clusters:
...
servers:
        - name: server-1
        flavor: my_argus-iso-18173
[OR]
common_info:
flavor: my_argus-iso-18173
```

Deploy the Site

To help deploy the target nodes, the next step is to create the site configuration data file. To deploy the site, execute the following:

```
# cp openstack-configs/argus_baremetal.EXAMPLE   /root/argus_baremetal.yaml
```

Cisco VIM Baremetal Manager Site Configuration

Listed below is an example of the Cisco VIM Baremetal Manager site config data to deploy the target server. You must make changes to this example format as per your use case:

```
# Cisco VIM Baremetal Manager CONFIGURATIONS:
```

```
# ARGUS BAREMETAL CONFIGURATIONS:
#*******************************
# User defined Baremetal configuration file, information specific to user setup

# Structure: Logical grouping of nodes to form a cluster and similar grouping of
# clusters to form a site.

# site
# `-- clusters
#     |-- cluster_0
#     |   `-- servers
#     |       |-- node_0.0
#     |       | .
#     |       | .
#     |       `-- node_0.n
#     | .
#     | .
#     |-- cluster_n
#     |   `-- servers
#     |       |-- node_n.0
#     |       | .
#     |       | .
#     |       `-- node_n.n
#     `-- common_info
# REQUIREMENTS AND CRITERIA:
#***************************
# Do not put values in this section; its just a explanatory section
# referencing to validations of keys used in Section 1 and 2

# Some validations for critical keys have been listed here:
##-------------------------------------------------------------------------
## 1. oob_password: BMC/CIMC PASSWORD                                     |
##-------------------------------------------------------------------------
## Applies for both UCS-C and Quanta BMC
## Passwords should satisfy at least 3 of the following conditions:
##     a. at least 1 letter between a to z
##     b. at least 1 letter between A to Z
##     c. at least 1 number between 0 to 9
##     d. at least 1 character from !$@%^-_+=
## AND
##     e. No space allowed
##     f. 8<= Length <=20

## 2. name: RESOURCE NAME (SITE/CLUSTER/NODE)                             |
##-------------------------------------------------------------------------
## Resource names should satisfy following criteria:
##     a. Required
##     b. Unique
##     c. ASCII chars
##     d. No space allowed
##     e. 1 <= Length <=32

## 3. info: RESOURCE INFORMATION (SITE/CLUSTER)                           |
##-------------------------------------------------------------------------
## Resource info keys should satisfy the following criteria:
##     a. Required
##     b. ASCII chars
##     c. 1 <= Length <=50

## 4. boot_network: SERVER'S BOOT NETWORK                                 |
##-------------------------------------------------------------------------
## Server's boot network holds following criteria:
##     a. Optional, defaults to:
##        -> management_*_v4: if Agent running on DHCP_MODE: v4
##        -> management_*_v6: if v6 management interface defined in
##                            server's ip_address section and Agent
##                            running on DHCP_MODE: v6
##     b. Should follow <api|management>_*_<v4|v6> pattern
##
##  * - Interface Representation Number
```

```
## 5. ip_address: SERVER'S NETWORKING INTERFACES AND CONFIGS           |
##-------------------------------------------------------------------
## api_*_v4 --> br_api, ipv4; api_*_v6 --> br_api, ipv6
## management_*_v4 --> br_mgmt, ipv4; management_*_v6 --> br_mgmt, ipv6
##
## Networking Interface(s) dictionary of the server to be deployed
## Dict should satisfy the following criteria:
##     a. Pattern of Keys:
##        # Should follow <api|management>_*_<v4|v6> OR
##                        <api|management>_*_gateway_<v4|v6> pattern
##        # Representation number: * of all interfaces should match
##
##     b. Mandatory Keys:
##        -> api_*_v4, api_*_gateway_v4
##        -> management_*_v4
##
##     c. Optional Keys:
##        -> management_*_gateway_v4
##        -> management_*_gateway_v6
##        # Any 1 of the below 3 keys defined, makes others mandatory
##        -> api_*_v6, api_*_gateway_v6
##        -> management_*_v6
##
##     d. Interfaces:
##        # Different interfaces should NOT share a common network
##        # Interfaces should be in valid v4 or v6 CIDR format
##        -> api_*_v4, api_*_v6
##        -> management_*_v4, management_*_v6
##
##     e. Gateways:
##        # Gateways should have a valid v4 or v6 IP
##        # IP should be in the respective interface network
##        -> api_*_gateway_v4, api_*_gateway_v6
##        -> management_*_gateway_v4, management_*_gateway_v6
##
##  -> No duplicate values allowed
##
##  * - Interface Representation Number                              |
## ------------------------------------------------------------------

## Representation number: The one which defines an interface's uniqueness
##         ( * )          Eg. '2' in case of api_2_v4
## ------------------------------------------------------------------

# SECTION 1. SITE INFORMATION AND COMMON CONFIGS:
#***********************************************

name: <overall_site_name>
info: <site_description>

# Required
common_info:
    # Required, common username for multiple BMC/CIMC
    # Can be overridden at server level
    oob_username: <oob_username>

    # Required, common password for multiple BMC/CIMC
    # Can be overridden at server level
    oob_password: <oob_password>

    # Required, time zone to be configured for node(s)
    # Daylight saving time not supported
    time_zone: <UTC or US/Pacific, etc>

    # Required
    domain_name: <your.domain.com>

    # Required, max of 3
    # Can be overridden in server level
    domain_name_servers:
      - <8.8.8.8>
```

```
    # OR
    domain_name_servers: [171.70.168.183, 173.36.131.10]

    # Required
    ntp_servers:
      - <1.pool.ntp.org>
    # OR
    ntp_servers: [ ntp.cisco.com, time.apple.com ]

    # Required, common flavor for each node
    # Forms the base of OS, Boot and Networking
    # Should be created by ISO import previous to deploy
    # Can be overridden at server level
    flavor: my_argus-iso-18173

    # Required, should start with $6
    # Run python script argus_password_hash.py in cvim_bm-<tag-id>/tools
    # to generate it from the plaintext.
    # Can be overridden at server level
    password_hash: <password hash>

    # Optional
    # Provided SSH key file should contain SSH public key of the node from
    # which password less SSH to all the deploy servers would be enabled.
    # By default password less SSH from the RMI management node will be enabled.
    # Providing a value here will disable the default behaviour as only one
    # public key mapping is supported for now.
    # Can be overridden at server level.
    ssh_key_file: <path_to_ssh_public_key_file>

# SECTION 2. CLUSTER(S) INFORMATION AND SERVER(S) NETWORKING CONFIGS:
#**********************************************************************

# Required, at least 1
clusters:
  - name: <cluster_name>
    info: <cluster_description>

    # Required, at least 1
    servers:
      - name: <target_server_name>

        # Required, BMC/CIMC IP of target server
        # IPv4 or v6
        oob_ip: 2001:420:293:2469:DAC4:97FF:FEE9:2D51

        # Optional, defaults to value in common_info
        oob_username: admin

        # Optional, defaults to value in common_info
        oob_password: *********

        # Optional, defaults to value in common_info
        # Should be created by ISO import, previous to the deploy
        flavor: my_argus-iso-26073

        # Optional, defaults to value in common_info; should start with $6
        # Run python script argus_password_hash.py in cvim_bm-<tag-id>/tools
        # to generate it from the plaintext.
        password_hash: <password hash>

        # Optional, defaults to value in common_info
        # Max of 3
        domain_name_servers: [171.70.168.183, 173.36.131.10]

        # Optional, defaults to value in common_info
        # Provided SSH key file should contain SSH public key of the node from
        # which password less SSH to this server would be enabled.
        # No entry in either common_info or here will enable password less SSH
        # from the RMI management node.
        ssh_key_file: <path_to_ssh_public_key_file>
```

```
        # ###################################################################
        # Server's Interface(s) example configs
        # Please refer validations mentioned in Requirements Section: 4 & 5
        # ###################################################################
        boot_network: api_1_v6

        # Required
        ip_address:
          api_1_v4: 10.30.117.248/28
          api_1_gateway_v4: 10.30.117.241
          api_1_v6: 2001:420:293:256a::1248/64
          api_1_gateway_v6: 2001:420:293:256a::2
          management_1_v4: 20.20.30.248/25
          management_1_gateway_v4: 20.20.30.1
          management_1_v6:  2001:420:293:2447:2f6:63ff:fedb:9e2/64
          management_1_gateway_v6:2001:420:293:2447::2

      - name: node-2
        oob_ip: 2001:420:293:2469:DAC4:97FF:FEE8:9690
        ip_address:
          api_2_v4: 10.30.117.246/28
          api_2_gateway_v4: 10.30.117.241
          management_2_v4: 20.20.30.248/25

##############################################################################
```


The information in the common sections is shared across all target servers in the cluster. However, you can overwrite it on a per-server basis. For example, flavor, oob username or password, passwpord_hash, domain_name_servers can be defined as per server level.

The password is an encrypted string from a plain text password. You can run the python script *argus_password_hash.py* in *Cisco VIM_bm-<tag-id>/tools* to generate it from the plaintext. The ssh_key is a public SSH key for a host, and if provided, you can automatically get authenticated and SSH into the deployed nodes after installation without a password. You can generate the public or private key pair using the command below:

Baremetal CLI Helper

```
[root@argus-mgmt~]# argus baremetal -h
usage: argus baremetal [-h] -a action [-f config_file] [-n name] [--status]

optional arguments:
        -h, --help      show this help message and exit
        -a action       list           - List site/cluster/node
                                         show           - Show details of a site/cluster/node
                                         fetch-config   - Fetch site yaml config
                                         deploy         - Create and deploy a site
                                         deploy-cluster - Add and deploy a cluster
                                         deploy-node    - Add and deploy a node
                                         delete         - Delete a site
                                         delete-cluster - Delete a cluster
                                         delete-node    - Delete a node
        -f config_file  Path of argus config-file
         -d dump_dir     Path of directory to dump site config yaml file
        -n name         Name of site/cluster/node on which operation is to be performed.
        --status        Get status of site/cluster
                                         Use this argument with 'show' action.
To start server deploy, the user needs to pass the above-created site config data to the Argus CLI with the
appropriate parser and
action.

# argus baremetal -a deploy -f /root/argus_baremetal.yaml

Performing this step will boot and deploy the server(s) with the provided flavor.

Do you want to continue?(Y/N)

+--------+--------+---------------+-----------------------------------------------+|
Action    | Status | Resource Name |                    Details                    |
```

```
+--------+--------+---------------+-------------------------------------------------+
| Deploy |  PASS  |  myimage-rms  | job_uuid:943c1a82-cfdb-4281-a655-d56eb9ce7318  |
|                 |                                        status: ToRun                        |
+--------+--------+---------------+-------------------------------------------------+
```

A job is created to deploy the site with UUID shown above. One can query its status as shown below:

```
# argus job -a show -u 943c1a82-cfdb-4281-a655-d56eb9ce7318

Job Details:

+----------------------+----------+----------+----------------+----------------------+------------------+------------
+--------+-------+-----+----+
|Description  | Stage   |  Status  |Created_at      |  Started_at          | Updated_at       | Aborted_at
|Command |Versio |Error|Log |
+-------------+---------+----------+----------------+----------------------+----------------------+--------
+--------+-------+-----+----+
|deploy site: | workflow| Running  |2019-07-29      |     2019-07-29       |2019-07-29        |   N.A      |
deploy |   v1  | N.A |N.A |
|myimage-rms  |         |          |10:24:20.326375 |17:24:20.684958544    |17:25:54.462980001|
|        |       |     |    |
|             |         |          |                |  +0000 UTC           |      +0000 UTC   |
|        |       |     |    |
+-------------+---------+----------+----------------+----------------------+------------------+------------
+--------+-------------------
```

Task Details:

```
+--------------------------------+----------+---------+--------------------------------
+--------------------------------+----------+-------
|             Server             | Stage    |  Status |           Started_at           |
Updated_at                    | Command | Error
+--------------------------------+----------+---------+--------------------------------
+--------------------------------+----------+-------
| myimage-rms/cluster-quanta-    | workflow | Running | 2019-07-29 17:24:20.976062896  | 2019-07-29 17:25:
29.424103923  | deploy  |  N.A |
|            rms/qr1            |          |         |           +0000 UTC            |           +0000
UTC            |         |
+--------------------------------+----------+---------+--------------------------------
+--------------------------------+----------+-------
| myimage-rms/cluster-quanta-    | workflow | Running | 2019-07-29 17:24:21.033556299  | 2019-07-29 17:25:
36.094923735  |  deploy | N.A  |
|            rms/qr2            |          |         |           +0000 UTC            |           +0000
UTC            |         |
+--------------------------------+----------+---------+--------------------------------
+--------------------------------+----------+-------
| myimage-rms/cluster-quanta-    | workflow | Running | 2019-07-29 17:24:21.034453335  | 2019-07-29 17:25:
44.136601455  | deploy  | N.A  |
|            rms/qr3            |          |         |           +0000 UTC            |           +0000
UTC            |         |
+--------------------------------+----------+---------+--------------------------------
+--------------------------------+----------+-------
```

If the site is already deployed,irrespective of its status (DeploySuccess or DeployFailed) above command will request Argus to re-deploy all the servers again.

NOTE: Please use re-deploy with caution.

To list all jobs, or fetch job(s) with particular status.

```
[root@africainstaller]# argus job -a list
List of Jobs:
-------------------------------------------------------------------------------------------------------------------------
-------------------------
|             Job uuid              |                  Description               |
Updated_at              |Stage   |Status
+-----------------------------------+--------------------------------------------
+-----------------------------------+--------+-------
```

```
|ed93738c-311b-4090-8db1-c9d9c1941d4 |         deploy site: myimage-rms             |2019-08-01 03:40:28.357371
+0000UTC |workflow|Success
|520335b8-dead-4d1b-b5a8-ce3a8c979fa |deploy cluster: myimage-rms/cluster-quanta-rms|2019-08-01 03:42:27.738706
+0000 UT |workflow|Failed
|04dcb381-4702-45de-a101-7ab178c46bd4|delete node: myimage-rms/cluster-quanta-rms/qr|2019-08-01 03:43:32.451262
+0000 TU |workflow|Running
+--------------------------------------+----------------------------------------------
+--------------------------------------+--------+--------

[root@africainstaller]# argus job -a list --failed

List of Jobs:

+--------------------------------------+----------------------------------------------
+--------------------------------------+--------+--------
|               Job uuid               |                 Description                  |
Updated_at                  | Stage  |Status
+--------------------------------------+----------------------------------------------
+--------------------------------------+--------+--------
|520335b8-dead-4d1b-b5a8-ce3a8c979fa8 |deploy cluster: myimage-rms/cluster-quanta-rms |2019-08-01 03:42:
27.738706 +0000 U |workflow| Failed
+--------------------------------------+----------------------------------------------
+--------------------------------------+--------+--------

[root@africainstaller]# argus job -a list --success

List of Jobs:

+--------------------------------------+---------------------------------
+--------------------------------------+---------+--------+
|              Job uuid                |        Description               |
Updated_at                        | Stage   | Status |
+--------------------------------------+---------------------------------
+--------------------------------------+---------+--------+
| ed93738c-311b-4090-8db1-c9d9c1941d44 |        deploy site: myimage-     | 2019-08-01 03:40:28.357371
+0000UTC  | workflow| Success|
+--------------------------------------+-------------------------------------------------
+-----------------------------------------+

[root@africainstaller]# argus job -a list --running

List of Jobs:

+--------------------------------------+----------------------------------------------
+--------------------------------------+---------+-------
|               Job uuid               |                 Description                  |
Updated_at               |Stage    |Status
+--------------------------------------+----------------------------------------------
+--------------------------------------+---------+-------
|04dcb381-4702-45de-a101-7ab178c46bd4  |delete node: myimage-rms/cluster-quanta-rms/qr|2019-08-01 03:43:
32.451262 +0000 TUC  |workflow |Running
+--------------------------------------+-------------------------------------------------
+--------------------------------------+---------+--------

To check the site details:

# argus baremetal -a show -n myimage-rms

Site Details:
+-------------+-----------------------------------------+-------------+-----------------------+---------------+
|     Name    |                  Info                   | Domain Name | Domain NameServer(s)  | NTP Server(s) |
+-------------+-----------------------------------------+-------------+-----------------------+---------------+
|myimage-rms  | Quanta MyImage remote management servers |  cisco.com  |    173.36.131.10      | ntp.cisco.com |
|             |                                         |             |    171.70.168.183     |               |
+-------------+-----------------------------------------+-------------+-----------------------+---------------+

Cluster(s) Node(s) Details:

+------------------+------+--------+-------------------------------------------------+--------------------
+---------------------------------
| Cluster(s)       |  Info| Node(s)|               IP Address           | Flavor          |
```

```
OOB IP           |OOB

Username
+--------------------+-------------+---------+----------------------------------------+--------------------
+---------------------------------
|                    |      |  qr1   |         api_1_v4: 10.30.117.244     |myimage-iso-18173|2001:420:293:2469:
DAC4:97FF:FEE9:2D51|admin
|                    |      |        |   api_1_v6: 2001:420:293:248b::1245
|                    |      |        |management_1_v6:2001:420:293:148b::245|
|                    |      |        |      management_1_v4: 20.20.0.245
|cluster-quanta-rms|test   |  qr2   |      management_2_v4: 20.20.10.246   |myimage-iso-18173|2001:420:293:2469:
DAC4:97FF:FEE9:336E|admin
|                    |      |        |management_2_v6: 2001:420:293:148c::24
|                    |      |        |         api_2_v4: 10.30.117.245      |
|                    |      |        |   api_2_v6: 2001:420:293:248c::1246
|                    |
|                    |      |  qr3   |management_3_v6:2001:420:293:2461::248|myimage-iso-18173|2001:420:293:2469:
DAC4:97FF:FEE8:9690 |admin
                                                                                                    management_3_v4:
20.20.30.248      |
                                                                                                api_3_v6: 2001:420:293:256a::
1248
|                    |       |       |         api_3_v4: 10.30.117.246       |
+--------------------+-------------+---------+----------------------------------------+--------------------
+-----------------------------------

Networking Details:

+------------------+------------------------+----------------------+
|    Interface     |         Subnet         |       Gateway        |
+------------------+------------------------+----------------------+
|     api_1_v4     |     10.30.117.0/28     |    10.30.117.241     |
|                  |                        |                      |
|     api_1_v6     |2001:420:293:248b::/64  | 2001:420:293:248b::2 |
|                  |                        |                      |
|     api_2_v4     |     10.30.117.0/28     |    10.30.117.241     |
|     api_2_v6     |2001:420:293:248c::/64  | 2001:420:293:248c::2 |
|                  |                        |                      |
|     api_3_v4     |     10.30.117.0/28     |    10.30.117.241     |
|     api_3_v6     |2001:420:293:256a::/64  | 2001:420:293:256a::2 |
| management_1_v4  |      20.20.0.0/25      |         N.A          |
|                  |                        |                      |
|management_1_v6   | 2001:420:293:148b::/64 |         N.A          |
|                  |                        |                      |
| management_2_v4  |     20.20.10.0/25      |         N.A          |
|                  |                        |                      |
|management_2_v6   | 2001:420:293:148c::/64 |         N.A          |
| management_3_v4  |     20.20.30.0/25      |         N.A          |
|management_3_v6   | 2001:420:293:2461::/64 |         N.A          |
+------------------+------------------------+----------------------+

Site Status Details:
+--------------------+---------+--------------------+--------------------+--------------------+
|    Cluster(s)      | Node(s) |    Node Status     |  Cluster Status    |    Site Status     |
+--------------------+---------+--------------------+--------------------+--------------------+
|                    |   qr1   |     Deploying      |                    |                    |
| cluster-quanta-rms |   qr2   |     Deploying      |      Deploying.    |      Deploying     |
|                    |   qr3   |     Deploying      |                    |                    |
+--------------------+---------+--------------------+--------------------+--------------------


The above command can also be used to get details for a specific cluster:
# argus baremetal -a show -n myimage_argusrakuten-rms/cluster-quanta-rms

Cluster Node(s) Details:
+-----------+---------+-----------------------------------------+--------------------
+---------------------------------------+--------------
|    Info   | Node(s) |                IP Address               |       Flavor       |                 OOB
IP                | OOB Username
+-----------+---------+-----------------------------------------+--------------------
+---------------------------------------+--------------
```

```
|           |   qr1   |        api_1_v4: 10.30.117.244          | myimage-iso-18173  | 2001:420:293:2469:DAC4:
97FF:FEE9:2D51 .  admin      |
|                      api_1_v6: 2001:420:293:248b::1245        |
|                                  |
|                     | management_1_v6: 2001:420:293:148b::245
|           |         |       management_1_v4: 20.20.0.245      |
|
|test quanta|  qr2    |      management_2_v4: 20.20.10.246       | myimage-iso-18173  |2001:420:293:2469:DAC4:
97FF:FEE9:336E  |   admin     |
                        |         | management_2_v6:2001:420:293:148c::246  |
|           |         |         api_2_v4: 10.30.117.245          |
|           |         |    api_2_v6: 2001:420:293:248c::1246     |                     |

|           |   qr3   | management_3_v6: 2001:420:293:2461::248 | myimage-iso-18173  | 2001:420:293:2469:DAC4:
97FF:FEE8:9690 |    admin    |
            |         |      management_3_v4:20.20.30.248        |                     |
                        api_3_v6: 2001:420:293:256a::1248      |
|           |         |         api_3_v4: 10.30.117.246          |
+-----------+---------+------------------------------------------+--------------------
+--------------------------------------+---------------
```

Cluster Status Details:

```
+---------+--------------------+--------------------+
| Node(s) |    Node Status     |   Cluster Status   |
+---------+--------------------+--------------------+
|   qr1   |     Deploying      |                    |
|   qr2   |     Deploying      |      Deploying     |
|   qr3   |     Deploying.     |                    |
+---------+--------------------+--------------------+
```

And also for a particular server:

```
# argus baremetal -a show -n myimage-rms/cluster-quanta-rms/qr1
```

Node Details:

```
+----------------------------------------+--------------------+--------------------------------------
+--------------+--------------------+
|                IP Address              |       Flavor       |                OOB IP                | OOB
Username |       Status       |
+----------------------------------------+--------------------+--------------------------------------
+--------------+--------------------+
|         api_1_v4: 10.30.117.244         | myimage-iso-18173  | 2001:420:293:2469:DAC4:97FF:FEE9:2D51 |
admin     |    Deploying       |
|    api_1_v6: 2001:420:293:248b::1245    |                    |
|              |                      |
| management_1_v6: 2001:420:293:148b::245 |                    |
|              |                      |
|       management_1_v4: 20.20.0.245      |                    |
|              |                      |
+----------------------------------------+--------------------+--------------------------------------
+--------------+--------------------+
```

The show command can also be used to get only status of the site with -status

```
# argus baremetal -a show -n myimage-rms -status
```

Site Status Details:

```
+--------------------+---------+--------------------+--------------------+--------------------+
|     Cluster(s)     | Node(s) |    Node Status     |   Cluster Status   |    Site Status     |
+--------------------+---------+--------------------+--------------------+--------------------+
|                    |   qr1   |    Deploying       |                    |                    |
| cluster-quanta-rms |   qr2   |    Deploying       |   Deploying        |    Deploying       |
|                    |   qr3   |    Deploying       |                    |                    |
+--------------------+---------+--------------------+--------------------+--------------------+
```

And also to get the status of a particular cluster

```
# argus baremetal -a show -n myimage-rms/cluster-quanta-rms -status
```

Cluster Status Details:

```
+---------+--------------------+--------------------+
| Node(s) |    Node Status     |   Cluster Status   |
```

```
+---------+--------------------+--------------------+
|   qr1   |    Deploying       |                    |
|   qr2   |    Deploying       |      Deploying     |
|   qr3   |    Deploying       |                    |
+---------+--------------------+--------------------+
Users can also abort the above job if required:
NOTE: Only deploy jobs can be aborted, not delete ones.

# argus job -a abort -u 943c1a82-cfdb-4281-a655-d56eb9ce7318
Performing this step will abort the ongoing deploy.
Do you want to continue?(Y/N)

+--------+--------+-------------------------------------------+
| Action | Status |                 Details                   |
+--------+--------+-------------------------------------------+
| Abort  |  PASS  | Abort job request accepted. Please Wait!! |
+--------+--------+-------------------------------------------+
```

All the above Argus CLI commands can be used with:

- --json: Prints the REST-API response in json format instead of tables
- --debug: Prints the CLI call as a CURL command, its relative logs along with the REST-API response
- Use –json and –debug together to achieve a collective behavior.

Delete the Site

The above-created site can be deleted as per user's choice, which is nothing but a power-off of all the servers and removal of their respective data from ETCD datastore.

```
Performing this step will power-off the server(s) and delete the site from Argus.

Do you want to continue?(Y/N)

[root@argus-mgmt ~]# argus baremetal -a delete -n my_argus-rms
+--------+--------+--------------------------------------------------+
| Action | Status |                    Details                       |
+--------+--------+--------------------------------------------------+
| Delete |  PASS  | job_uuid: ef648d52-20eb-49d7-b16d-b84cb52eae66 |
|        |        |                 status: ToRun                    |
+--------+--------+--------------------------------------------------+
```

Deploy Cluster

You can add a new cluster to a deployed site using the modified baremetal file that was used with the site deploy. You need to add the new cluster info in the baremetal file and pass that to the Argus CLI.

```
# vim /root/argus_baremetal.yaml
  Add the new node info under 'clusters-> <cluster_name> -> servers' key and save.
# argus baremetal -a deploy-cluster -n cluster-rakuten-bms/qr3 -f /root/argus_baremetal.yaml
Performing this step will boot and deploy the server(s) with the provided flavor.
Do you want to continue?(Y/N)

+--------+--------+-----------------------------------+-------------------------------------------------+
| Action | Status |            Resource Name          |                    Details                      |
+--------+--------+-----------------------------------+-------------------------------------------------+
| Deploy |  PASS  | myimage-rms/cluster-quanta-bms/qr3 | job_uuid: 943c1a82-cfdb-4281-a655-d56eb9ce7318 |
|        |        |                                   |                 status: ToRun                   |
+--------+--------+-----------------------------------+-------------------------------------------------+

If the node is already deployed, irrespective of its status (DeploySuccess or DeployFailed) above command will
request Argus to re-deploy the server again.
NOTE: Please use re-deploy with caution.
```

Delete Cluster

Similar to site delete, you can delete a cluster which will again power-off all the servers present in that cluster and delete the server's entry from the ETCD datastore.

```
[root@argus-mgmt ~]# argus baremetal -a delete-cluster -n my_argus-rms/cluster-quanta-bms
+--------+--------+-------------------------------------------------+
| Action | Status |                    Details                      |
+--------+--------+-------------------------------------------------+
| Delete |  PASS  | job_uuid: ef648d52-20eb-49d7-b16d-b84cb52eae66 |
|        |        |                 status: ToRun                   |
+--------+--------+-------------------------------------------------+
```

Deploy Node

A new node can be added to a deployed cluster using the modified bare-metal file. You need to add the new node info in the desired cluster in the baremetal file and pass that to the Argus CLI.

```
# vim /root/argus_baremetal.yaml
  Add the new node info under 'clusters-> <cluster_name> -> servers' key and save.
# argus baremetal -a deploy-node -n cluster-rakuten-bms/qr3 -f /root/argus_baremetal.yaml
Performing this step will boot and deploy the server(s) with the provided flavor.
Do you want to continue?(Y/N)

+--------+--------+-----------------------------------+-------------------------------------------------+
| Action | Status |           Resource Name           |                    Details                      |
+--------+--------+-----------------------------------+-------------------------------------------------+
| Deploy |  PASS  | myimage-rms/cluster-quanta-bms/qr3 | job_uuid: 943c1a82-cfdb-4281-a655-d56eb9ce7318 |
|        |        |                                   |                 status: ToRun                   |
+--------+--------+-----------------------------------+-------------------------------------------------+

If the node is already deployed, irrespective of its status (DeploySuccess or DeployFailed) above command will
request Argus to re-deploy the server again.
NOTE: Please use re-deploy with caution.
```

Delete Node

When you delete a node, it is powered off and the server's entry from the ETCD datastore is deleted.

```
[root@argus-mgmt ~]# argus baremetal -a delete-node -n myimage-rms/cluster-quanta-bms/qr3

Performing this step will power-off the server(s) and delete the server from cluster.

Do you want to continue?(Y/N)

+--------+--------+-------------------------------------------------+
| Action | Status |                    Details                      |
+--------+--------+-------------------------------------------------+
| Delete |  PASS  | job_uuid: ef648d52-20eb-49d7-b16d-b84cb52eae66 |
|        |        |                 status: ToRun                   |
+--------+--------+-------------------------------------------------+
```

Fetch Configuration

After the first deployment (ongoing or success), you can fetch the passed site configuration. This helps you to add more clusters or nodes to the existing site in case multiple users use the system and have no idea of previous deployments. Cisco recommends you to fetch the site configuration after you delete a cluster or a node as the existing config contain stale entries of the deleted cluster and node.

```
# argus baremetal -a fetch-config -n rakuten -d /var
Site config dumped at: /var/myimage-rms.yaml
```

Centralizing Management Node

Centralizing Management Node

For architectural information, see Management Node Centralization

Assumptions/Best practice

To achieve centralization of the management node, the following assumptions are made:

- The QCOW2 generated by Cisco VIM release must be used as a management node VM.
- There is a one-to-one relationship between the management node VM and target pod.
- Since the management node VMs are curated to manage Cisco VIM pods, a fully automated orchestration (backed with RestAPI) is provided to manage the same.
- The management node VMs can only be hosted on a Cisco VIM based cloud with pod type as micro, fullon, UMHC, or NGENAHC. Careful planning of storage must be made on the pod that hosts the management node VMs. This hosting pod typically requires a physical management node to be managed.
- In Cisco VIM 3.4.3, the management node VMs can manage micro, fullon, UMHC, NGENAHC, or edge pod. For micro, UMHC or NGENAHC pod hosting the virtual Cisco VIM management node, the following restrictions apply:

    a. The setup_data must run with CEPH_OSD_RESERVED_PCORES: 6
    b. The setup_data must run with cinder_percentage_data of 80 or more in CEPH_PG_INFO. This is a Day 0 configuration.

- The management node VMs can also be hosted on pods where Cinder is supported via Zadara, SolidFire, or multi-backend ceph. For multi-backend ceph, by default, the VMs are booted off volumes created on SSDs. For SolidFire, SSD, and HDD, the volume types with the names central_mgmt_solidfire, central_mgmt_ceph_ssd, and central_mgmt_ceph_hdd respectively are reserved by the system, and not to be used elsewhere in the cloud.
- For all types of pods hosting the virtual Cisco VIM management nodes, NOVA_RAM_ALLOCATION_RATIO must be 1.0 globally or on a per compute basis for all the computes belonging to Availability Zone (AZ) defined in CENTRAL_MGMT_AZ of the *setup_data.CentralMgmt.yaml*
- For the pod hosting the virtual Cisco VIM management nodes, the corresponding VMs are hosted in a project called *central_mgmt,* so that CVIM MON can monitor these nodes as special resources. The project *central_mgmt* is created automatically via the Cisco VIM orchestrator that handles the management node VMs.
- If the cloud is sharing workloads with other VNFs, it is recommended to add at least one compute node to the host aggregate created by the cloud admin. This is an optional manual step which helps to streamline the operation. The entry of CENTRAL_MGMT_AGGREGATE in the *setup_data. CentralMgmt.yaml* reflects the name of the host aggregate which hosts the management node VMs. With this approach, the cloud administrator can add more computes to the AZ as needed. For details on adding computes, see Adding Target Compute Nodes to AZ
- Admin must allocate a minimum of two routable networks for the management (br_mgmt) and api (br_api) networks of the VMs. When the VM is a Cisco VIM software hub, the two routable networks are br_public and br_private. For UM, only the API network (br_api) is used by the VM.
- File system access to the public key that is imported during VM deployment is needed.
- For managing the lifecycle of the management node VMs, all associated cloud resources are defined in a *setup_data,* example of which is available at */root/openstack-configs/setup_data.CentralMgmt.yaml.*
- If cloud is running with huge pages, the management node VMs are automatically launched using huge pages. It is assumed that all computes hosting the management node VMs have the same huge page size and percentage.
- Given the criticality of the management node, ensure that CVIM MON is enabled on the cloud hosting the management node VMs and the pods managed by the management node VMs.
- The pod managed by centralized VM, needs to run off a central CVIM-MON infrastructure. Use local CVIM-MON only as a transition phase to ensure optimal use of system resources.
- The NFVBench is not supported in the deployment of central management VMs.
- Provider networks belonging to VMTP section should not be used for creating central management VMs networks.
- After launch of central management VMs, the administrator *must not* forget to take a manual backup of the management node and copy the snapshot to another server.

Support Matrix

In Cisco VIM 3.4.3, management node VMs can be used to drive the following:

Pod Hardware Type	Management Network	BMC User and Network Requirements
Quanta servers	v6/v4	BMC User needs to have Admin, KVM, and VMedia access privileges. Layer 3 connectivity from management node VM to pod management network. v6 network must be routable.
Cisco UCS C-Series	v6/v4 or v4	Layer 3 connectivity from management node VM to pod management network. v4 network must be routable. Need to identify the management subnets and configure the DHCP relays on the ToRs attached to the target Cisco VIM OpenStack cloud. The DHCP IP relay address points to the management VM's br_mgmt interface (over v4), which serves the DHCP requests for the cloud hosts via cobbler.

DHCP Relay Configuration for UCS based Pods

```
F13_N93180_1# show run dhcp

!Command: show running-config dhcp
!Running configuration last done at: Tue Sep 3 12:17:01 2019
!Time: Tue Sep 3 12:17:18 2019

version 9.2(1) Bios:version 07.64
feature dhcp

service dhcp
ip dhcp relay
ipv6 dhcp relay


interface Vlan<id>                                                    --> Target Pod's management network
  ip address <a.b.c.d
/mask>                                                                                  --> SVI address
for VLAN 1228
  ip dhcp relay address <br_mgmt_v4_addr of Management node VM>       --> Management node VM's br_mgmt IPv4
address
```

Add the necessary routing on the ToRs, so that the management node VM's gateway is reachable from the ToR.

Add Target Compute(s) to AZ for Management Node VMs (Optional)

If the cloud is sharing workloads with other VNFs, it is recommended to have target compute nodes for management node VMs. To achieve that, the cloud administrator must create a host aggregate. This is a manual step which helps to streamline the operation. The entry of CENTRAL_MGMT_AGGREGATE in the *setup_data.CentralMgmt.yaml* reflects the name of the host aggregate which hosts the management node VMs. With this approach, cloud administrator can add more computes to the AZ as needed.

```
# cd /root/installer-xxx/openstack-configs
# source openrc

Fetch Hypervisor List
# openstack hypervisor list

Create Availability Zone for Central Management VM
# openstack aggregate create <target_az_name>               # Should match the value of CENTRAL_MGMT_AZ defined
in setup_data for Central VM management
# openstack aggregate set --zone <target_az_name>_az <target_az_name>  # while the Zone name can be different
from the availability_zone setting, it is recommended to append "_az" to the name to set the AZ for operation
ease

Add hypervisor to the AZ, one at a time
# openstack aggregate add host <target_az_name> <hypervisor_name1>
# openstack aggregate add host <target_az_name> <hypervisor_name2>
.
.

Check output of Availability Zone for Central Management VM
# openstack aggregate show <target_az_name>
```

Workflow/Usage

1. You must download the QCOW2 image from the release link onto the right directory of the management node of the cloud hosting the management node VMs. For example,

   ```
   cd to <dir_for_qcow2_image>

   curl -o cvim-image-NNNN.qcow2 https://cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases
   /<target-release>/buildnode-<release>.qcow2
   ```

2. For Cisco VIM Software Hub based installation, use the following:

   ```
   cd to <dir_for_qcow2_image>

   curl -o cvim-image-NNNN.qcow2 https://<sds-registry-host>/mercury-releases/cvim34-rhel7-osp13/releases
   /<target-release>/buildnode-<release>.qcow2
   ```

3. Create the *setup_data.CentralMgmt.yaml* by defining required resources to be created on the host pod.

   The following resources must be defined based on the information in *setup_data.CentralMgmt.yaml*:

   - Provide username/password for the OpenStack project of *central_mgmt*.
   - Provider network and subnets for API and management network segments.
   - Security group and rules.
   - Glance image for the CVIM QCOW2 image.
   - Flavor specification.
   - Keypair to import.
   - VOLUME_BACKEND: To indicate the target device type (SSD or HDD) to boot off in a multi-backend ceph. If not defined, system defaults to SSD for creation of volumes.
   - Servers and the corresponding network ports and bootable volume for the source image.

   > ⚠ The following are the best practice recommendations:
   >
   > - Use a host aggregate, so that computes dedicated for management node VMs are placed in it.
   > - Define the timezone at a global or per sever level.
   > - Define the *cvimadmin_password_hash* for console access to the management node at a global or per sever level.

Typical VM Flavor

With the characterization done so far, ensure that the management node VM contain 8 vCPUs, 25G RAM, and 1 TB HDD. Listed below is the corresponding flavor name:

```
- name: 'cvim-mgmt.8x24-nonlocal'
  ram: 24576
  vcpus: 8
  disk: 1024
```

Listed below is a sample of the *setup_data.CentralMgmt.yaml,* where all the target resources are defined:

```
#
# This is an example file for Centralizing the management node. It assumes that each of the management node is
running a VM in a cloud powered by Cisco VIM. There is a cloud # image that is released as part of the
artifacts used to get it going
#
PODTYPE: MGMT_CENTRAL

CENTRAL_MGMT_USER_INFO:
  username: <userrname>
  password: <password>


TIMEZONE: <entry as defined in TZ database name or notes of https://en.wikipedia.org/wiki
/List_of_tz_database_time_zones>
                            # Optional; the local value at a per server level overrides the global value;
                            # if local or global is not defined, it will take the timezone of the management
node that is hosting the VMs.

# List of network segments, min of 2
NETWORKS:
- segment: management   # can be either management or api
  vlan_id: <unique vlan_id part of provider network>
  name: <unique name of the network>
  subnets:
  - name: <unique name of the v4 subnet>
    network_cidr: a.b.c.d/mask
    gateway: x.y.x.w
    range: ['e.f.g.h', 'i.j.k.l']     # Start and End IP range to launch VM off
    ip_version: 4
    dns_nameservers: ['v4_dns_server']   # list of v4 DNS servers; max of 3
  - name: <unique name of the v6 subnet>  # Optional only needed if v6 is there
    network_cidr: '<cidr_in_v6 with mask>'  # cidr in v6
    gateway: '<gateway_in_v6>'         # gateway in v6
    range: ['start_ipv6_address', 'end_ipv6_address']   # Start and End IP range to launch VM off
    ip_version: 6
    dns_nameservers: ['v6_dns_server_list'] # list of v6 DNS servers; max of 3
- segment: api  # can be either management or api
  vlan_id: <unique vlan_id part of provider network>
  name: prov-net-api-2001
  subnets:
  - name: <unique name of the network>
    network_cidr: e.g.f.h/mask     # Unique CIDR
    gateway: p.q.r.s             # Corresponding Gateway
    range: ['e.f.g.d', 'i.t.k.l']  # Start and End IP range to launch VM off
    ip_version: 4
    dns_nameservers: [v4_dns_server]   # list of v4 DNS servers; max of 3
  - name: <unique name of the v6 subnet>  # Optional only needed if v6 is there
    network_cidr: '<cidr_in_v6 with mask>'  # cidr in v6
    gateway: '<gateway_in_v6>'         # gateway in v6
    range: ['start_ipv6_address', 'end_ipv6_address']   # Start and End IP range to launch VM off
    ip_version: 6
    dns_nameservers: ['v6_dns_server_list'] # list of v6 DNS servers; max of 3


 # List of Images for Management Node, min of 1
IMAGES:
- name: <unique_image_name>       # Unique name of images
  file_location: '<qcow_image_path>'

# Flavor info for Management Node, min of 1 info
FLAVORS:
```

```
- name: '<unique_flavor_name>'      # Unique name of flavor
  ram: <4096 to 200000>
  vcpus: <4 to 20>
  disk: <512 to 8192>          # Optional, but must be mutually exclusive for disk_vol_size on a per server
basis, between disk and disk_vol_size one of them has to be defined

# List of Keypairs for Management Node, min of 1
KEYPAIRS:
- name: mgmt_vm_keypair         # Unique Name of KEYPAIRS
  public_key_file: '/root/.ssh/id_rsa.pub'


#CVIMADMIN_PASSWORD_HASH should be the output from:

#  python -c 'import crypt; print crypt.crypt("<plaintext_strong_password>")'
# username is: cvimadmin
#CVIMADMIN_PASSWORD_HASH: <Please generate the admin pwd hash using the step above; verify if the output starts
with $6>



# Optional, mechanism to group computes dedicated for Virtual Management Node into one host aggregate
CENTRAL_MGMT_AGGREGATE: <Name of Host Aggregator> # Admin has to add the computes to the host aggregator named
here


# Optional, only allowed when Ceph is multi-backend (HDD and SSD based); if not defined SSD will be used to
create volume in a multi-backend environment. Also, for the entire system there is an uniform backend
#VOLUME_BACKEND: <SSD or HDD>


# List of Management Node in VM, min of 1
SERVERS_IN_VMS:
- name: <unique name of servers in VM>
  keypair: mgmt_vm_keypair     # Keypair name that is defined under KEYAPAIR/name
  image: <unique_image_name>   # image name that is defined under IMAGES/name
  flavor: '<unique_flavor_name>'  # flavor name that is defined under FLAVORS/name
  disk_vol_size: <512 to 8192> # integer, value in Gig, min of 512, max of 8192 Gig; optional but need to be
mutually exclusive for the relevant flavor, between disk and disk_vol_size one of them has to be defined
  node_type: <management or um or sds>
  domain_name: <your.domain.com> # optional
  timezone: <<entry as defined in TZ database name or notes of https://en.wikipedia.org/wiki
/List_of_tz_database_time_zones>
                            # Optional; the local value at a per server level overrides the global value;
                            # if local or global is not defined it will take the timezone of the
                            # management node that is hosting the VMs

  cvimadmin_password_hash: <Generate the admin pwd hash using the step above; verify if the output starts with
$6>
                            # Optional if defined globally; refer to the CVIMADMIN_PASSWORD_HASH section on how
to generate the password;
                            # username is: cvimadmin

  nics:                     # entry of 2 Items for node_type management or sds, entry of 1 is when node_type is
um

    - name: <unique_nic_name_across_all_vms>  # For br_mgmt
      network_name: prov-net-mgmt-2000        # Should Match Provider Network Name
      fixed_ips:
      - subnet: v4_mgmt_subnet                # IPv4 subnet network name
        ipaddress: <ipv4_address>             # IPV4 address belonging to v4_mgmt_subnet
      - subnet: v6_mgmt_subnet                # IPv6 subnet network name
        ipaddress: '<ipv6_address>'           # IPV6 address belonging to v6_mgmt_subnet
    - name: <unique_nic_name_across_all_vms>  # for br_api
      network_name: prov-net-api-2001         # Should Match Provider Network Name
      fixed_ips:
      - subnet: v4_api_subnet                 # IPv4 subnet network name
        ipaddress: <ipv4_address>             # IPV4 address belonging to v4_api_subnet
      - subnet: v6_api_subnet                 # IPv6 subnet network name
        ipaddress: '<ipv6_address>'           # IPV6 address belonging to v6_api_subnet
```

Execution of Deployment Orchestration

- Create the right host aggregate for the management node VMs and assign the right set of computes (Optional and API driven process).
- Update the target *CentalManagement setup_data* with the relevant VM information to spawn the management node VMs.
- Execute the ciscovim CLI to launch one or more VMs.

Tooling Usage

```
[root@cvim-mgmt ~]# ciscovim help central-vm
usage: ciscovim central-vm [--vms <vm_name1,vm_name1,...>]
                           [--file <setup_data_central_vm.yaml>] [-y]

                           <launch-all|clean-all|add-vms|delete-vms|list-vms|result|join>

Central Management VM Commands

Positional arguments:
  <launch-all|clean-all|add-vms|delete-vms|list-vms|result|join>
                                The Command to Perform for Central VM
                                Management

Optional arguments:
  --vms <vm_name1,vm_name1,...>   Comma separated list of VM names
  --file <setup_data_central_vm.yaml>
                                Provide a valid 'setup_data_central_vm.yaml'
                                file
  -y, --yes                     Yes option to perform the action
```

Launching Resources

To launch resources defined in *setup_data.CentralMgmt.yaml*, use the below command:

```
# To launch Central VMs for the first time
ciscovim central-vm launch-all --file <target_setup_data> [-y]

# To add VMs later
ciscovim central-vm add-vms --file <target_setup_data> --vms <, separated vms> [-y]   # In the target
setup_data, the target VMs are present in the SERVERS_IN_VMS section
```

Management Node VM Removal

To remove a specific or all management node VMs, use the following command:

```
# To delete all Central VMs
ciscovim central-vm clean-all --file <target_setup_data> [-y]   # In the target setup_data the section
SERVERS_IN_VMS should be absent

# To delete specific VMs
ciscovim central-vm delete-vms --file <target_setup_data> --vms <, separated vms> [-y] # In the target
setup_data the target VMs are absent in the SERVERS_IN_VMS section
```

Once the VM comes up, in case of management node, it contains all the artifacts for *ciscovim* client and *mercury-restapi* installed and running. Depending on the node type, the network interfaces are appropriately configured.

As the VM password management is not handled by this workflow deployment, the operator must login using the sshkey and then change the password in the VM.

After launch of central management VMs, the administrator must take a manual backup of the management node and copy the snapshot to another server.

Management Node VM and Resource Status

To list the status of the management node VMs and the resources available to launch additional management node VMs, use the following command:

```
# To list all Central VMs
ciscovim central-vm list-vms [-y]
```

The output lists the summary of management node VMs, their status and the interface IP addresses. Also, it lists the total number of VMs currently running and the resources such as compute, vCPU, RAM and storage available to launch additional management node VMs.

Central VM Management Result

To view the last result of the run, execute the following:

```
# To list all Central VMs
ciscovim central-vm result [-y]
```

Accessing Management Node VMs

If the management node VM is in Active state, some additional Cisco VIM services are available automatically. SSH to management node is not allowed, while availing the additional Cisco VIM services. To check if all the services are up and SSH is allowed, execute the following OpenStack command as a cloud admin:

```
# source /root/openstack-configs/central_mgmt.openrc

# To check if VM is ready for SSH access
# nova console-log <vm_name> | grep -o 'CVIM RestAPI install completed'
 or
# openstack console log show <vm_name> | grep -o 'CVIM RestAPI install completed'
```

Once the VM is ready for SSH access, you can set up the management node VM login in the following ways:

1. From the management node of the cloud hosting the VM, you can SSH to the VM and set the password via linux password mechanism and use it for access.
2. Log into the VM as root user, using the private ssh key corresponding to the public key that is provided as part of the KEYPAIRS entry in */root /openstack-configs/setup_data.CentralMgmt.yaml.*

- Only the cvimadmin user whose password is defined by: CVIMADMIN_PASSWORD_HASH, have console access, and not the remote user. Attempting to login with this user with SSH will not work.
- After the launch of central management VMs, the administrator must take a manual backup of the management node and copy the snapshot to another server.

Setup Data Changes for Management Node VM

To support the installation of management node VM over Layer 3, use the following command:

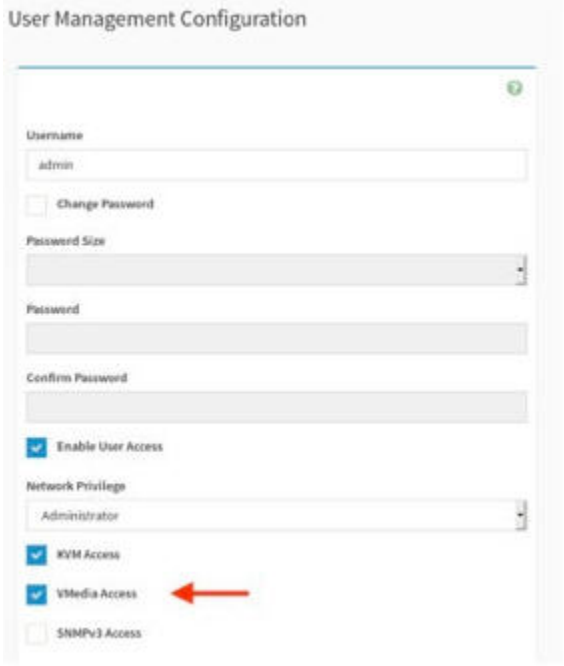
```
NETWORKING:

  domain_name: <domain_name>
  domain_name_servers: [dns_name_server_list]

# Optional, only allowed when the management node is centralized.
# need info of br_mgmt of the Centralized Management Node, IPV6 info is needed for dual stack environment
  remote_management:
   gateway: <ipv4_gateway>
   ipv6_gateway: '<ipv6_gateway>'
   ipv6_subnet: '<ipv6_subnet_with_cidr>'
   subnet: <ipv4_subnet_with_cidr>

  networks:
  - gateway: <v4_gateway>
    ipv6_gateway: <v6_gateway>
    ipv6_pool: [v6_pool_range]
    ipv6_subnet: <v6_subnet_cidr>
    pool: [v4_pool_range]
    segments: [management, provision]
    subnet: <v4_subnet_cidr>
    vlan_id: <management_vlan_id>
```

The pod's provision and management traffic continue to flow between management node VM's br_mgmt and OpenStack node's br_mgmt/mx interface, but over Layer 3. Since the management node is running in a VM, a faster log rotation within the VM is defaulted. It is recommended to configure the management node VMs with external syslog server, to ensure that you have access to all the necessary logs.

Additional Setting for Quanta BMC

For the central management VM feature to work, the BMC user must have Admin, KVM, and VMedia access privileges as depicted below. To enable it, execute the following:

1. Go to each of the Quanta BMC Web UI
2. In the UI, go to **Settings** > **User Management** > **<User account>**
3. Verify whether **Enable User Access (as Administrator), KVM Access,** and **VMedia Access** options are selected:



CVIM Monitor and Inventory Service Configuration

CVIM Monitor (CVIM-MON) and Inventory Service Configuration

Overview of CVIM Monitor

The Cisco VIM Monitor feature (CVIM-MON) provides a comprehensive solution for monitoring the health and for tracking the usage of resources in the CVIM pod infrastructure. This solution is available as a configuration option and provides the following services:

- Infrastructure-level metric collection from all nodes in the pod
- Metric aggregation into a time-series database (TSDB)
- Rule-based alerting engine integrated with the TSDB
- Web UI with with pre-defined dashboards customized for Cisco VIM
- REST API to query the TSDB
- REST API to query and silence alerts
- Alert notifications using SNMP traps or alternate alert notification protocols
- User-configurable alerting rules
- User-configurable web UI dashboards

The software components that provide the CVIM-MON service is called a CVIM-MON stack. The default deployment mode for CVIM-MON is to deploy the CVIM-MON stack on the pod management node.

The size of the TSDB depends on the frequency of the polling (configurable) and the number of compute nodes. By default, the metrics collected in each management node are kept for 15 days.

Enabling CVIM-MON on Cisco VIM

You can enable CVIM-MON on an existing pod that is installed with Cisco VIM 3.0.0 or later, through the reconfigure option by extending the *setup_data.yaml* file with relevant information.

The components of CVIM-MON are as follows:

- CVIM_MON: It provides the base functionality of monitoring and KPIs
- SNMP: to enable sending CVIM-MON alerts as SNMP traps (available only if CVIM-MON is enabled)
- SERVER_MON**:** to enable collecting UCS-C bare metal alerts into CVIM-MON. This featureis available only on Cisco UCS C-series servers

To enable CVIM-MON, the **CVIM_MON** and **PODNAME** keys must be added to the *setup_data.yaml* file.

The CVIM_MON key has the following properties:

- enabled: a boolean value indicating whether CVIM-MON is enabled.
- polling_interva**ls**: a dictionary defining the interval between metrics sampling.
- ui_access: A boolean indicating whether CVIM-MON UI access is enabled or not.

PODNAME is mandatory for CVIM-MON and is a name that identifies uniquely each CVIM pod.

SNMP traps can be enabled using the SNMP key with the following attributes:

- enabled: a boolean value indicating whether SNMP is enabled. CVIM_MON must also be enabled.
- managers: a list of SNMP managers to send the SNMP traps to. This list contains SNMPv2 or SNMPv3 managers. For SNMPv2, community and port can be set. For SNMPv3, the Engine_id and list of users must be specified, where the Engine_id is the EngineContextID which is used to send trap of the SNMP manager.

SNMP traps are sent without setting any authentication or security engine_id for the user.

The following table shows the list of properties with their default values and description:

Property Group and Name	Values	Default Value	Description
PODNAME:	<string>	(required)	Must be provided for identifying each pod if CVIM_MON is enabled.
CVIM_MON: enabled	true|false	false	A boolean indicating whether CVIM-MON is enabled or not. Set to True to enable CVIM_MON.
CVIM_MON: ui_access	true|false	true	A boolean indicating whether CVIM-MON UI access is enabled or not.
CVIM_MON: external_servers	List of external server IPs (v4 or v6) that must be monitored by CVIM MON	-	Optional. For more information, see Monitoring External Servers Using CVIM-MON
CVIM_MON: polling_intervals: high_frequency:	10s to 10m	15s	Metric collection sampling interval in seconds or minutes It is recommended to set to 1m in production deployments
SNMP: enabled	true|false	false	A Boolean indicating whether CVIM-Trap is enabled or not. If true, CVIM_MON:enabled must also be set to true.
SNMP: managers:	-	-	A list of up to 3 SNMP managers to send traps.
address	<ipv4 or ipv6>	(required)	IPv4 or IPv6 address of the SNMP manager
port	1-65535	162	Optional, port to send traps
version	v2c|v3	v2c	SNMP manager version
community	<string>	public	Used for SNMPv2c
SNMP: managers: users:			Required for SNMPv3, up to 3 users.
engine_id	<hexadecimal string>	(required v3)	Uniquely identifies the SNMP engines and entities. The SNMP engine IDs are composed of 5 to 12 octets and have no standard display format. It must be a hexadecimal string and cannot have all zeros or all 255s ("ff"). RFC 3411 specifies that the engine can be formatted with IPv4, IPv6, MAC address, text, and octets (and must start with 80). Listed below is a summary of the constraints. ContextEngineId is unique across all managers. Minimum length is 5 and maximum length is 32. All cannot be 00s or FFs and must start with 80.
name	<string>	(required v3)	User name
auth_key	<string>	(required v3)	Authorization password. Must be eight characters at least.
authentication	SHA|MD5	SHA	Authentication protocol
privacy_key	<str>	(auth_key)	Encryption key
encryption	'AES128'|'AES192'|'AES256'	'AES128'	Encryption protocol
SERVER_MON: enabled	true|false	false	Enable SNMP traps for CIMC faults (UCS C-series only)
host_info:	'ALL' or list of servers	'ALL'	Specifies the UCS-C servers to be monitored.
rsyslog_severity	emergency | alert| critical | error| warning| notice| informational | debug	(Optional)	Specifies the minimum severity from the UCS C-server logs that are to be sent to remote syslog servers

If SERVER_MON.rsyslog_severity is configured, you must configure SYSLOG_EXPORT_SETTINGS as well to indicate the remote syslog servers to send the logs.

Example of *setup_data.yaml* section related to CVIM-MON (not all possible optional values are represented):

```
CVIM_MON:
  enabled: true
  polling_intervals:
     high_frequency: 1m
SNMP:
 enabled: true
 managers:
 - address: 10.10.10.54
SERVER_MON:
  enabled: true
  host_info:
     - ALL
  rsyslog_severity: error
```

Monitoring External Servers Using CVIM-MON

From Cisco VIM 3.4.1, CVIM-MON can monitor external non-CVIM servers running RHEL or CentOS 7.6. CVIM-MON monitors these servers by installing a Telegraf agent on them to collect bare metal and libvirt metrics. The telegraf agent runs as a new systemctl service and collects metrics from the local server. These metrics are available for a remote scraper on port 9273.

Assumptions for Monitoring External Servers Using CVIM-MON

The following are the assumptions and prerequisites associated with this feature.

- The external servers must be reachable from the management node from the local or central CVIM-MON deployments.
- The external servers must run on UCS M4 or M5 hardware similar to the Cisco VIM management node BOM.
- The external servers must run Cisco VIM management node ISO or CentOS 7.7.
- The external nodes must run on the same site as the monitoring Cisco VIM pod. The scraping of metrics occurs over unauthenticated and unencrypted HTTP connections on port 9273.

Installation Procedure for Monitoring External Servers Using CVIM-MON

For monitoring external servers using CVIM-MON, you must update the *setup_data.yaml* file with the details of the external_servers, and run fresh installation or reconfiguration. As part of the fresh installation or reconfiguration operation, an *external-monitoring-<telegraf version>.tar.gz* tar file is created in the management node at */var/cisco/artifacts*.

To enable monitoring of the external servers using CVIM-MON, you must execute the following steps on each of the target external servers:

1. Untar the package file:

    a. Copy the *external-monitoring-<telegraf version>.tar.gz* file from the management node to the home directory of the external server.
    b. Untar the external-monitoring-<telegraf version>.tar.gz tar file. This will install the following three files under the *external-monitoring-1.12.1-V1* directory:

File	Description
extern.conf	Provides the telegraf configuration.
telegraf<version>.x86_64.rpm	Installs telegraf on the server.
monitor_external.sh	Deploys telegraf on the external server.

2. Customize the telegraf configuration based on configuration of the external server. The telegraf agent needs to listen on port 9273 being open.
3. Edit the *extern.conf* file as following:

    - If the external servers have certificate files to be monitored, provide the full path name of certificate files in *x509_cert* section. If there are no certificate files to be monitored, you can remove the *x509_cert* section.
    - Remove the *libvirt* section, if libvirt is not installed. This can happen when there are no VMs running.
4. Deploy telegraf on the external server, run the *monitor_externalbash* script in privileged mode:

    ```
    sudo ./monitor_external.sh
    ```

    If the script runs successfully, TELEGRAF INSTALL SUCCESS message is displayed. You can now access either the local/central Prometheus or Grafana, and monitor the external server.

Enabling CVIM-MON Post Pod Installation

You can enable CVIM-MON, SNMP traps and UCS-C bare metal alerts (SNMP, SERVER_MON) using the reconfigure option, post installation of Cisco VIM.

> ⚠ After you enable the CVIM-MON or CVIM-TRAP, it cannot be disabled again.

To enable CVIM-MON and SNMP traps features or to change the individual parameters in CVIM-MON, SNMP, or SERVER_MON:

1. Take a backup of setup_data file and update it manually with the configuration details by entering the following command:

```
# cd /root/
# mkdir MyDir
# cp /root/openstack-configs/setup_data.yaml /root/MyDir
# cd /root/MyDir
```

2. Edit the setup data.
3. Save the file and execute the below command:

```
ciscovim --setupfile /root/MyDir/setup_data.yaml reconfigure
```

> ⚠ The migration from SNMPv2 to SNMPv3 is only supported, but not vice-versa.

CVIM-MON Grafana/Prometheus and AlertManager with LDAP Backend

The CVIM-MON LDAP feature allows you to login with LDAP credentials. You can enable this feature by configuring the connection to the LDAP server and setting a valid filter to access Grafana/Prometheus and AlertManager with your LDAP credentials. Once the filter is set, it is possible to map the user groups with specific roles of permission in Grafana.

CVIM-MON Grafana supports the roles of:

- Viewer: Can only view dashboards and cannot modify them.
- Editor: Can view, create, copy, modify and save dashboards.

For Prometheus and AlertManager, users belonging to group mapped with *Admin* org_role have access.

To enable LDAP, you must modify the *setup_data.yaml* file by adding a *ldap* section under the CVIM_MON section as following (replace example values as appropriate):

```
CVIM_MON:

  central: false

  enabled: true

  ldap:

    domain_mappings:
    - attributes: {email: email, name: givenName, surname: sn, username: uid}
      bind_dn: <bind_dn>
      bind_password: <bind_password>
      domain_name: <domain_name>
      group_search_base_dns: ['ou=Groups,dc=org,dc=com']
      group_search_filter: (&(objectClass=posixGroup)(memberUid=%s))
      group_search_filter_user_attribute: uid
      ldap_uri: ldaps://<ldap_ip/ldap_fqdn>
          group_attribute: <group_attribute>
      group_attribute_is_dn: true/false
      root_ca_cert: <path_to_root_ca_cert>
          search_base_dns: ['dc=org,dc=com']
      search_filter: (uid=%s)
      use_ssl: true/false

    group_mappings:
    - {group_dn: 'cn=group2,ou=Groups,dc=org,dc=com', org_role: Admin}
    - {group_dn: 'cn=group3,ou=Groups,dc=org,dc=com', org_role: Viewer}

  polling_intervals: {high_frequency: 10s, low_frequency: 2m, medium_frequency: 1m}

  ui_access: true
```

Property	Field Required	Description
search_filter	Mandatory	Filter for the queries.
search_base_dns	Mandatory	It is the base DNS name used for all queries.
ldap_uri	Mandatory	Default port is 389. Takes the value 636, if use_ssl = True and port is not defined.
group_mappings	Mandatory	Must contain at least one group with org_role *Admin.* Optionally, you can add a second group with org_role *Viewer.* You can add multiple LDAP groups mapped to org_role *Admin* or *Viewer.*
domain_name	Mandatory	Any non-empty name is acceptable.
domain_mappings	Mandatory	Must contain one domain exactly.
bind_password	Conditional	Mandatory if LDAP supports binding. Not required for anonymous bind.
bind_dn	Optional	Mandatory if LDAP does not support anonymous bind.
attributes	Optional	Mandatory key but individual attributes are optional.
use_ssl	Optional	Optional. If not provided, defaults to False.
start_tls	Optional	Optional. If not provided, defaults to False.
client_cert	Optional	Authentication against LDAP servers requiring client certificates.
client_key	Optional	Authentication against LDAP servers requiring client certificates.
root_ca_cert	Optional	Path to your root CA certificate.
group_search_filter	Optional	To search group members.
group_search_base_dns	Optional	Base DN to search groups.
group_search_filter_user_attribute	Optional	Indicates the distinguished name of the client username.

group_attribute_is_dn	Optional	Default is True. If set to True, the distinguished name of the client username is used for checking group membership, otherwise, the client username is used.
group_attribute	Optional	Default value is memberUid.

Inventory Discovery as Tech-Preview Only

From Cisco VIM 3.4.3, CVIM-MON supports an optional Inventory discovery service to extract the inventory details from monitored nodes in the Cisco VIM pod. It is recommended that this feature be not rolled into production without talking to Cisco VIM PM team on its viability for support in production.

This Inventory discovery service provides a REST API to allow remote applications to control inventory scheduling and query the detailed inventory database. This inventory database is different from the TSDB and only contains the last snapshot of the pod inventory.

CVIM-MON is a prerequisite to enable inventory discovery. You can enable this feature by setting the following flag in the *setup_data.yaml* file:

```
INVENTORY_DISCOVERY: {enabled: true}
```

Highly Available CVIM Monitor

Highly Available CVIM Monitor

Overview of HA CVIM-MON

Overview of Highly Available Cisco VIM Monitor

From Cisco VIM 3.4.3, you can monitor CVIM pods either:

- Individually using the local CVIM Monitor (CVIM-MON) or
- Centrally using the new HA CVIM Monitor (HA CVIM-MON)

The local CVIM-MON (introduced in CVIM 3.0) provides pod-level monitoring based on a Prometheus stack that is hosted on the pod management node. This local solution supports the largest supported CVIM pod size (128 nodes).
Local CVIM-MON has the following limitations:

- Not highly available as a downtime of the management node stops all metric collection in the pod.
- Multi-site monitoring of large deployments with a large number of sites (dozens or hundreds of sites) is difficult as the pod-level time series database (TSDB) is isolated
- Very small sites with severely limited HW resources (edge cloud) cannot afford the resources to run a dedicated Prometheus stack per site. There is also operational complexity to manage a very large number of Prometheus stacks.

HA CVIM-MON addresses the above issues and has the following features:

- Integrated and highly-available monitoring of multiple Cisco VIM pods.
- Centralized TSDB, alarm and web-based GUI dashboards.
- Scales to hundreds of Cisco VIM pods and thousands of nodes.
- Provides a longer retention time for collected metrics (months instead of 15 days for the local CVIM-MON)
- Low sampling interval of 1 minute for largest deployments.
- Monitor pods of any size including very small pods (edge deployments) and individual bare metal servers.
- Monitored pods or servers are hierarchically grouped into metros and metros in regions.

A single HA CVIM-MON stack or two independent CVIM-MON stacks (for disaster recovery) can monitor the same set of monitored pods, or metros, or regions that form a monitoring domain.
HA CVIM-MON supports and requires a limited set of hardware configurations. You can install HA CVIM-MON on bare metal using a fully automated installer and by updating the setup data configuration file.

Hardware Requirements for HA CVIM MON

Hardware Requirements for HA CVIM-MON

HA CVIM-MON is available for Cisco UCS C-Series servers or Quanta servers with:

- One server used as a management node.
- Three or more servers to form a cluster managed by Kubernetes.

To achieve the required network throughput, you need one of the following:

- Each UCS server requires two Intel X710 cards.
- Each Quanta server requires one Intel XXV 710 card.

Networking Layout

Networking Layout for HA CVIM-MON

Public Network

The public network (br_api) interfaces with:

- External applications using HA CVIM-MON such as an OSS/BSS system querying the TSDB or browsers connecting to the HA CVIM-MON GUI.
- Managed Cisco VIM pods (for metrics collection).
- Managed servers.
- HA CVIM-MON administrators (ssh).

This public network is implemented by the br_api interface and provides external access to the following services:

- Kubernetes infrastructure administrator services.
- Kubernetes cluster nodes (ssh).
- Grafana, Prometheus, and Alertmanager HTTP services.

The public network segment needs one VLAN and at least five IPv4 or IPv6 addresses in an externally accessible subnet:

- One IP address for the management node.
- One IP address for each of the cluster nodes.
- One IP address for external_lb_vip for accessing the HA CVIM-MON services.

Management and Provisioning Segment

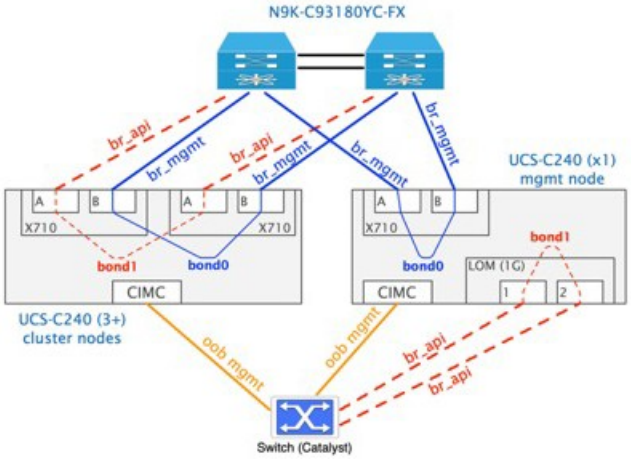
The management segment (br_mgmt) needs one separate VLAN and one subnet with an address pool large enough to accommodate all the current and future servers planned for the cluster for initial provisioning (PXE boot Linux) and for all Kubernetes internal communication. This VLAN and subnet can be local to CVIM-MON for UCS C-Series and Quanta deployments. All cluster nodes need an IP address from this subnet. The BMC or CIMC network must be accessible through the public network.

Network Topologies

Network Topologies for HA CVIM-MON

UCS C-Series Network Topology

UCS-C series based servers use Intel X710 NIC (4x10G, two NICs for each cluster node, and one NIC for the management node). Teaming is used for the *br_api* and *br_mgmt* links with dual N9K TORs.
The management node saves one Intel X710 NIC by using X710 for both *br_mgmt* links and LOM ports for the *br_api* links.



NXOS Switch Configuration for CVIMMON HA UCS Nodes

It is assumed that switches are preconfigured in virtual port channel mode. For NXOS configuration details, see *NXOS Switch Configuration Guide*. Listed below are the corresponding NXOS switch configuration of the port A and B links for each of the UCS nodes that make up the CVIMMON HA cluster.

The NXOS switch configuration connected to Intel NIC port A on the UCS nodes that make up the CVIMMON HA cluster is:

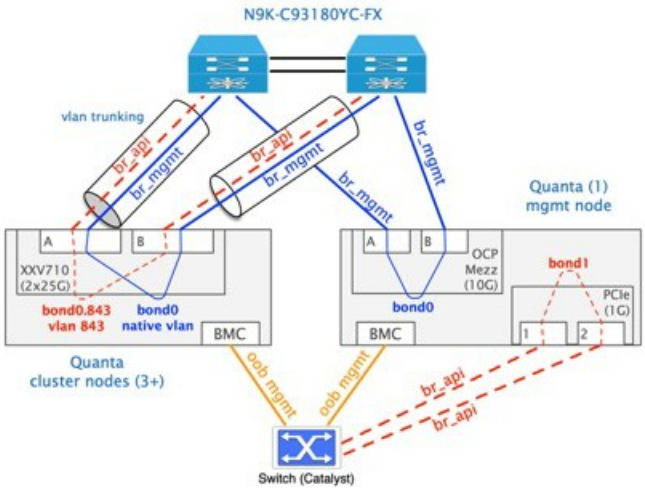
```
interface port-channel <pc_id_3>
  description mgmt API interface
  switchport
  switchport access vlan <api_vlan_id>
  spanning-tree port type edge
  no lacp suspend-individual
  vpc <pc_id_3>


interface Ethernet1/<id_3>
  description mgmt API interface
  switchport
  switchport access vlan <api_vlan_id>
  channel-group <pc_id_3> mode active
  no shutdown
```

The NXOS switch configuration connected to Intel NIC port B on the UCS nodes that make up the CVIM MON HA cluster is:

```
interface port-channel <pc_id_4>
  description mgmt interface
  switchport
  switchport access vlan <mgmt_vlan_id>
  spanning-tree port type edge
  no lacp suspend-individual
  vpc <pc_id_4>

interface Ethernet1/<id_4>
  description america2 mgmt interface
  switchport
  switchport access vlan <mgmt_vlan_id>
  channel-group <pc_id_4> mode active
  no shutdown
```

Quanta (QCT) Network Topology

The cluster nodes are connected to the ToR switches from the Intel XXV710 card ports as shown below. The *br_api* and *br_mgmt* interfaces are mapped on two different VLANs sharing the same physical links that are connected to the dual N9K TORs using VLAN trunking.



The management node uses the OCP Mezz NIC for *br_mgmt* (2x10G on VLAN 843) and the PCIe NIC for *br_api* (2x1G on native VLAN). The two *br-api* links of the management node are wired to the OOB switch.

NXOS Switch Configuration for CVIMMON HA QCT nodes

It is assumed that switches are preconfigured in virtual port channel mode. For more details on NXOS switch configuration, see *NXOS switch configuration guide*. Listed below are the specific configuration of the of the port A and B links for each of the Quanta nodes that make up the CVIM MON HA cluster.

NXOS switch configuration connected to 25G Intel NIC of the Quanta nodes that make up the CVIM MON HA cluster:

```
interface port-channel <pc_id_3>
  description mgmt and API interface
  switchport
  switchport mode trunk
  switchport trunk native vlan <mgmt_vlan>
  switchport trunk allowed vlan <mgmt_vlan,api_vlan>
  no lacp suspend-individual
  vpc <pc_id_3>

interface Ethernet1/<id_3>
  description mgmt and API interface ports
  switchport
  switchport mode trunk
  switchport trunk native vlan <mgmt_vlan>
  switchport trunk allowed vlan <mgmt_vlan,api_vlan>
  spanning-tree port type edge trunk
  channel-group <pc_id_3> mode active
  no shutdown
```

NXOS Switch Configuration for Management Node (QCT or UCS)

It is assumed that switches are pre-configured in virtual port channel mode (for NXOS configuration details one should refer to the NXOS switch configuration guide). Listed below are the specific configuration of the br_api (over LOM interface via Copper) and br_mgmt links for the UCS or Quanta based Management node of CVIM MON HA cluster.

The NXOS switch configuration of *br_api* (over 1G) for the management node in the CVIMMON HA cluster:

```
interface port-channel <pc_id_1>
  description API interface
  switchport
  switchport access vlan <api_vlan_id>
  spanning-tree port type edge
  no lacp suspend-individual
  vpc <pc_id_1>


interface Ethernet1/<id_1>
  description API interface
  switchport
  switchport access vlan <api_vlan_id_>
  channel-group <pc_id_1> mode active
  no shutdown
```

The NXOS switch configuration of *br_mgmt* (over 10G interface) for the management node in the CVIMMON HA cluster:

```
interface port-channel <pc_id_2>
  description mgmt interface
  switchport
  switchport access vlan <mgmt_vlan_id>
  spanning-tree port type edge
  no lacp suspend-individual
  vpc <pc_id_2>

interface Ethernet1/<id_2>
  description america2 mgmt interface
  switchport
  switchport access vlan <mgmt_vlan_id>
  channel-group <pc_id_2> mode active
  no shutdown
```

Architecture

Overview of HA CVIM-MON Architecture

The purpose of the cluster nodes is to run the functions of Kubernetes master and worker nodes.
The minimum configuration runs with only three master nodes. In this configuration, the three master nodes host the Kubernetes control plane components and the application containers that perform the HA CVIM-MON function. You can extend this configuration with one or more worker nodes based on computational and storage requirements. Worker nodes host only application containers.

PortWorx storage and data management platform forms the persistent and highly available storage and takes care of replicating the storage blocks across all cluster nodes and is transparent to the applications.

For more information on stacks, see HA CVIM-MON Stacks

For information on monitoring external servers using HA CVIM-MON , see External Servers

HA CVIM-MON Stacks

HA CVIM-MON Stacks

Overview of HA CVIM-MON Stacks

An HA CVIM-MON stack is a set of containers running in the same Kubernetes namespace that is in charge of a monitoring domain.
A monitoring domain includes one or more regions. Each region includes one or more metros. Each metro includes one or more Cisco VIM pods.

Each stack is identified by its name and provides the following services:

- Collection and storage of all the metrics generated by monitored Cisco VIM pods.
- Prometheus query REST interface to query the metrics.
- Grafana GUI to view pre-built monitoring dashboards.
- Pre-built alerting rules to generate alerts on Cisco VIM pods infrastructure fault conditions.
- Alert notification using SNMP traps or webhook requests - if configured.

Although most HA CVIM-MON deployments require only one stack per cluster, you can create more than one stack on the same cluster.
For example, you can create one stack for production and another for experimentation purposes. You can also create several stacks to monitor large group of different pods.
Different stacks have different configurations and do not share any common storage. Each stack provides its own service point URL.

Scale limitations

The main load of a stack is related to the following activities:

- Collecting metrics from all the remote Cisco VIM pods (networking load).
- Processing the collected metrics and generate alerts (cpu load).
- Store these metrics into a highly available storage (storage load).
- Handling the service metric queries coming from Grafana front-end or from external applications (mostly CPU load).

Depending on the total number of metrics to process, each stack can use a substantial amount of CPU, memory, storage, and network bandwidth.

In the current version with the recommended HA cluster hardware:

- The recommended limit per stack is 8,000 nodes or 1,000 Cisco VIM pods - whichever comes first (using 1m sampling interval).
- The recommended limit per HA cluster is 1 stack per cluster node with 1 spare cluster node.

For example, an HA cluster configuration with 3 master nodes and 2 worker nodes can run up to 4 stacks for a total of 32,000 nodes or 4,000 Cisco VIM pods. Such large configuration can typically process in the order of 1 million metrics per second (or a quarter million metrics per second per stack).

Adding HA CVIM-MON Stacks

You can execute the add-stack operation after adding new stacks to the *cvim-mon-stacks* list in the *candidate setup data* file. New stacks must have different names from the current stacks in the *reference setup data* file. The stacks must also follow the same target hierarchy or layout as the other working stacks. Any changes to the *candidate setup data* file besides adding new stacks to the *cvim-mon-stacks* list result in a validation failure.

After updating the *candidate setup data* file, run the *add-stack* operation from the current working installer directory using the following command:

```
[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --add-stack --setupfile
<path_to_candidate_setup_data_file>
The logs for this run are available at /var/log/cvimmonha/2019-10-22_121443_260335

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/2][VALIDATION: INIT]                                                    [   \   ]    0min 3secs

 Input File Validations!
+----------------------------------+--------+-------+
| Rule                             | Status | Error |
+----------------------------------+--------+-------+
| Schema Validation of Input File  |  PASS  | None  |
| Check for Valid Keys             |  PASS  | None  |
| Valid Operation Check            |  PASS  | None  |
| Pod operations for CVIM-MON-HA   |  PASS  | None  |
| Check for duplicate keys         |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature |  PASS  | None  |
| Check duplicate Cvim-Mon target  |  PASS  | None  |
| Information                      |        |       |
+----------------------------------+--------+-------+
[1/2][VALIDATION: INIT]                                                    [ DONE! ]    0min 4secs

Ended Installation [VALIDATION] [Success]

[2/2][HELM_INFRA: INIT]                                                    [ DONE! ]    0min 2secs
[2/2][HELM_INFRA: nginx-ingress-controller-Check whether helm binary exi...   [ DONE! ]    0min 3secs
[2/2][HELM_INFRA: nginx-ingress-controller-List installed Helm charts.]       [ DONE! ]    0min 4secs
[2/2][HELM_INFRA: prometheus-stack2->Clear the old-version file]              [ DONE! ]    9mins 1sec
[2/2][HELM_INFRA: prometheus-stack2->Faile the update if rollback was du...   [ DONE! ]    9mins 5secs

Ended Installation [HELM_INFRA] [Success]

Executing autobackup for CVIM MON
Executing autobackup at :/var/cisco/cvimmonha_autobackup/cvimmonha_autobackup_3.3.20_2019-10-22_12:23:55
[DONE] autobackup of CVIM MON HA Node successfully.
The logs for this run are available at /var/log/cvimmonha/2019-10-22_121443_260335
```

Deleting HA CVIM-MON Stacks

You can execute the *delete-cvim-pod* operation after deleting the existing OpenStack targets from the existing stacks in the *candidate setup data* file. Any changes to the *candidate setup data* file besides deleting targets from the existing *cvim-mon-stacks* list result in a validation failure.

After updating the *candidate setup data* file, execute the *k8s_runner.py* command with the *delete-cvim-pod* option from the current working installer directory:

The following example shows how to use the reconfigure option:

```
# ./bootstrap/k8s-infra/k8s_runner.py --delete-stack --setupfile <path_to_candidate_setup_data_file>
```

Reconfiguring HA CVIM-MON Stacks

You can reconfigure HA CVIM-MON stacks in the following ways:

Reconfiguration Options	Related Section
Update global options that are applicable to all HA CVIM-MON stacks.	Reconfiguring Global Options of HA CVIM-MON Stacks
Update parameters for each HA CVIM-MON stack.	Reconfiguring Individual HA CVIM-MON Stacks
Update the HA proxy certificate and HA CVIM-MON proxy password of each pod.	Reconfiguring a Cisco VIM OpenStack Pod

Reconfiguring Global Options of HA CVIM-MON Stacks

You can use the reconfigure option to modify global parameters that apply to all HA CVIM-MON stacks.

You can reconfigure the following global stack parameters:

Stack parameter	Description
log_rotation_frequency	Frequency of log rotation
log_rotation_size	Maximum size of each log. When the size of the log exceeds this value, a rotation occurs.
log_rotation_del_older	Number of compressed archive log files to keep for each log file. The old archive log files are deleted.

To reconfigure the above parameters, you must update them in a *candidate setup data* file and run the *k8s_runner.py* command with the *reconfigure* option.

The following example shows how to use the *reconfigure* option:

```
# ./bootstrap/k8s-infra/k8s_runner.py --reconfigure --setupfile <path_to_candidate_setup_data_file>
```

Reconfiguring Individual HA CVIM-MON Stacks

You can use the *reconfigure-stack* option to change the SNMP parameters under each stack section in the *setupdata.yaml* file. You can modify the following fields using the *reconfigure-stack* option:

- Enable SNMP feature
- Add or remove SNMP manager
- Change the IP address of the SNMP manager
- Change version of SNMP manager

You cannot configure the following options:

- Scrape interval
- LDAP configuration

The following example shows how to use the *reconfigure-stack* option:

```
# ./bootstrap/k8s-infra/k8s_runner.py --reconfigure-stack --setupfile <path_to_candidate_setup_data_file>
```

Reconfiguring a Cisco VIM OpenStack Pod

You can use the *reconfigure-cvim-pod* option to update the HA proxy certificate (cert) and HA CVIM-MON proxy password (cvim_mon_proxy_password) of each pod. You can execute the *reconfigure-cvim-pod* operation after changing the certificate or the proxy password keys of the existing OpenStack targets from the existing stacks in the *candidate setup data* file. Any changes to the *candidate setup data* file besides these keys in the existing cvim-mon-stacks list result in a validation failure.

After updating the *candidate setup data* file, execute the *reconfigure-cvim-pod* operation from the current working installer directory using the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --reconfigure-cvim-pod --setupfile <path_to_candidate_setup_data_file>
```

Modifying Monitored Targets in a Stack

The Prometheus server in each stack is configured to pull metrics from the list of configured target Cisco VIM pods at a given interval. These pull requests are scheduled concurrently to spread equally within the interval window. This action enables a better distribution of the bandwidth within each scrape interval.

Adding a Target Cisco VIM OpenStack Pod

You can execute the *add-cvim-pod* operation after adding new Cisco VIM OpenStack targets to the existing stacks of the cvim-mon-stacks list in the *candidate setup data* file. The new targets must have different names and a different target IP from the other targets in the stack. Any changes to the *candidate setup data* file besides adding new targets to existing stacks result in a validation failure.

After updating the *candidate setup data* file, execute the *add-cvim-pod* operation from the current working installer directory using the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --add-cvim-pod --setupfile <path_to_candidate_setup_data_file>
```

Deleting a Target Cisco VIM OpenStack Pod

You can execute the *delete-cvim-pod* operation after deleting the existing OpenStack targets from the existing stacks in the *candidate setup data* file. Any changes to the *candidate setup data* file besides deleting targets from the existing cvim-mon-stacks list result in a validation failure.
After updating the *candidate setup data* file, execute the *delete-cvim-pod* operation from the current working installer directory using the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --delete-cvim-pod --setupfile <path_to_candidate_setup_data_file>
```

External Servers

Prerequisites for Monitoring External Servers Using HA CVIM MON

You can monitor the external servers such as standalone Linux servers that are not managed by any Cisco VIM pod, using an HA CVIM-MON stack. You must provide the server name and its IP address followed by port 9273 in the setup data file.
The servers must meet the following prerequisites:

- Servers must be reachable from the Prometheus server in the HA CVIM-MON stack.
- Servers must run on hardware that is similar to the CVIM Management Node BOM.
- Servers must run the CVIM Management node ISO or CentOS 7.7.
- Servers must have the Telegraf agent provided by the HA CVIM-MON stack installer.
- Servers must run in the same site as the HA CVIM-MON cluster.

Prometheus collects the server metrics over unauthenticated and unencrypted HTTP connections on port 9273.
Cisco VIM distinguishes the metrics collected from external servers from the Cisco VIM pod metrics by a node_type label value of external. By default, Cisco VIM associates the metrics for all CPUs with the label tag set to host. You can customize this with additional steps during installation.

Default built-in alerting rules and custom alerting rules equally apply to external nodes unless restricted to certain node types in the rule.
For more information on how HA CVIM-MON stack monitors external servers, see Monitoring External Servers

Installation Modes

Installation Modes for HA CVIM-MON

You can install HA CVIM-MON using three installation modes.

CVIM-MON installation must be done using a VNC or screen so that the session is not lost. If you do not have a VNC environment, execute the same from KVM console of the management node. Ensure that you do not run this command in background or with nohup option to avoid failure

Connected Mode of Install

You can perform this mode of installation, when the Cisco VIM management node has internet connectivity. All the artifacts and docker images needed for installation are directly fetched from the internet and utilized by the installer. This is the default mode of HA CVIM-MON install. You must provide the following information in the *setup data* file to fetch artifacts from cvim-registry.com:

```
REGISTRY_USERNAME: <username>
REGISTRY_PASSWORD: <password>
REGISTRY_EMAIL: <email>
```

Air-Gapped Install using USB

The following procedure describes how to download the Cisco NFVI installation files onto a USB drive of the staging server with Internet access. You can use the USB to load the Cisco NFVI installation files onto the management node without Internet access.

Ensure that you use Virtual Network Computing (VNC), a terminal multiplexer, or similar screen sessions to complete the following steps.

Before you begin you must have a CentOS 7 staging server (VM, laptop, or UCS server) with a 64 GB USB 2.0 drive. You can use USB 3.0 64GB if the management node is of type Cisco UCS M5. The staging server must have a wired Internet connection to download the Cisco VIM installation files onto the USB drive. Once downloaded, you can copy the installation files onto the management node from a USB drive.

1. Fetching artifacts to the staging server:
    a. On the staging server, use yum to install the following packages:
        - PyYAML
        - Python-requests
        - Centos-release-scl
        - Python 3.6
          Check if python 3.6 binary is located at /opt/rh/rh-python36/root/bin/, if not copy the python 3.6 binary to /opt/rh/rh-python36/root/bin/.

    b. Log into Cisco VIM software download site and download the *getartifacts.py* script from the external registry:

```
# download the new getartifacts.py file (see example below)
curl -o getartifacts.py
https://username:password@cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/3.4.3
/getartifacts.py
Change the permission of getartificats.py chmod +x getartifacts.py
```

    c. Run *getartifacts.py*.

    The script formats the USB2.0 drive (or USB3.0 drive for M5/Quanta based management node) and downloads the installation files. You must provide the registry username and password, tag ID, and USB partition on the staging server.

```
# ./getartifacts.py -t <tag_id > -u <username> -p <password> -d <device_path> --mgmtk8s [--proxy]
<proxy>
```

d. Use the following command to verify the downloaded artifacts and container images:

```
# create a directory
sudo mkdir -p /mnt/Cisco
# You need to mount the partition with the steps given below:
sudo mount <device_path> /mnt/Cisco
cd /mnt/Cisco
# execute the verification script
./test-usb
```

e. If the *test-usb* script reports any failures, you can unmount the USB and run the *getartifacts* command again with the *--retry* option.

```
sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d <device_path> --mgmtk8s --retry
```

f. Mount the USB and then run the *test-usb* command to validate if all the files are downloaded:

```
# create a directory sudo mkdir -p /mnt/Cisco
# You need to mount the partition with the steps given below: sudo mount <device_path> /mnt/Cisco
cd /mnt/Cisco
# execute the verification script
./test-usb
```

g. When the USB integrity test is done, unmount the USB drive by using the following command:

```
# Unmount USB device
sudo umount /mnt/Cisco
```

Importing artifacts from the USB on to the management node.

2. On the CVIM MON HA management node, use the prepared USB stick and complete the following steps:

a. Insert the USB stick into the management node drive, after you install the *buildnode.iso*.
b. Use *import_artifacts.sh* script to copy all the artifacts onto the management node. After successful completion, the installation artifacts are copied to */var/cisco/artifacts* on the management node. After the artifacts are available in the management node, the steps to install HA CVIM MON pod remain the same.

```
# Run import artifacts script
cd ~/installer-<tag_id>/tools
./import_artifacts.sh
```

3. Configure the setup data file:

HA CVIM MON *setup data* file has a configuration to set the install mode. Set the install mode as disconnected to prevent the management node from fetching the artifacts from Internet. For example:

```
INSTALL_MODE: disconnected
```

Air-Gapped Installation Using Software Delivery Server

The Software Delivery Server (SDS) is also called the Cisco VIM Software Hub.
Cisco VIM Software Hub alleviates the need for Cisco VIM management nodes to have internet connectivity and helps to remove the logistics of shipping USBs to multiple pods across the enterprise for software installation or update of the cloud. You can install and download the HA CVIM MON artifacts on the SDS server.
For more information on the hardware requirements of the SDS server and steps to install artifacts, see Installing Cisco VIM Software Hub in Air-gapped Mode.

Configuration of Setupdata File

After you pre-install the artifacts on the Cisco VIM Software Hub, you can start the HA CVIM MON installation using SDS.

⚠ Ensure that the br_api IP address can reach the br_private IP address of the SDS server.

1. Install the management node with build node ISO.
2. Add the following fields in the HA CVIM MON *setup data* file.

```
REGISTRY_NAME: '<registry_name>' # Mandatory Parameter.
```

HA CVIM MON *setup data* file requires the REGISTRY_USERNAME and REGISTRY_PASSWORD to connect to the docker registry and fetch docker images.

To fetch the docker images from Cisco VIM Software Hub node, provide the user credentials available in the SDS_READ_ONLY_USERS section of *sds_setup_data.yaml*. The details of an admin user with read or write access to the docker registry are provided in **SDS_REGISTRY_USERNAME** and **SDS_REGISTRY_PASSWORD**. Hence, it is recommended that you have a read-only user on the Cisco VIM pod.

Setup File

Configuring Setup Data File for HA CVIM-MON

Overview

Before you begin, install the management node ISO on the management node. You must select the management node install option during the ISO install process.

The setup data file describes all the parameters of the HA CVIM-MON cluster and is required for the installation of the HA CVIM-MON cluster after the management node is up and running.
Following are the naming conventions used:

- setup data file: Refers to various version of the *setup_data.yaml* file that reside on the management node
- setup data targets file: An optional file that contains per-stack specific targets, named *<stack_name>.yaml* (there can be as many side car files, as there are stacks).

  The targets files are always associated to a setup data file and are always located in the same directory. They are also called side car files.
- setup data file set: A group files that include a setup data file and zero or more associated targets files.

HA CVIM-MON always keep a copy of the current setup data file set under */root/openstack-configs* called the *reference setup data file set*. The reference setup data file is */root/openstack-configs/setup_data/yam*l and must be considered read-only for all operations. This file must never be modified directly.

An example setup data file is available at: */root/openstack-configs/setup_data.yaml.HA CVIM-MON.EXAMPLE*.

> ⚠ For a fresh install, the reference setup data file is not expected to be present in the current workspace. A candidate setup data file set must be created outside of the */root/openstack-configs/* directory and passed as an argument to the installer *(–setupfile <pathname>*).
>
> After a successful installation, the reference setup data file set is updated with the candidate setup data file set to reflect the current state of the cluster. You cannot directly modify or remove those files under any circumstances.

You must configure the following parameters in the candidate setup data file.

General HA CVIM-MON cluster parameters

Configure the general parameters of the HA CVIM-MON cluster such as:

- IP address for the internal load balancer for the br_mgmt network (this is an internal IP address)
- IP address for the external load balancer for the br_api network (external IP address)
- NTP servers
- Domain suffix to use for all external URLs to HA CVIM-MON services
- Virtual router ID (for VRRP)

The IP addresses to provide are either IPv4 or IPv6 based on selected IP version (set in the Argus bare metal section).
The final domain suffix is of the following format:

```
.cvimmon-<stack_name>.<domain_suffix>
```

HA CVIM-MON Stack Parameters

Configure the stack properties such as:

Stack property	Description
Stack name	Identifies each stack. The name can only be lower-case alphanumeric characters. '-' is the only special character allowed.

Metric retention time	Metrics retention time in the Prometheus TSDB. The unit can be "d" (days), "w" (weeks), "m" (months), "y" (years) Older metrics will be purged past the retention time. It is recommended to keep the retention time to the strict minimum especially at very large scale to limit disk usage. Unless you have well set requirement on how long yo keep the metrics, the suggested default metric retention time is 3 months (value: 12w or 3m) Also see below to see the impact on storage requirements.
Metrics volume size	Storage size reserved for the the stack in GB. See below for calculation.
Metric scraping interval	Frequency with which monitored CVIM pods are scraped for their metrics. The recommended setting is to use 1 minute scraping interval (value: 1m)
Regions, Metros, Pods	The list of regions, metros, and pods that the stack monitors.
Static credentials of the Grafana server	• Admin user name • Admin password

Disk Size Calculation

The required disk size depends on four main factors:

- metric retention time
- scraping interval
- number of monitored nodes
- number of time series per node

The formula below assumes typical loads and could be adjusted based on actual conditions:

```
needed_disk_space_per_month = ingested_samples_per_month * bytes_per_sample * replication_factor
```

where:

ingested_samples_per_month is the total number of metrics ingested in a month.

bytes_per_sample is the disk space required to store one metric in the TSDB. The typical space used per sample is 1 to 2 bytes. Prometheus compresses samples in the TSDB.

replication_factor is the number of times each storage block is stored in the storage cluster for high availability. This is set to 3 in HA CVIM-MON.

The number of metrics depend directly on the number of time series generated by the monitored nodes. A time series is a sequence of metric values that track a property of a monitored resource. Hence, there is 1 time series per monitored resource and per property.

For example, a virtual interface is a monitored resource that has over 10 properties (rx/tx packet counter, byte counter, error counter...) and each virtual interface generates as many time series as the number of properties.

The number of time series is a function of the following parameters:

- The number of nodes to monitor.
- Type of node such as compute, storage, and controller.
- Type of hardware used, for example, CPU cores, physical interfaces, and physical disks.
- The number of virtual resources used in these pods. For example, number of VMs and virtual interfaces.

Typical OpenStack nodes (a node here is a bare metal server) generate between 1000 and up to 5000 time series per server.

The number of metrics ingested per sampling interval is equal to the number of time series.

Assumptions:

- 3000 time series per node
- 1-minute sampling interval, the number of minutes per month is 60 * 24 * 30

Required raw disk space in GB per month per node = 3000 * (60 * 24 * 30) * 2 * 3 / 1000000000 = ~0.78 GB which can be rounded up to:

```
Required_Disk_Space = 1GB/node/month
```

Example:

- 20 sites of 20 nodes each
- 3 month retention
- Required_disk_space=400*3=1200GB=1.2TB

Regions, Metros, and Pods

The region, metro, and pod names must be unique within the monitoring domain. They can be any ASCII string. These names are only used as a metric label value.
You must configure each region with the following parameters:

- A region name
- A list of metros

You must configure each metro with the following parameters:

- A metro name
- A list of Cisco VIM pods

You must configure each Cisco VIM pod with the following parameters:

- A pod name
- Pod IP address (IPv4 or IPv6)
- Pod HA proxy certificate
- User name and password to access the pod

Log Rotation

You must configure the following parameters for the infrastructure logs:

- Frequency of log rotation
- Maximum size of each log. When the size of the log exceeds this value, a rotation occurs.
- Number of compressed archive log files to keep for each log file. The old archive log files are deleted.

SNMP

You must configure SNMP for each stack only if SNMP traps are enabled. When SNMP traps are enabled, all HA CVIM-MON alerts in the stack are forwarded to the configured SNMP managers using the selected SNMP version.
You must configure the following parameters for SNMP:

- IPv4 or IPv6 address and port to send traps to.
- SNMP version: v2c (default) or v3.
- SNMP credentials:
  - v2c-Community string
  - v3-engine ID, credentials and encryption settings

LDAP Support for Grafana (CVIM MON Stacks)

Grafana has two default users with dynamically assigned passwords and different roles:

- Viewer: Cannot create new or modify existing dashboards.
- Admin: Can create new and modify existing dashboards.

LDAP configuration consists of two main sections:

1. Domain mappings
2. Group mappings

Domain Mappings

- attributes
  - email
  - member_of
  - name
  - surname
  - username
- bind_dn
- bind_password
- use_ssl
- start_tls
- client_cert
- client_key

- root_ca_cert
- group_search_filter
- group_search_base_dns
- group_search_filter_user_attribute
- domain_name
- ldap_uri
- search_base_dns
- search_filter

Group Mappings

These mappings are required to authorize users from a specific group in ldap to access Grafana with *Admin* or *Viewer* permissions.

- group_dn : 'CN=group2,OU=GroupsDC=OrgName,DC=com' , org_role: Admin
- group_dn : 'CN=group3,OU=GroupsDC=OrgName,DC=com' , org_role: Viewer

Users from Group Employees get Admin access for Grafana whereas users from Read-Only Employees get Viewer privileges.

For example:

```
cvim_mon_stacks:
- name: qomstack
  ldap:
    domain_mappings:
      - attributes:
        email: email
        name: givenName
        surname: sn
        username: uid
        bind_dn: <bind_dn>
        bind_password: <bind_password>
        domain_name: corp_ldap1
        group_search_base_dns: ['ou=Groups,dc=OrgName,dc=com']
        group_search_filter: "(&(objectClass=posixGroup)(memberUid=%s))"
        group_search_filter_user_attribute: uid
        ldap_uri: ldap(s)://<ldap_url>:<Port>
        root_ca_cert: "/root/cvimha_certs/<cert_name>"
        search_base_dns: ['dc=OrgName,dc=com']
        search_filter: "(uid=%s)"
        start_tls: false
        use_ssl: true
    group_mappings:
      - group_dn: cn=group2,ou=Groups,dc=OrgName,dc=com
        org_role: Admin
      - group_dn: cn=group3,ou=Groups,dc=OrgName,dc=com
        org_role: Viewer
```


- Only one LDAP server can be configured per stack
- LDAP support is only enabled for Grafana Dashboard.

LDAP Support for Grafana (CVIM MON HA Cluster Monitor)

CVIM MON HA cluster itself is monitored by default on all CVIM MON HA pods. Grafana, Prometheus, and Alertmanager are installed in an isolated cvimmon-monitor namespace. Default admin credentials are generated during installation to access Grafana dashboard. Also, the LDAP users are allowed to access the dashboard. Example snippet of *setup_data.yaml* to add LDAP support for cvimmon-monitor is provided below:

```
CVIMMONHA_CLUSTER_MONITOR:
  ldap:
    domain_mappings:
      - attributes:
        email: email
        name: givenName
        surname: sn
        username: uid
        bind_dn: <bind_dn>
        bind_password: <bind_password>
        domain_name: corp_ldap1
        group_search_base_dns: ['ou=Groups,dc=OrgName,dc=com']
        group_search_filter: "(&(objectClass=posixGroup)(memberUid=%s))"
        group_search_filter_user_attribute: uid
        ldap_uri: ldap(s)://<ldap_url>:<Port>
        root_ca_cert: "/root/cvimha_certs/<cert_name>"
        search_base_dns: ['dc=OrgName,dc=com']
        search_filter: "(uid=%s)"
        start_tls: false
        use_ssl: true
    group_mappings:
      - group_dn: cn=group2,ou=Groups,dc=OrgName,dc=com
        org_role: Admin
      - group_dn: cn=group3,ou=Groups,dc=OrgName,dc=com
        org_role: Viewer
```

External Servers

LDAP support can be added or removed as a Day 1 operation using reconfigure operation.

The servers must meet a few pre-requisites. For more information, see External Servers.
You must configure the following parameters for external servers:

- Server name
- Server IP address followed by port 9273

For more information on monitoring the external servers, see CVIMMON > *Monitoring External Servers Using CVIM MON*

Argus Bare Metal

You must configure the following parameters for the Argus Bare metal:

- HA CVIM-MON release deployment image
- IPv4 or IPv6 selection for the cluster deployment
- br_api network addressing
- br_mgmt network addressing
- Bare metal access credentials (CIMC or BMC)
- Linux root credentials
- DNS and NTP settings
- Time zone selection

Run the HA CVIM-MON installer. For more information, see HA CVIM-MON Installer

HA CVIM-MON Installer

Using HA CVIM-MON Installer

Before you Begin

Before using the HA CVIM-MON installer, see the following:

- Installation Modes for HA CVIM-MON
- Configuring Setup File for HA CVIM-MON

Management Node Installation

CVIM-MON management node installation procedure is same as Cisco VIM management node installation. To install the management node, see Management Node on Quanta Servers and Management Node on UCS Servers

Management Node Preparation

You must perform the installation operations from the installer directory under */root/installer-<build>*. The build number is specific for each HA CVIM-MON release. The installer script is *./bootstrap/k8s-infra/k8s_runner.py*.
The installation process has the following steps:

1. Validation
   Verifies the hardware and software configuration.

2. Bootstrap Infra
   Prepares the management node for CVIM MON HA installation for setting up local docker registry, installing repos, host packages on management node, and so on.

3. Setup Argus
   Prepares bare metal installation.

4. Argus bare metal
   Installs and configures the operating system.

5. CVIM-MON Infra
   Prepares Cisco VIM MON nodes for Kubernetes and application install.

6. Kubernetes Provisioner
   Installs the Kubernetes infrastructure.

7. Helm Infra
   Installs the HA CVIM-MON stacks.

You can list all steps using the *-l* argument and you can execute the steps individually:

```
# ./bootstrap/k8s-infra/k8s_runner.py -l

     !!  CVIM MON HA ORCHESTRATOR  !!
========================================
+------------------------+--------------+
| Operations             | Operation ID |
+------------------------+--------------+
| VALIDATION             |      1       |
| BOOTSTRAP_INFRA        |      2       |
| SETUP_ARGUS            |      3       |
| ARGUS_BAREMETAL        |      4       |
| COMMON_CVIM_MON_INFRA  |      5       |
| KUBERNETES_PROVISIONER |      6       |
| HELM_INFRA             |      7       |
+------------------------+--------------+
```

Complete Installation

For complete installation, run the script passing *install* and *setupfile* arguments:

```
# ./bootstrap/k8s-infra/k8s_runner.py --install --setupfile <path_to_candidate_setup_data_file>

                       ############################
                        CVIM MON HA ORCHESTRATOR
                       ############################


[1/5][VALIDATION: INIT]                                                 [   -   ]    0min 12secs

 Input File Validations!
+-----------------------------------+--------+-------+
| Rule                              | Status | Error |
+-----------------------------------+--------+-------+
| Schema Validation of Input File   |  PASS  | None  |
| Check for Valid Keys              |  PASS  | None  |
| Valid Operation Check             |  PASS  | None  |
| Check for duplicate keys          |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature|  PASS  | None  |
| Check duplicate Cvim-Mon target   |  PASS  | None  |
| Information                       |        |       |
| Check Argus api network information|  PASS  | None  |
| Check Argus management network    |  PASS  | None  |
| information                       |        |       |
| Check Argus api network information|  PASS  | None  |
| Check Argus management network    |  PASS  | None  |
| information                       |        |       |
| Pod operations for CVIM-MON-HA    |  PASS  | None  |
+-----------------------------------+--------+-------+
[1/5][VALIDATION: INIT]                                                 [   \   ]    0min 50secs
```

The installation is considered complete, when the Step 7 completes successfully.

The *k8s_runner.py* script forbids all operations other than *--install* or *--list-steps* (or *-l*), until the installation is completed successfully.

Installation Failure

Installation can fail for various reasons. The most common cause of failure is the use of incorrect setup data configuration. Most of the errors are detected in Step 1, but other errors can be detected at a later step.

The failure recovery procedure depends on the step where the failure occurs:

- If the failure occurs in Step 1 or Step 2, fix the errors causing the failure or contact the TAC support to find out the root cause.
- If the failure occurs from Step 3 to Step 7, contact TAC support.

Resources

Resources for Managing HA CVIM-MON Cluster

You can manage your HA CVIM-MON cluster using various commands.

Configuration File and Secrets

The reference setup data file is available at:

```
~/openstack-configs/setup_data.yaml
```

The secrets are saved under:

```
~/openstack-configs/secrets.yaml
```

The *secrets.yaml* file is readable only from the root. This file contains the username and password for accessing Grafana, Prometheus, and Alertmanager for each stack.
An example of *secrets.yaml* file is given below:

```
Prometheus-Password-cvimmon-monitor(Username:admin):YyZM5f3DdyCKxklw1vIN4i0l0M2EoRbkjb+UKm0Sa5Y=
Grafana-Password-cvimmon-monitor(Username:admin):59QRzzo+PEedz8MDfdX26+DoaMJ/OgVgoqGWdUhDS78=
Grafana-Password-stack1(Username:admin):h72DhjEnVS/Rr4nFCZmmxKRmuK/t7qjyZJJrFbTyCtM=
Prometheus-Password-stack1(Username:admin):1Ph5AI8JUhiHgX0vjHB3W0Wzgjy2jWfiC5egAQJuuIs=
Grafana-Password-stacktsdb(Username:admin):N/ABGdX0ym5VhJ7Q/k8TO1oeqRXuzvbOmU9JeunA1As=
Prometheus-Password-stacktsdb(Username:admin):F8SPq+1qUSKM08EvlL+bTbL6RU8BI8Qcz/Yjzi0s7gw=
```

Stack Services URLs

To get information about sStack services URLs, use the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py  --get-endpoint [<stack-name> | "all"]
Listing Endpoints for : stack2
+-------------------------------------------------------------------------+
| Endpoint FQDN                                                           |
+-------------------------------------------------------------------------+
|  <IP Address> cvimmon-grafana-stack2.cisco.com                          |
|  <IP Address> cvimmon-alertmanager-stack2.cisco.com                     |
|  <IP Address> cvimmon-prometheus-stack2.cisco.com                       |
+-------------------------------------------------------------------------+
```

If you use *all* as a parameter to *--get-endpoint,* the table lists all URLs of all stacks in the cluster.

For a given stack, all URLs are assigned the same IP address. The HTTP server at this IP address reroutes the traffic to the appropriate service container based on the requested URL.

Kubernetes Resources

To list Kubernetes nodes, use the following command:

```
[root@queensland installer]# kubectl get nodes
NAME       STATUS   ROLES    AGE   VERSION
cvmonq1    Ready    master   56m   v1.15.2
cvmonq2    Ready    master   56m   v1.15.2
cvmonq3    Ready    master   61m   v1.15.2
cvmonq4    Ready    <none>   54m   v1.15.2
```

In the above example, the Kubernetes cluster has three master nodes and one worker node.

To get the status of the cluster, use the following command:

```
[root@Antarctica ~]# kubectl cluster-info
Kubernetes master is running at https://[2001:420:293:241f:172:29:75:115]:6443
KubeDNS is running at https://[2001:420:293:241f:172:29:75:115]:6443/api/v1/namespaces/kube-system/services
/kube-dns:dns/proxy
```

To debug and diagnose cluster problems, use the *kubectl cluster-info dump* command.

Cisco VIM implements each HA CVIM-MON stack as a separate Kubernetes namespace that contains several pods. A pod is a wrapper for a Kubernetes container.

To list all namespaces including HA CVIM-MON stacks, use the following command:

```
[root@Antarctica ~]# kubectl get pods --all-namespaces | grep grafana
cvimmon-monitor   grafana-cvimmon-monitor-65656cd4cb-qtzfp                          1/1     Running
0          17d
stack1            grafana-stack1-549d4f7997-6p5fb                                  1/1     Running
6          17d
stacktsdb         grafana-stacktsdb-56c6cd4875-hp97p                               1/1     Running
5          16d
stacktsdb2        grafana-stacktsdb2-7fb6c7dc5c-m9dq5                              1/1     Running
3          16d
stackv6           grafana-stackv6-6d656b868-znz5f                                  1/1     Running
1          3d20h
```

To list all the pods of a given stack, use the following command:

```
[root@Antarctica ~]# kubectl get pods -n stackv6
NAME                                          READY   STATUS    RESTARTS   AGE
grafana-stackv6-6d656b868-znz5f               1/1     Running   1          3d20h
prometheus-stackv6-alertmanager-9f557fdb5-96h4z   2/2     Running   0          3d20h
prometheus-stackv6-server-5cffbb5b49-wh4p7        2/2     Running   0          3d20h
```

To display the node on which each pod of a stack is running, use the following command:

```
[root@Antarctica ~]# kubectl get pod -o=custom-columns=NODE:.spec.nodeName,NAME:.metadata.name -n stackv6
NODE          NAME
antarctica2   grafana-stackv6-6d656b868-znz5f
antarctica1   prometheus-stackv6-alertmanager-9f557fdb5-96h4z
antarctica1   prometheus-stackv6-server-5cffbb5b49-wh4p7
```

To display the persistent volume chain (PVC) attached to each pod, use the following command:

```
[root@Antarctica ~]# kubectl get pvc -n stackv6
NAME                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES
STORAGECLASS   AGE
grafana-stackv6                     Bound    pvc-61af7b58-6b7a-48a5-8562-2e3fcb662f65   10Gi       RWX
portworx-sc    14d
prometheus-stackv6-alertmanager   Bound    pvc-5b9dedc8-2540-4edf-aa5e-4296ff03b5a9   50Gi       RWX
portworx-sc    14d
prometheus-stackv6-server         Bound    pvc-1a9ded1d-70c5-43ea-af83-c62ceee241d1   2000Gi     RWO
portworx-sc    14d
```

Pod Operations

Supported Pod Operations

> All CVIM-MON pod-operations must be executed in a VNC or screen so the session is not lost. If you do not have a VNC environment, execute the same from KVM console of the management node. Ensure that you do not run this command in background or with *nohup* option to avoid failure.

Replacing a Master Node

You must replace a master node if there are any hardware issues, power failure, disk failure, and so on. HA CVIM-MON provides an option to replace the master node to help in the recovery of the master node. A master node can be online or offline during the master replace operation.
The conditions for replacing the master node are given below:

- You must not change the setup data especially the node details for the replace node option.
- The replaced node and the defective node must have the same CIMC or BMC version.
- You can replace only one master node at a time. You cannot use the replaced node, if more than one master node is defective.

When you replace a node, the master node is removed from the Kubernetes cluster and replaced with a new master node with the same name and the hardware details.
The following example shows how to replace a master node:

```
cd /root/installer-<build_number>
# ./bootstrap/k8s-infra/k8s_runner.py --replace-master <node_name> --setupfile
<path_to_candidate_setup_data_file>

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --replace-master cvmonq1 --setupfile ~
/Save/new_setup_data.yaml
The logs for this run are available at /var/log/cvimmonha/2019-10-22_145736_574029

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/4][CLEANUP: INIT]                                                    [ DONE! ]    0min 2secs
[1/4][CLEANUP: check-kubernetes-node-Check if the node is present]      [ DONE! ]    0min 2secs
<SNIP>
[1/4][CLEANUP: delete-etcd-member-Get ClusterConfiguration config map fo...   [ DONE! ]    3mins 30secs
[1/4][CLEANUP: delete-etcd-member-Remove the node from the clusterstatus...   [ DONE! ]    3mins 40secs

Ended Installation [CLEANUP] [Success]

[2/4][ARGUS_BAREMETAL: INIT]                                            [ DONE! ]    0min 0sec
[2/4][ARGUS_BAREMETAL: Validating Argus Configs..]                      [ DONE! ]    0min 2secs
<SNIP>
[2/4][ARGUS_BAREMETAL: Servers are pxe-booting..Takes Time!!]           [ DONE! ]    16mins 56secs
[2/4][ARGUS_BAREMETAL: Server(s) deploy operation finished: Success]    [ DONE! ]    17mins 3secs

Ended Installation [ARGUS_BAREMETAL] [Success]

[3/4][COMMON_CVIM_MON_INFRA: INIT]                                      [ DONE! ]    0min 1sec
[3/4][COMMON_CVIM_MON_INFRA: update-known-hosts-Set backup_name fact for...   [ DONE! ]    0min 1sec
<SNIP>
 [3/4][COMMON_CVIM_MON_INFRA: ntp-Restore old selinux label]             [ DONE! ]    6mins 51secs
[3/4][COMMON_CVIM_MON_INFRA: ntp-Enable ntpd service]                   [ DONE! ]    6mins 52secs

Ended Installation [COMMON_CVIM_MON_INFRA] [Success]

[4/4][KUBERNETES_PROVISIONER: delete-etcd-member-Remove the node from th...   [ DONE! ]    0min 3secs
[4/4][KUBERNETES_PROVISIONER: kube-apiserver-podpreset-Add node-monitor-...   [ DONE! ]    10mins 23secs
[4/4][KUBERNETES_PROVISIONER: kube-apiserver-podpreset-Add pod-eviction-...   [ DONE! ]    10mins 33secs

Ended Installation [KUBERNETES_PROVISIONER] [Success]

Executing autobackup for CVIM MON
Executing autobackup at :/var/cisco/cvimmonha_autobackup/cvimmonha_autobackup_3.3.20_2019-10-22_15:35:56
```

Adding a Worker Node

You can add a worker node to the HA CVIM-MON cluster in the following two ways:

- Pre-define in the inital *setup data* file so that the worker node is installed when you install the HA CVIM-MON cluster.
- Add the worker node post-deployment using the *--add-worker* option, in a *candidate setup data* file.

Following are the conditions for adding the worker node to the HA CVIM-MON cluster:

- You must add the hardware details of the worker node in a *candidate setup data* file (Argus bare metal section).
- You can add only one worker at a time to the HA CVIM-MON cluster.
- The worker node hardware and the network hardware must conform to the same BOM defined by the HA CVIM-MON master nodes.
- You must apply the same networking schema of the HA CVIM-MON masters for all worker nodes.

Configuring Setup data File for Worker Node

You must use the following schema for defining a worker node in a *setup data* file. The same schema is used for the master nodes except for the role field. You must explicitly define the role field as a worker for the worker node.

```
- name: Worker1
            oob_ip: 10.10.10.10
            role: worker
            ip_address:
              management_1_v4: 10.10.11.10/24
              management_1_gateway_v4: 10.10.11.1
              api_1_v4: 10.10.12.10/24
              api_1_gateway_v4: 10.10.12.1
```

Add Worker Command

To add the worker to the HA CVIM-MON cluster, use the following command:

```
cd /root/installer-<build_number
# ./bootstrap/k8s-infra/k8s_runner.py --add-worker <node_name> --setupfile <path_to_candidate_setup_data_file>

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --add-worker cvmonq4 --setupfile ~/Save
/new_setup_data.yaml
The logs for this run are available at /var/log/cvimmonha/2019-10-22_140832_817059

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/5][VALIDATION: INIT]                                                    [   -   ]    0min 3secs

 Input File Validations!
+-----------------------------------+--------+-------+
| Rule                              | Status | Error |
+-----------------------------------+--------+-------+
| Schema Validation of Input File   |  PASS  | None  |
| Check for Valid Keys              |  PASS  | None  |
| Valid Operation Check             |  PASS  | None  |
| Check for duplicate keys          |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature|  PASS  | None  |
| Check duplicate Cvim-Mon target   |  PASS  | None  |
| Information                       |        |       |
| Check Argus api network information|  PASS  | None  |
| Check Argus management network    |  PASS  | None  |
| information                       |        |       |
| Check Argus api network information|  PASS  | None  |
| Check Argus management network    |  PASS  | None  |
| information                       |        |       |
| Pod operations for CVIM-MON-HA    |  PASS  | None  |
+-----------------------------------+--------+-------+
[1/5][VALIDATION: INIT]                                                    [   \   ]    3mins 1sec

  UCS Hardware Validations
+----------------------------+--------+----------------+
| UseCase                    | Status | Failure Reason |
+----------------------------+--------+----------------+
| CIMC Firmware Version Check|  PASS  | None           |
| Argus NIC Adapter Check    |  PASS  | None           |
| Argus Num Disks Check      |  PASS  | None           |
+----------------------------+--------+----------------+
[1/5][VALIDATION: INIT]                                                    [ DONE! ]    3mins 2secs

Ended Installation [VALIDATION] [Success]

[2/5][GENERATE_INVENTORY: INIT]                                            [ DONE! ]    0min 0sec
[2/5][GENERATE_INVENTORY: Get Artifacts Phase...Takes Time !!]             [ DONE! ]    0min 2secs
[2/5][GENERATE_INVENTORY: generate-inventory-Check if Argus Site File is...  [ DONE! ]    0min 2secs
[2/5][GENERATE_INVENTORY: generate-inventory-Copy Rendered Inventory Fil...  [ DONE! ]    0min 3secs

Ended Installation [GENERATE_INVENTORY] [Success]

[3/5][ARGUS_BAREMETAL: INIT]                                               [ DONE! ]    0min 0sec
[3/5][ARGUS_BAREMETAL: Validating Argus Configs..]                         [ DONE! ]    0min 2secs
```

```
[3/5][ARGUS_BAREMETAL: Initiating Argus Baremetal node operation..]           [ DONE! ]    0min 2secs
[3/5][ARGUS_BAREMETAL: Initiating Node deploy: cvmonq4..]                     [ DONE! ]    0min 3secs
[3/5][ARGUS_BAREMETAL: Servers are pxe-booting..Takes Time!!]                 [ DONE! ]    15mins 56secs
[3/5][ARGUS_BAREMETAL: Server(s) deploy operation finished: Success]          [ DONE! ]    16mins 3secs

Ended Installation [ARGUS_BAREMETAL] [Success]

[4/5][COMMON_CVIM_MON_INFRA: generate-inventory-Copy Rendered Inventory ...   [ DONE! ]    0min 1sec
[4/5][COMMON_CVIM_MON_INFRA: update-known-hosts-Set backup_name fact for...   [ DONE! ]    0min 2secs
[4/5][COMMON_CVIM_MON_INFRA: ntp-Restore old selinux label]                   [ DONE! ]    7mins 47secs
[4/5][COMMON_CVIM_MON_INFRA: ntp-Enable ntpd service]                         [ DONE! ]    7mins 48secs

Ended Installation [COMMON_CVIM_MON_INFRA] [Success]

[5/5][KUBERNETES_PROVISIONER: INIT]                                           [ DONE! ]    0min 3secs
[5/5][KUBERNETES_PROVISIONER: kubeadm-Remove swapfile from /etc/fstab]        [ DONE! ]    0min 5secs
[5/5][KUBERNETES_PROVISIONER: kubeadm-Turn swap off]                          [ DONE! ]    0min 7secs
<SNIP>

[5/5][KUBERNETES_PROVISIONER: reconfig-kubelet-Restart Kubelet if Change...   [ DONE! ]    6mins 20secs

Ended Installation [KUBERNETES_PROVISIONER] [Success]

Executing autobackup for CVIM MON
Executing autobackup at :/var/cisco/cvimmonha_autobackup/cvimmonha_autobackup_3.3.20_2019-10-22_14:42:00
[DONE] autobackup of CVIM MON HA Node successfully.
```

Removing a Worker Node

You can remove a worker node from the cluster if required. An HA CVIM-MON cluster can operate without any worker nodes. You can also remove all the worker nodes. After this operation, Cisco VIM deletes the node from the HA CVIM-MON Kubernetes cluster. All the running pods are automatically migrated to the other workers or masters.
The conditions for removing a worker node are given below:

- You can remove only one worker node at a time.
- You must delete the node details of the worker node from the *candidate setup data* file, before executing the remove worker operation.

To remove the worker node, use the following command:

```
cd /root/installer-<build_number>
# ./bootstrap/k8s-infra/k8s_runner.py --remove-worker <node_name> --setupfile
<path_to_candidate_setup_data_file>

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --remove-worker cvmonq4 --setupfile ~
/Save/new_setup_data.yaml
The logs for this run are available at /var/log/cvimmonha/2019-10-22_134955_053095

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/4][VALIDATION: INIT]                                                       [   /   ]    0min 2secs

 Input File Validations!
+-----------------------------------+--------+-------+
| Rule                              | Status | Error |
+-----------------------------------+--------+-------+
| Schema Validation of Input File   |  PASS  | None  |
| Check for Valid Keys              |  PASS  | None  |
| Valid Operation Check             |  PASS  | None  |
| Check for duplicate keys          |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature|  PASS  | None  |
| Check duplicate Cvim-Mon target   |  PASS  | None  |
| Information                       |        |       |
| Check Argus api network information|  PASS  | None  |
| Check Argus management network    |  PASS  | None  |
| information                       |        |       |
| Check Argus api network information|  PASS  | None  |
| Check Argus management network    |  PASS  | None  |
```

```
| information                          |        |       |
| Pod operations for CVIM-MON-HA       |  PASS  | None  |
+--------------------------------------+--------+-------+
[1/4][VALIDATION: INIT]                                                    [   /   ]    2mins 43secs

  UCS Hardware Validations
+-----------------------------+--------+----------------+
| UseCase                     | Status | Failure Reason |
+-----------------------------+--------+----------------+
| CIMC Firmware Version Check |  PASS  | None           |
| Argus NIC Adapter Check     |  PASS  | None           |
| Argus Num Disks Check       |  PASS  | None           |
+-----------------------------+--------+----------------+
[1/4][VALIDATION: INIT]                                                    [ DONE! ]    2mins 44secs

Ended Installation [VALIDATION] [Success]

[2/4][CLEANUP: INIT]                                                       [ DONE! ]    0min 2secs
[2/4][CLEANUP: check-kubernetes-node-Check if the node is present]         [ DONE! ]    0min 2secs
[2/4][CLEANUP: portworx-Get the node status for the replace node]          [ DONE! ]    1min 59secs
[2/4][CLEANUP: portworx-Get the node status for the replace node]          [ DONE! ]    1min 59secs
[2/4][CLEANUP: portworx-Remove the node from the cluster]                  [ DONE! ]    2mins 50secs

Ended Installation [CLEANUP] [Success]

[3/4][ARGUS_BAREMETAL: INIT]                                               [ DONE! ]    0min 0sec
[3/4][ARGUS_BAREMETAL: Validating Argus Configs..]                         [ DONE! ]    0min 2secs
[3/4][ARGUS_BAREMETAL: Initiating Argus Baremetal node operation..]        [ DONE! ]    0min 2secs
[3/4][ARGUS_BAREMETAL: Initiating Node delete: cvmonq4..]                  [ DONE! ]    0min 54secs
[3/4][ARGUS_BAREMETAL: Server(s) delete operation finished: Success]       [ DONE! ]    1min 1sec

Ended Installation [ARGUS_BAREMETAL] [Success]

[4/4][GENERATE_INVENTORY: INIT]                                            [ DONE! ]    0min 1sec
[4/4][GENERATE_INVENTORY: generate-inventory-Check if Argus Site File is...  [ DONE! ]  0min 1sec
[4/4][GENERATE_INVENTORY: generate-inventory-Copy Rendered Inventory Fil...  [ DONE! ]  0min 2secs

Ended Installation [GENERATE_INVENTORY] [Success]

Executing autobackup for CVIM MON
Executing autobackup at :/var/cisco/cvimmonha_autobackup/cvimmonha_autobackup_3.3.20_2019-10-22_13:56:36
[DONE] autobackup of CVIM MON HA Node successfully.
The logs for this run are available at /var/log/cvimmonha/2019-10-22_134955_053095
```

Regenerating Certificates

You can regenerate Kubernetes, ETCD, and application certificates using HA CVIM-MON.

Kubernetes Certificates

To regenerate Kubernetes certificates, use the following command:

```
./bootstrap/k8s-infra/k8s_runner.py --renew-k8s-certs

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --renew-k8s-certs
The logs for this run are available at /var/log/cvimmonha/2019-10-22_112657_292383

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/2][VALIDATION: INIT]                                                    [   /   ]    0min 3secs

 Input File Validations!
+-----------------------------------+--------+-------+
| Rule                              | Status | Error |
+-----------------------------------+--------+-------+
| Schema Validation of Input File   |  PASS  | None  |
| Check for Valid Keys              |  PASS  | None  |
| Valid Operation Check             |  PASS  | None  |
| Pod operations for CVIM-MON-HA    |  PASS  | None  |
| Check for duplicate keys          |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature |  PASS  | None  |
| Check duplicate Cvim-Mon target   |  PASS  | None  |
| Information                       |        |       |
+-----------------------------------+--------+-------+
[1/2][VALIDATION: INIT]                                                    [ DONE! ]    0min 4secs

Ended Installation [VALIDATION] [Success]

[2/2][KUBERNETES_PROVISIONER: INIT]                                        [ DONE! ]    0min 4secs
[2/2][KUBERNETES_PROVISIONER: kubernetes-renew-certs-Check Cluster State]  [ DONE! ]    0min 7secs
[2/2][KUBERNETES_PROVISIONER: kubernetes-renew-certs-Fail if any of the ...  [ DONE! ]    2mins 53secs
[2/2][KUBERNETES_PROVISIONER: kubernetes-renew-certs-Check if all Pods i...  [ DONE! ]    2mins 55secs

Ended Installation [KUBERNETES_PROVISIONER] [Success]

The logs for this run are available at /var/log/cvimmonha/2019-10-22_112657_292383
```

ETCD Certificates

To regenerate ETCD certificates, use the following command:

```
./bootstrap/k8s-infra/k8s_runner.py --renew-etcd-certs

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --renew-etcd-certs
The logs for this run are available at /var/log/cvimmonha/2019-10-22_113204_415606

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/2][VALIDATION: INIT]                                                    [   -   ]    0min 3secs

 Input File Validations!
+-----------------------------------+--------+-------+
| Rule                              | Status | Error |
+-----------------------------------+--------+-------+
| Schema Validation of Input File   |  PASS  | None  |
| Check for Valid Keys              |  PASS  | None  |
| Valid Operation Check             |  PASS  | None  |
| Pod operations for CVIM-MON-HA    |  PASS  | None  |
| Check for duplicate keys          |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature |  PASS  | None  |
| Check duplicate Cvim-Mon target   |  PASS  | None  |
| Information                       |        |       |
+-----------------------------------+--------+-------+
[1/2][VALIDATION: INIT]                                                    [ DONE! ]    0min 4secs

Ended Installation [VALIDATION] [Success]

[2/2][KUBERNETES_PROVISIONER: INIT]                                        [ DONE! ]    0min 4secs
[2/2][KUBERNETES_PROVISIONER: etcd_upgrade-Configure | Check if etcd clu...   [ DONE! ]    0min 4secs
[2/2][KUBERNETES_PROVISIONER: etcd_upgrade-Fail if any of the ceritficat...   [ DONE! ]    0min 32secs
[2/2][KUBERNETES_PROVISIONER: etcd_upgrade-Configure | Check if etcd clu...   [ DONE! ]    0min 34secs

Ended Installation [KUBERNETES_PROVISIONER] [Success]

The logs for this run are available at /var/log/cvimmonha/2019-10-22_113204_415606
```

Self-Signed Application Certificates

To regenerate self-signed application certificates, use the following command:

```
./bootstrap/k8s-infra/k8s_runner.py --regenerate-certs --setupfile <path_to_candidate_setup_data_file>

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --regenerate-certs --setupfile ~/Save
/new_setup_data.yaml
The logs for this run are available at /var/log/cvimmonha/2019-10-22_120629_288207

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/2][VALIDATION: INIT]                                                    [   -   ]    0min 2secs

 Input File Validations!
+----------------------------------+--------+-------+
| Rule                             | Status | Error |
+----------------------------------+--------+-------+
| Schema Validation of Input File  |  PASS  | None  |
| Check for Valid Keys             |  PASS  | None  |
| Valid Operation Check            |  PASS  | None  |
| Pod operations for CVIM-MON-HA   |  PASS  | None  |
| Check for duplicate keys         |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature |  PASS  | None  |
| Check duplicate Cvim-Mon target  |  PASS  | None  |
| Information                      |        |       |
+----------------------------------+--------+-------+
[1/2][VALIDATION: INIT]                                                    [ DONE! ]    0min 3secs

Ended Installation [VALIDATION] [Success]

[2/2][HELM_INFRA: INIT]                                                    [ DONE! ]    0min 2secs
[2/2][HELM_INFRA: nginx-ingress-controller-Check whether helm binary exi...   [ DONE! ]    0min 3secs
[2/2][HELM_INFRA: prometheus-stack1->Check Rollout Status of Prometheus-...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Check the status of Prometheus-stac...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Ensure Prometheus-stack1 Deployment...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Clear the old-version file]              [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Faile the update if rollback was du...   [ DONE! ]    1min 12secs

Ended Installation [HELM_INFRA] [Success]

Executing autobackup for CVIM MON
Executing autobackup at :/var/cisco/cvimmonha_autobackup/cvimmonha_autobackup_3.3.20_2019-10-22_12:07:46
[DONE] autobackup of CVIM MON HA Node successfully.
The logs for this run are available at /var/log/cvimmonha/2019-10-22_120629_288207
```

Custom Application Certificates

With central CVIM-MON, you can provide trusted CA signed x509 certificates which are used to access the Prometheus, Grafana, and Alertmanager applications in the HA CVIM-MON cluster. If certificates are not provided, self-signed certificates are generated for these URLs by default. To find the ingress URLs configured for Prometheus, Grafana, and Alertmanager in each stack, execute the following command:

```
./bootstrap/k8s-infra/k8s_runner.py --get-endpoint all
Listing Endpoints for : stack1
+-----------------------------------------------+
| Endpoint FQDN                                 |
+-----------------------------------------------+
| 1.2.3.4 cvimmon-grafana-stack1.cisco.com      |
| 1.2.3.4 cvimmon-alertmanager-stack1.cisco.com |
| 1.2.3.4 cvimmon-prometheus-stack1.cisco.com   |
+-----------------------------------------------+
```

Based on the result, you can use the application FQDN's as Common Name (CN) or alternative DNS names in the x509 certificate.

The central CVIM-MON supports two types of custom x509 Certificates:

- Domain level wildcard certificates
- Stack level certificates

A trusted CA signed certificate comprises of multiple files (root CA certificate, intermediate CA certificate, application certificate, and certification key). A Privacy Enhanced Mail (PEM) bundle comprising of all these files must be created using the following steps:

```
$ cat user-ca.crt >> user-bundle.pem ( Root CA and intermediate CA  )(Optional)
$ cat user.crt >> user-bundle.pem ( Certificate file )
$ cat user.key >> user-bundle.pem ( Key File )
$ mv user-bundle.pem /root/cvimha_certs
```

⚠ Private key of a trusted CA signed certificate must not have any passphrase (non-encrypted key)

Domain Level Wildcard Certificates

A wildcard certificate can support multiple subdomains for a particular domain.

To generate this certificate, ensure that the following conditions are met:

- Must match the *cvimmon_domain_suffix* defined in the *setup data* file.
- Must be defined at a global level in the *setup data* file so that it can be used to access Grafana, Prometheus, and Alertmanager of all CVIM-MON stacks.

An example of wildcard certificate is provided below:

```
$ grep cvimmon_domain_suffix /root/openstack-configs/setup_data.yaml
cvimmon_domain_suffix: lab.test.com

$ openssl x509 -in /root/cvimha_certs/user-bundle.pem -text -noout
. . .
Subject: C=US, ST=California, L=San Jose, O=IT, CN=*.lab.test.com
```

To define a domain level custom certificate, edit the *setup data* file and add the path to the certificate as given below:

```
$ grep cvimmon_domain /root/openstack-configs/setup_data.yaml
cvimmon_domain_suffix: lab.test.com
cvimmon_domain_ca_cert: /root/cvimha_certs/user-bundle.pem
```

Stack Level Certificates

You can generate stack level certificates for individual stacks using the stack service URLs as hostname. Grafana URL can be provided in certificate CN and Prometheus/Alertmanager URLs can be added as Subjective Alternative Names (SANs) for the certificate. An example of stack level certificate is given below:

```
$ openssl x509 -in /root/cvimha_certs/user-bundle.pem -text -noout
. . .
Subject: C=US, ST=California, L=San Jose, O=IT, CN=cvimmon-grafana-stack1.lab.test.com
. . .
X509v3 extensions:
X509v3 Subject Alternative Name:
DNS:cvimmon-alertmanager-stack1.lab.test.com, DNS:cvimmon-prometheus-stack1.lab.test.com, DNS:cvimmon-grafana-
stack1.lab.test.com
```

To add a stack level certificate, edit the *setup data* file and add the path of the certificate under the stack parameters.

```
- name: "stack1"
  metrics_retention: "8m"
  stack_ca_cert: /root/cvimha_certs/user-bundle.pem
```

- You can switch from self-signed certificate to custom certificates or vice versa using the *--regenerate-certs* command line option.
- You can add the appropriate certificate path in the *candidate setup data* file and run the *--regenerate-certs* for using the certificate.
- If you remove the certificate path from the *candidate setup data* file and re-run the *./bootstrap/k8s-infra/k8s_runner.py --regenerate-certs,* you are switched back to self-signed certificates.

Regenerating Secrets

During the deployment of CVIM MON HA cluster Grafana, Prometheus and AlertManager passwords are auto generated. These passwords are for admin user and can be used to access respective dashboards. Additional CLI's have been provided with k8s_runner.py script to list passwords for each stack and regenerate passwords.

To configure passwords for above services, use the following:

1. Regenerate Secrets
2. Custom Secrets

View Secrets

To view passwords for each application, first execute *list-secrets* command to fetch the secret keys.

```
# ./bootstrap/k8s-infra/k8s_runner.py --list-secrets all

+-----------------------------------------------------+
| Secret Keys                                         |
+-----------------------------------------------------+
| Grafana-Password-cvimmon-monitor(Username:admin)    |
| Grafana-Password-stacker1(Username:admin)           |
| Grafana-Password-stacker2(Username:admin)           |
| Prometheus-Password-cvimmon-monitor(Username:admin) |
| Prometheus-Password-stacker1(Username:admin)        |
| Prometheus-Password-stacker2(Username:admin)        |
+-----------------------------------------------------+
```

After fetching the secret keys, execute *get-password* command with secret key to view the configured password for the service.

```
# ./bootstrap/k8s-infra/k8s_runner.py --get-password "Grafana-Password-cvimmon-monitor(Username:admin)"

+-----------------------------------------------------+----------------------------------------------+
|                   Secret Key                        |                  Password                    |
+-----------------------------------------------------+----------------------------------------------+
| Grafana-Password-cvimmon-monitor(Username:admin) | k2nP8mKR2oHqBrXUEZbaqepa/ahAshKmoAJ+hghW9Is= |
+-----------------------------------------------------+----------------------------------------------+
```

Secret key must be provided in double quotes ("") with *--get-password* cli.

Regenerate Secrets

To regenerate passwords for all stacks at once, use the following command

```
./bootstrap/k8s-infra/k8s_runner.py --regenerate-secrets

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --regenerate-secrets
The logs for this run are available at /var/log/cvimmonha/2019-10-22_120629_288207

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/2][VALIDATION: INIT]                                                  [   -   ]    0min 2secs

 Input File Validations!
+-----------------------------------+--------+-------+
| Rule                              | Status | Error |
+-----------------------------------+--------+-------+
| Schema Validation of Input File   |  PASS  | None  |
| Check for Valid Keys              |  PASS  | None  |
| Valid Operation Check             |  PASS  | None  |
| Pod operations for CVIM-MON-HA    |  PASS  | None  |
| Check for duplicate keys          |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature |  PASS  | None  |
| Check duplicate Cvim-Mon target   |  PASS  | None  |
| Information                       |        |       |
+-----------------------------------+--------+-------+
[1/2][VALIDATION: INIT]                                                  [ DONE! ]    0min 3secs

Ended Installation [VALIDATION] [Success]

[2/2][HELM_INFRA: INIT]                                                  [ DONE! ]    0min 2secs
[2/2][HELM_INFRA: nginx-ingress-controller-Check whether helm binary exi...   [ DONE! ]    0min 3secs
[2/2][HELM_INFRA: prometheus-stack1->Check Rollout Status of Prometheus-...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Check the status of Prometheus-stac...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Ensure Prometheus-stack1 Deployment...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Clear the old-version file]              [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Faile the update if rollback was du...   [ DONE! ]    1min 12secs

Ended Installation [HELM_INFRA] [Success]

Executing autobackup for CVIM MON
Executing autobackup at :/var/cisco/cvimmonha_autobackup/cvimmonha_autobackup_3.3.20_2019-10-22_12:07:46
[DONE] autobackup of CVIM MON HA Node successfully.
The logs for this run are available at /var/log/cvimmonha/2019-10-22_120629_288207
```

Custom Secrets

You can set custom passwords for Grafana, Prometheus, Alertmanager applications in each stack. To configure custom passwords, use the below command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --list-secrets stacker1
+-------------------------------------------+
| Secret Keys                               |
+-------------------------------------------+
| Grafana-Password-stacker1(Username:admin)    |
| Prometheus-Password-stacker1(Username:admin) |
+-------------------------------------------+
```

To change password, create a new yaml file and the key you want to set password for:

For example:

To change password for *Grafana-Password-stacker1,* create a file and update the file with following:

```
Grafana-Password-stacker1(Username:admin): "<New Password>"
```

⚠ Ensure that you use the same key name as shown in the output including "Username:admin", otherwise command is not executed.

Password Policy

1. Only alphanumeric and special characters are allowed for secrets
2. Passwords must contain at least 1 letter, 1 special character, 1 digit, without blank spaces.
3. Password length must be >=8 and <= 44.
4. Allowed special characters [_@./#+-=]

Save the yaml file where you entered the custom password and execute the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --set-secrets <path to yaml file>

[root@queensland installer-22898]# ./bootstrap/k8s-infra/k8s_runner.py --set-secrets /path/to/yaml/file
The logs for this run are available at /var/log/cvimmonha/2019-10-22_120629_288207

                        ############################
                         CVIM MON HA ORCHESTRATOR
                        ############################

[1/2][VALIDATION: INIT]                                                    [   -   ]    0min 2secs

 Input File Validations!
+-----------------------------------+--------+-------+
| Rule                              | Status | Error |
+-----------------------------------+--------+-------+
| Schema Validation of Input File   |  PASS  | None  |
| Check for Valid Keys              |  PASS  | None  |
| Valid Operation Check             |  PASS  | None  |
| Pod operations for CVIM-MON-HA    |  PASS  | None  |
| Check for duplicate keys          |  PASS  | None  |
| Check Cvim-Mon Target Nomenclature |  PASS  | None  |
| Check duplicate Cvim-Mon target   |  PASS  | None  |
| Information                       |        |       |
+-----------------------------------+--------+-------+
[1/2][VALIDATION: INIT]                                                    [ DONE! ]    0min 3secs

Ended Installation [VALIDATION] [Success]

[2/2][HELM_INFRA: INIT]                                                    [ DONE! ]    0min 2secs
[2/2][HELM_INFRA: nginx-ingress-controller-Check whether helm binary exi...   [ DONE! ]    0min 3secs
[2/2][HELM_INFRA: prometheus-stack1->Check Rollout Status of Prometheus-...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Check the status of Prometheus-stac...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Ensure Prometheus-stack1 Deployment...   [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Clear the old-version file]           [ DONE! ]    1min 8secs
[2/2][HELM_INFRA: prometheus-stack1->Faile the update if rollback was du...   [ DONE! ]    1min 12secs

Ended Installation [HELM_INFRA] [Success]

Executing autobackup for CVIM MON
Executing autobackup at :/var/cisco/cvimmonha_autobackup/cvimmonha_autobackup_3.3.20_2019-10-22_12:07:46
[DONE] autobackup of CVIM MON HA Node successfully.
The logs for this run are available at /var/log/cvimmonha/2019-10-22_120629_288207
```

Updating Nodes

Updating Software of HA CVIM MON Nodes

You can update the software of HA CVIM-MON nodes using the following three actions:

Action	Description
Update	Gets the new software version and updates the HA CVIM-MON software in the nodes.
Rollback	Rolls back to the previous version of the software if there are problems after the software update.
Commit	Commits the software update. You cannot roll back to an older version after you commit the software.

Update

An update is an initial phase used to update the software on the HA CVIM-MON nodes. The update action performs the following operations:

- Downloads the new software version and the container images.
- Updates the software and containers in the management nodes.
- Updates the software in the HA CVIM-MON master and worker nodes.
- Updates the HA CVIM-MON stacks running on the nodes.

Following are the steps to update the software of HA CVIM-MON nodes:

1. Get the new installer tar.
2. Extract the tar to the root directory by using the following command:

```
tar --no-same-owner -xvzf mercury-installer.tar.gz
```

3. Change to the new workspace and update the HA CVIM-MON software by using the following command:

```
cd /root/<new_ws>
./bootstrap/k8s-infra/k8s_runner.py --update
```

4. After the update finishes, you can verify the update by checking the *root/openstack-configs* directory. It shows the new workspace.

```
ls -rtl /root/openstack-configs
lrwxrwxrwx. 1 root root 46 Oct 3 11:46 /root/openstack-configs -> /root/<new_ws>
```

Rollback

A rollback rolls back to the previous software version if there are problems after the software update. The rollback action performs the following operations:

- The containers in the management node are rolled back to the previous software version, but the repo containers are not rolled back.
- The HA CVIM-MON stacks are rolled back to the previous software version.

Following are the steps to rollback the software of HA CVIM-MON nodes:

1. Move to the previous workspace where the software version is running by using the following command:

```
# cd /root/<new_ws>
```

2. Use the rollback command to rollback the HA CVIM-MON software to the older version:

```
# ./bootstrap/k8s-infra/k8s_runner.py --rollback
```

3. After the rollback is done, you can verify the rollback by checking the *root/openstack-configs* directory. It shows the old workspace.

```
# ls -rtl /root/openstack-configs
lrwxrwxrwx. 1 root root 46 Oct 3 11:46 /root/openstack-configs -> /root/<old_ws>
```

Commit

This action commits the software update of the HA CVIM-MON nodes. You cannot rollback to an older version after you commit the software.
The commit action performs the following operations:

- The old version of the software running in the containers of the management node is removed.
- The software version of the HA CVIM-MON stacks is committed to the running version.
- All intermediate files and temporary files are removed.

Following are the steps to commit the software of HA CVIM-MON nodes:

1. Move to the new workspace from where HA CVIM-MON is running by using the following command:

```
# cd /root/<new_ws>
```

2. Use the commit command to commit the HA CVIM-MON software to the newer version:

```
# ./bootstrap/k8s-infra/k8s_runner.py --commit
```

Custom Grafana Dashboards

Custom Grafana Dashboards for HA CVIM MON

Overview

HA CVIM-MON allows you to create and persist custom dashboards. After you create new dashboards or makes changes in Grafana, you can save the work and persist the new or updated dashboards in the custom dashboard repository located in the management node.
As you cannot modify or persist built-in dashboards, ensure that you duplicate the built-in dashboards and edit the copies as custom dashboards.

Following options are supported:

```
# ./bootstrap/k8s-infra/k8s_runner.py -h

--cvimmon-custom-dashboards
                        Local CVIM MON custom dashboard
  --save-dashboard      Persist Custom Dashboards
  --list-dashboard      List Custom Dashboards
  --upload-dashboard    Upload Custom Dashboards
  --force             Force option to delete custom dashboards with upload op.
  --preserve            Only works with upload option. If passed all existing dashboards will be preserved with
new dashboards.
  --dir-path DIR_PATH   Dir path from where custom dashboards will be uploaded to grafana
  --dry-run             To view what changes will be made on grafana. No actual changes will be made.
  --stack-name STACK_NAME
                        Stack name for which info for dashboards is required.
```

--cvimmon-custom-dashboards is required if you want to execute any operation related to custom dashboards.
--stack name is required to specify which stack is targeted for the custom dashboard operation.

You can perform the following actions on the custom dashboards:

- Listing custom dashboards
- Saving custom dashboards

Listing Custom Dashboards

To list the custom dashboard per stack, use the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --cvimmon-custom-dashboards --list-dashboard --stack-name stack3
```

The above example lists out all the custom dashboards on the stack3 namespace.

Saving Custom Dashboards from Grafana to Management Node

The save dashboard operation synchronizes all custom dashboards from the Grafana server to the management node repository.
To save custom dashboards from Grafana to the management node, use the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --cvimmon-custom-dashboards --save-dashboard --stack-name <stack_name>
```

During the sync operation if there is a dashboard present on the management node repository and not on the Grafana server (for example, if the dashboard has been deleted from Grafana):

- The command succeeds and deletes the stale dashboard in the management node repository if *--force* passes.

You can copy all custom dashboards to any user-provided and user-managed empty directory on the management node if *--dir-path* is provided. This option is useful if you want to version and save all the custom dashboards in a version control system (for example, Git).

This operation succeeds only if the Grafana server and management node repository are in sync. Hence, a sync operation is required before copying the custom dashboards to a user directory.

Following is an example of the *--dir-path* option:

```
# ./bootstrap/k8s-infra/k8s_runner.py --cvimmon-custom-dashboards --save-dashboard --stack-name <stack_name> --
dir-path /root/sync_dash/
```


If you pass the *--dry-run* option to any of these options, you can see relevant logs but no actual sync operation between the Grafana server and the management node repository.

Cisco VIM does not persist Grafana dashboard folders.

Uploading Custom Dashboards from Management Node to Grafana Server

The upload dashboard operation synchronizes the management node repository with the Grafana server. You can use either the *--force* or *--preserve* optio n if only one or more dashboards are present in Grafana.

If you use the *--force* option, Cisco VIM deletes all existing custom dashboards in the Grafana server and uploads all dashboards in the management node repository to the Grafana server. Cisco VIM deletes only the dashboards present in the Grafana server.

If you use the *--preserve* option, Cisco VIM preserves all existing dashboards. If it encounters a dashboard with the same name, the saved dashboard from the management node repository overwrites the one on the Grafana server. Cisco VIM preserves only dashboards present in the Grafana server.

To upload custom dashboards from a user-managed directory to the management node repository and the Grafana server, use the *--dir-path* option. This functionality works only when the Grafana server and the management node repository are in sync.

Following is an example of the *--force* option:

```
# ./bootstrap/k8s-infra/k8s_runner.py --cvimmon-custom-dashboards --upload-dashboard --dir-path /root
/sync_dash/ --stack-name <stack_name> --force
```

Following is an example of the *--preserve* option:

```
# ./bootstrap/k8s-infra/k8s_runner.py --cvimmon-custom-dashboards --upload-dashboard --dir-path /root
/sync_dash/ --stack-name <stack_name> --preserve
```

The above options are useful if you want to upload a new set of custom dashboards from a git repository onto a newly deployed HA CVIM-MON stack.

If you use the *--dry-run* option to run the operations without actual sync, you can see logs for operations between the Grafana server and the management node.

Alert Rules

Customizing Alerting Rules

Overview

Alerting rules define how alerts must be triggered based on conditional expressions on any available metric.

You can view the alerts from the Grafana user interface or Alerting dashboard or send them optionally to a number of supported receivers. After deployment, the pod administrators can customize the alerting rules based on their requirements.

For example, you can trigger an alert when any performance metric such as CPU usage, network throughput, or disk usage reaches a certain threshold. HA CVIM-MON has a set of default built-in alerting rules that cover the most important error conditions that can occur in the pod.

You can customize alerting rules by using the following steps:

- Create a custom alerting rules configuration file to add new rules, modify, or delete built-in rules.
- Verify that the custom alerting rules file is valid using a verification tool.
- Update the alerting rules by applying the custom alerting rules file.

Update Alerting Rules

The update operation for alerting rules always merges the following two files:

- Default alerting rules file (built-in file)
- Custom alerting rules file

Applying a second custom alerting rules file does not preserve alerting rules from the previously applied custom alerting rules file. The update operation does not include previously applied custom alerting rules.

To update the alerting rules, run the *k8s_runner.py* command with the *--alerting_rules_config* option, path to the *custom_alerting_rules.yml* file and a name of the stack for which the operation needs to be performed.

For example:

```
# ./bootstrap/k8s-infra/k8s_runner.py --alerting_rules_config /root/custom_alerting_rules.yaml --stack-name
<stack_name>
```

The merge tool output file consists of:

- All rules from the *custom_alerting_rules.yml* file that do not belong to the *change-rules* or *delete-rules* group.
- Rules from the *default_alerting_rules.yml* that:
    - Do not duplicate rules from custom file.
    - Must not be deleted.
    - Are modified according to *change-rules* input.

Format of Custom Alerting Rules File

The format of *custom_alerting_rules.yml* is identical to the one used by the Prometheus configuration file with a few additional semantic extensions to support the deletion and modification of pre-built existing rules.

The groups entry contains a list of groups identified by **group_name**, where each group can include one or more rules. The labels are used for determining the severity and other SNMP trap attributes.
The limitations when setting labels are given below:

- You must set the values of **severity**, **snmp_fault_code**, and **snmp_fault_severity** to the values specified in the example below.
- You must set the value of **snmp_fault_source** to indicate the metric used in the alert expression.
- You must not change the value of **snmp_node**.
- You must set the value of **snmp_podid** as the pod name specified in the *setup data* file.

```
groups:
- name: {group_name}
  rules:
  - alert: {alert_name}
    annotations:
      description: {alert_description}
      summary: {alert_summary}
    expr: {alert_expression}
    for: {pending_time}
    labels:
      severity: {informational/warning/critical}
      snmp_fault_code: {other/resourceUsage/resourceThreshold/serviceFailure/hardwareFailure
/networkConnectivity}
      snmp_fault_severity: {emergency/critical/major/alert/informational}
      snmp_fault_source: {fault_source}
      snmp_node: '{{ $labels.instance }}'
      snmp_podid: {pod_id}
```

Adding Alert Rules

Any alert rule specified under a group that is not named *change-rules* or *delete-rules* is populated to the merged output file. Custom rules are prioritized over the preexisting rules. If there are two alerts with the same name in both files, only the one from the custom file is retained as a result of the merge.

Modifying Alert Rules

You can modify any preexisting rule using the following syntax:

```
groups:
- name: change-rules
  rules:
  - alert: {alert_name}
    expr: {new_alert_expression}
    annotations:
      summary: {new_alert_summary}
```

The merge script looks only for a group named *change-rules* and changes the expression or summary of the updated alert.
If the alert to be changed does not exist, it is not created and changes are not made.

Deleting Alert Rules

You can delete any built-in rule by using the following construct in the *custom_alerting_rules.yml* file:

```
groups:
- name: delete-rules
  rules:
  - alert: {alert_name/regular_expression}
```

The merge script looks only for a group named *delete-rules* and deletes pre-existing rules that match the provided names or regular expressions.
If the alert to be deleted does not exist, changes are not made.

The following custom configuration file includes examples of a new alerting rule, a modified alerting rule and a deleted alerting rule:

```
groups:
- name: cpu
  rules:
  - alert: cpu_idle
    annotations:
      description: CPU idle usage is too high - resources underutilized
      summary: CPU idle too high
    expr: cpu_usage_idle > 80
    for: 5m
    labels:
      severity: informational
      snmp_fault_code: resourceUsage
      snmp_fault_severity: informational
      snmp_fault_source: cpu_usage_idle
      snmp_node: '{{ $labels.instance }}'
      snmp_podid: pod7
  - alert: cpu_iowait
    annotations:
      description: CPU iowait usage is too high
      summary: CPU iowait too high
    expr: cpu_usage_iowait > 10
    for: 3m
    labels:
      severity: warning
      snmp_fault_code: resourceUsage
      snmp_fault_severity: alert
      snmp_fault_source: cpu_usage_iowait
      snmp_node: '{{ $labels.instance }}'
      snmp_podid: pod7
- name: change-rules
  rules:
  - alert: disk_used_percent
    expr: disk_used_percent > 99
    annotations:
      summary: Disk used > 99%
  - alert: reboot
    annotations:
      summary: Server rebooted
  - alert: system_n_users
    expr: system_n_users > 10
- name: delete-rules
  rules:
  - alert: disk_filling_up_in_4h
  - alert: mem.*
```

Validation Script for Custom Alerting Rules

You must validate any custom alerting rules file before an updation using the following CLI command:

```
/opt/cisco/check_promtool.py -v <custom_alerts_file>
```

The validation script uses the Prometheus *promtool* script but skips some of its checks to allow updation and deletion of rules. It also checks if the SNMP severities and fault codes are supported.

The following example shows the output of the *promtool* script in case of a successful validation:

```
# /opt/cisco/check_promtool.py -v /root/alerting_custom_rules.yaml
check_promtool.py: checking /root/alerting_custom_rules.yaml
check_promtool.py: success:
check_promtool.py:  rules to be changed: 2
check_promtool.py:  rules to be added: 2
```

The following example shows the output of the *promtool* script in case of a failure:

```
# /opt/cisco/check_promtool.py -v /root/alerting_custom_rules.yaml
check_promtool.py: checking /root/alerting_custom_rules.yaml
check_promtool.py: failure:
check_promtool.py:    line 22: field for already set in type rulefmt.Rule
check_promtool.py:    line 23: field labels already set in type rulefmt.Rule
```

Alert Manager

Customizing Alert Manager and Receivers

Overview

The Alert Manager component in CVIM-MON is in charge of the routing, grouping, and inhibiting alerts that are sent by the Prometheus alert rule engine to the appropriate receivers.
By default, CVIM-MON forwards each alert to the SNMP agent to be sent to the SNMP managers as SNMP traps, if enabled in the configuration file.
After deployment, you can add custom alert routes, alert grouping, alert inhibitions and receivers by following the below steps:

1. Create a proper custom alerting rules configuration file:
    a. Create a custom alert manager rule configuration file named alertmanager_custom_config.yml.
    b. Edit the content using your favorite editor (see format below).
    c. Verify that the custom alerting rule file is valid using the provided tool.
2. Once the file is validated, you can execute the following command:

```
# ./bootstrap/k8s-infra/k8s_runner.py --alertmanager_config <alertmanager_config_file> --stack-name
<stack_name>
```

Supported Receivers

The Alert Manager supports the following list of receivers:

- webhook
- pagerduty
- e-mail
- pushover
- wechat
- opsgenie
- victorops

Alert Manager Custom Configuration File Format

General Format
The following listing shows the general format of the alert manager configuration file. Most custom configuration files must include only a small subset of the available options.
global:

```
# ResolveTimeout is the time after which an alert is declared resolved # if it has not been updated.
[ resolve_timeout: <duration> | default = 5m ]

# The default SMTP From header field. [ smtp_from: <tmpl_string> ]
# The default SMTP smarthost used for sending emails, including port number.
# Port number usually is 25, or 587 for SMTP over TLS (sometimes referred to as STARTTLS).

# Example: smtp.example.org:587 [ smtp_smarthost: <string> ]
# The default hostname to identify to the SMTP server. [ smtp_hello: <string> | default = "localhost" ]
[ smtp_auth_username: <string> ]
# SMTP Auth using LOGIN and PLAIN. [ smtp_auth_password: <secret> ]
# SMTP Auth using PLAIN.
[ smtp_auth_identity: <string> ] # SMTP Auth using CRAM-MD5.
[ smtp_auth_secret: <secret> ]
# The default SMTP TLS requirement.
[ smtp_require_tls: <bool> | default = true ]

# The API URL to use for Slack notifications. [ slack_api_url: <secret> ]
[ victorops_api_key: <secret> ]
[ victorops_api_url: <string> | default = "https://alert.victorops.com/integrations/generic/20131114/alert/" ]
[ pagerduty_url: <string> | default = "https://events.pagerduty.com/v2/enqueue" ] [ opsgenie_api_key: <secret> ]
[ opsgenie_api_url: <string> | default = "https://api.opsgenie.com/" ] [ hipchat_api_url: <string> | default =
"https://api.hipchat.com/" ]  [ hipchat_auth_token: <secret> ]
[ wechat_api_url: <string> | default = "https://qyapi.weixin.qq.com/cgi-bin/" ] [ wechat_api_secret: <secret> ]
[ wechat_api_corp_id: <string> ]

# The default HTTP client configuration [ http_config: <http_config> ]
# Files from which custom notification template definitions are read.
# The last component may use a wildcard matcher, e.g. 'templates/*.tmpl'. templates:
[ - <filepath> ... ]

# The root node of the routing tree. route: <route>

# A list of notification receivers. receivers:
- <receiver> ...

# A list of inhibition rules. inhibit_rules:
[ - <inhibit_rule> ... ]
```

The custom configuration must be a full working configuration file with the following template. It must contain three main keys such as global, route, and receiver.
The global configuration must have at least one attribute, for example, resolve_timeout = 5m. Ensure that all new receivers must be part of the route, so the alerts are routed to the proper receivers. The receiver name cannot be snmp.
You can find the configuration details for creating route/receiver in the Prometheus Alert Manager documentation (publicly available online).

```
global: resolve_timeout: 5m

route: <route>

receivers:
- <receiver> ...

The following is a custom config to add a webhook receiver.

global:
  resolve_timeout: 5m

route:
  group_by: ['alertname', 'cluster', 'service']
  group_wait: 30s
  group_interval: 5m
  repeat_interval: 8737h
  receiver: receiver-webhook

receivers:
- name: 'receiver-webhook'
  webhook_configs:
  - send_resolved: true
    url: 'http://webhook-example:####/xxxx/xxx'
```

Default Built-in Configuration File

Two different default configuration files are available to define the following in order:

1. Generic route for all alerts to the SNMP agent running on the management node.
2. Route to a generic receiver that can be customized to add a channel of notification (webhook, slack and others).

Default configuration file with SNMP enabled

```
:
global:
  resolve_timeout: 5m

route:
  group_by: ['alertname', 'cluster', 'service']
  group_wait: 30s
  group_interval: 5m
  repeat_interval: 8737h

  # A default receiver
  receiver: snmp

receivers:
- name: 'snmp'
  webhook_configs:
  - send_resolved: true
    url: 'http://localhost:1161/alarms'
```

Default configuration file with SNMP disabled

```
route:
  receiver: recv
  group_by:
  - alertname
  - cluster
  - service
  group_wait: 30s
  group_interval: 5m
  repeat_interval: 8737h
receivers:
- name: recv
```

SNMP Trap Receivers

You can send the SNMP traps to SNMP managers enabled in the Cisco VIM configuration file setup_data.yaml.

Example: inhibit (mute) alerts matching a set of labels
Inhibit alerts is a tool that prevents certain alerts to be triggered if other alert/alerts is/are trigged. If one alert having the target attribute matches with the another alert having source attribute, this tool inhibits the alert with target attribute.
This is the general format for inhibit alerts. You can set a regex to match both the source and target alerts and to filter the alerts per label name.

```
# Matchers that have to be fulfilled in the alerts to be muted.
target_match:
  [ <labelname>: <labelvalue>, ... ]
target_match_re:
  [ <labelname>: <regex>, ... ]

# Matchers for which one or more alerts have to exist for the
# inhibition to take effect.
source_match:
  [ <labelname>: <labelvalue>, ... ]
source_match_re:
  [ <labelname>: <regex>, ... ]

# Labels that must have an equal value in the source and target
# alert for the inhibition to take effect.
[ equal: '[' <labelname>, ... ']' ]
```

Example: Inhibit alerts if other alerts are active

The following is an example of inhibit rule that inhibits all the warning alerts that are already critical.

```
inhibit_rules:
- source_match:
    severity: 'critical'
  target_match:
    severity: 'warning'
  # Apply inhibition if the alertname is the same.
  equal: ['alertname', 'cluster', 'service']
```

This is an example of inhibit all alerts docker_container in containers that are down (which has the alert docker_container_down on).

```
inhibit_rules:
  - target_match_re:
      alertname: 'docker_container.+'
    source_match:
      alertname: 'docker_container_down'
    equal: ['job', 'instance']
```

Validation Script

When a new configuration is set, execute amtool script and ensure that you get a SUCCESS in the output from the configuration POV.

```
> /opt/cisco/amtool check-config <alertmanager_config_file>
Checking '<alertmanager_config_file>'  SUCCESS
Found:
 - global config
 - route
 - 0 inhibit rules
 - 1 receivers
 - 0 templates
```

Backup

Backing Up HA CVIM-MON

Overview

Backup of the management node is useful to recover from any situation where the management node has a catastrophic failure.

The HA CVIM-MON management node can be backed up in two ways:

- automatically through cluster management operations that change the state of the cluster (for example, commit following an update)
- manually

In any case, the backup operation creates a backup directory locally. Ensure that you copy this directory from the management node to a safe location.

Auto-backup initiates only if the last executed operation changes the cluster state and completes in the success state. Also, backup is not started if the CVIM-MON pod is in the middle of an update.

Backup executes only from the workspace from where HA CVIM-MON is deployed.

Manual Backup

Navigate to *<installer-ws>/bootstrap/k8s-infra/cvimmon_backup*. The following example shows how to perform a manual backup:

```
# ./cvimmon_ha_backup.py --backup

Backup dir: /var/cisco/cvimmonha_backup/<backup_dir>
Log dir: /var/log/cvimmonha_backup/<log_file name>
```

Information about the backup directory and log file appears in the console after the execution of the operation. To see details of the backup operation use *--debug* option along with the execution script.

Auto Backup

After successful completion of any state change operation, k8s_runner.py executes an auto-backup.

Following options do not execute auto-backup:

- --renew-k8s-certs
- --renew-etcd-certs
- --update (backup is done on the commit following the update)

The auto-backup directory is located at:

```
/var/cisco/cvimmonha_autobackup/<backup_dir>
```

The log directory is located at:

```
/var/log/cvimmonha/<uuid>/mercury_baremetal_install.log
```

Saving Backup Directory out of the Management Node

After each successful backup, you must move the created backup directory to a well-defined remote location, so that it can be used later when needed while restoring a management node.

Restore

Restoring HA CVIM-MON

Overview

You can restore a previous backup of the management node, typically after replacing the management node server and reinstalling it with the management node ISO.

The restore operation restores the state of the management node back to the backed up state.

Pre-requisites

Before you restore HA CVIM-MON, ensure that the following conditions are met:

- You must create the backup directory for recovery, from an HA CVIM-MON version that is identical to the version of the management node ISO being used to reinstall the management node.
- Timezone, hostname, and IP configuration for the management node must be identical to the backup. If not, the restoration fails.
- You must execute restore from the */var/cisco/* directory.
- You must not modify the backup directory. If modified, the restoration fails.

Restoring Management node from Backup

After the ISO installation:

- Copy the backup directory from the remote backup server to the management node under */var/cisco/cvimmon_backup*. You can skip this step if your backup directory is still present from the previous backup run.
- Navigate to the backup directory (*/var/cisco/cvimmonha_backup/<backup-folder>*) and execute the following command:

```
./cvimmon_restore
```

To view detailed messages, add *--v* parameter to the *cvimmon_restore* script.

After Cisco VIM restores all the necessary configuration data on the management node, the script initiates the first three steps of installation:

```
!!  CVIM MON HA ORCHESTRATOR  !!
=========================================
+------------------------+--------------------+
| Operations             | Operation ID       |
+------------------------+--------------------+
| VALIDATION             |      1             |
| BOOTSTRAP_INFRA        |      2             |
| SETUP_ARGUS            |      3             |
```

After a successful completion of the restore operation, you can execute the *kubectl get pods --all-namespaces* command and see if all the pods are in the running state.

You can also verify by logging into Grafana using the old password and confirm if all the data is visible.

Reinstallation of CVIM-MON HA Pod

Reinstallation of CVIM-MON HA Pod

Due to unforeseen circumstances, there might be a need to reinstall the CVIM MON HA pod with the same image version. To alleviate the need for reimaging the management node followed by re-installation of the CVIM MON HA pod, reinstall the pod under the assumption that the management node is compatible with the same tag.

> ⚠ For reinstallation, ensure that you use the same target CVIM-MON servers in which the original installation is done. If you are using a different or subset of servers for reinstallation, power off the servers in which the previous installation is done, to prevent floating of the duplicate IPs in the network.

Listed below are the steps to reinstall the pod without reimaging the management node for CVIM MON HA:

1. Copy the *setup_data.yaml* from */root/openstack-configs/* directory to *~/Save/*

   ```
   cd ~/installer-<x.x.x>
    ./cvim_mon_ha_unbootstrap.sh -k
   ```

2. To verify that no docker containers are running, use the command:

   ```
   docker ps -a
   ```

3. To verify that no docker images are present, use the command:

   ```
   docker images
   ```

4. To re-run the Cisco VIM MON HA installation, use the command:

   ```
   cd ~/installer-<xxx>
   ./bootstrap/k8s-infra/k8s_runner.py --install --setupfile ~/Save/setup_data.yaml
   ```

CVIM MON HA Cluster Monitoring

CVIM MON HA Cluster Monitoring

Overview

HA CVIM-MON has an inbuilt mechanism to monitor the cluster itself apart from monitoring the Cisco VIM pods. The HA CVIM-MON cluster is made up of kubernetes master and kubernetes workers. The objective of the cluster monitor is to monitor the health of the entire kubernetes cluster. The cluster monitor provides the following information.

1. Health of the cluster.
2. Resource utilization of the nodes.
3. Status of various Kubernetes objects.
4. Portworx (Storage) monitoring
5. Alerts for various conditions.

Components of HA CVIM-MON Cluster Monitoring

The HA CVIM-MON cluster monitor uses the following components to monitor the kubernetes cluster:

1. Kube-state-metrics.
2. cAdvisor
3. Node-exporter
4. Prometheus to collect metrics .
5. Grafana to display the metrics.

All the tools for monitoring the cluster run under the *cvimmon-monitor* namespace.

Cluster Monitoring Endpoint URL's

To get information about cluster monitoring endpoint service URLs, use the following command:

```
# kubectl get ingress -n cvimmon-monitor
NAME HOSTS ADDRESS PORTS AGE
grafana-cvimmon-monitor ha-cluster-1-cvimmon-grafana.cisco.com 80, 443 37m
prometheus-cvimmon-monitor-alertmanager ha-cluster-1-cvimmon-alertmanager.cisco.com 80, 443 38m
prometheus-cvimmon-monitor-server ha-cluster-1-cvimmon-prometheus.cisco.com 80, 443 38m
```

The prefix *ha-cluster-1* is the name of the cluster given in the *setup_data.yaml* under the section ARGUS_BAREMETAL.

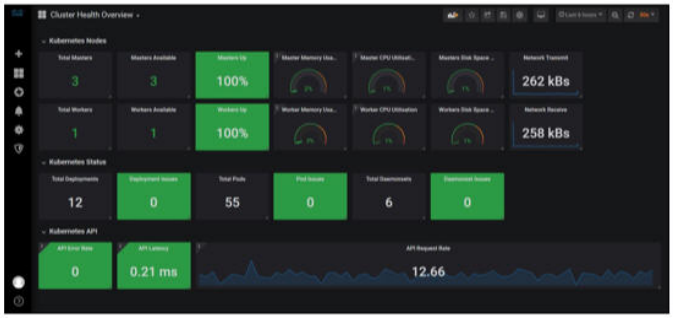
Secrets for HA CVIM-MON Cluster Monitoring

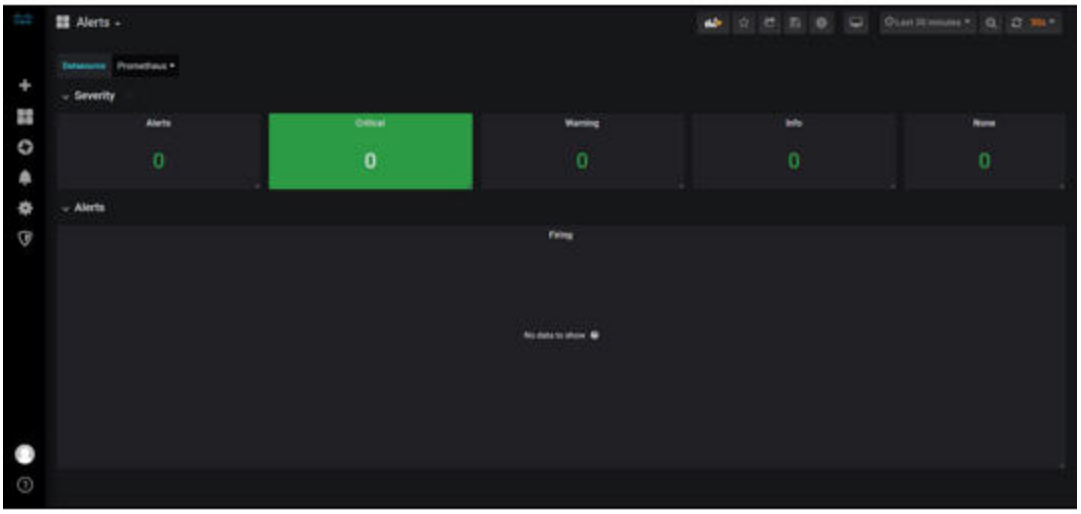
To get the secrets for the HA CVIM-MON cluster monitor, use the following commands:

```
Grafana Dashboard
# ./bootstrap/k8s-infra/k8s_runner.py --get-password "Grafana-Password-cvimmon-monitor(Username:admin)"

+-------------------------------------------------+-------------------------------------------+
| Secret Key                                      | Password                                  |
+-------------------------------------------------+-------------------------------------------+
| Grafana-Password-cvimmon-monitor(Username:admin) | vpUphAfQF6EMcZeWfGIA7fnXk8Gs7zqqFKo8npWjWLk= |
+-------------------------------------------------+-------------------------------------------+

Prometheus Dashboard
# ./bootstrap/k8s-infra/k8s_runner.py --get-password "Prometheus-Password-cvimmon-monitor(Username:admin)"

+-------------------------------------------------+-------------------------------------------+
| Secret Key                                      | Password                                  |
+-------------------------------------------------+-------------------------------------------+
| Prometheus-Password-cvimmon-monitor(Username:admin) | w7NTKssuaeOgKT/RB+VInZVR9vHGtn8BzpA8GDr8vow= |
+-------------------------------------------------+-------------------------------------------+
```

Grafana Dashboards

The grafana dashboards can be accessed with the URL from the above step. Some of the Dashboards in cluster monitoring are shown below:





Alerts

The alerts are generated based on the predefined alerting rules. The predefined alerting rules are triggered based on the metrics obtained by the Prometheus server. The alerts can be monitored using the web interface or api. Some of the common alerts are mentioned in the table below:

Alert	Severity	Description
KubeAPIDown	critical	KubeAPI Server is down in some of the nodes.
KubeStateMetricsDown	critical	KubeStateMetrics is down.

KubeletDown	critical	Kubelet is down in one of the nodes.
NodeExporterDown	critical	NodeExporter is down.
KubePodCrashLooping	critical	Some of the pods are crash looping.
KubePodNotReady	critical	Some pods are not in the ready state even after 15 minutes.
KubeDeploymentReplicasMismatch / KubeStatefulSetReplicasMismatch	critical	The number of replicas do not match the number of replicas requested in kubernetes deployment / statefulset
KubePersistentVolumeUsageCritical	critical	The persistent volume claimed by a pod is nearing 85% of the allocated space.
KubePersistentVolumeFullInTwelveDays	critical	The persistent volume is expected to be full in twelve days.
KubeCronJobRunning / KubeJobCompletion	warning	Kubernetes CronJob / Job is running for a long time or more than 1 hour.
KubeCPUOvercommit,KubeMemOvercommit	warning	Overcommited CPU/memory resource requests on pods more than the CPU available in the nodes.
KubeNodeNotReady	warning	The node is in not ready state for more than an hour.
KubeClientErrors	warning	Kubernetes API client requests are experiencing errors.
KubeletTooManyPods	warning	The number of pods running in a node is more than the defined limit (110).
KubeClientCertificateExpiration	warning	Kubernetes API certificate is expiring in less than 15 days.
NodeDiskRunningFull	warning	The node disk will fill up within the next 24 hours.

Cisco VTS

Installing Cisco VTS

VTS Overview

VTS Overview

Understanding VTS

The Cisco Virtual Topology System (VTS) is an optional Cisco NFVI application that uses the Neutron driver and supports Cisco Vector Packet Processing. It is a standard-based, open, overlay management, and provisioning system for data center networks.

Note the following OpenStack tenant restrictions when using VTS with Cisco NFVI.

Restriction	Description
Nova flavors: VM RAM > 512MB and equal to a multiple of 512MB	This limitation is due to NUMA and huge pages.
Nova Flavors: nova flavor-key m1.medium set hw: mem_page_size=large	VHOST mode is the only mode supported by VTS installation. To support VHOST connections, nova needs the following configurations on each flavor that is used.

VTS Features

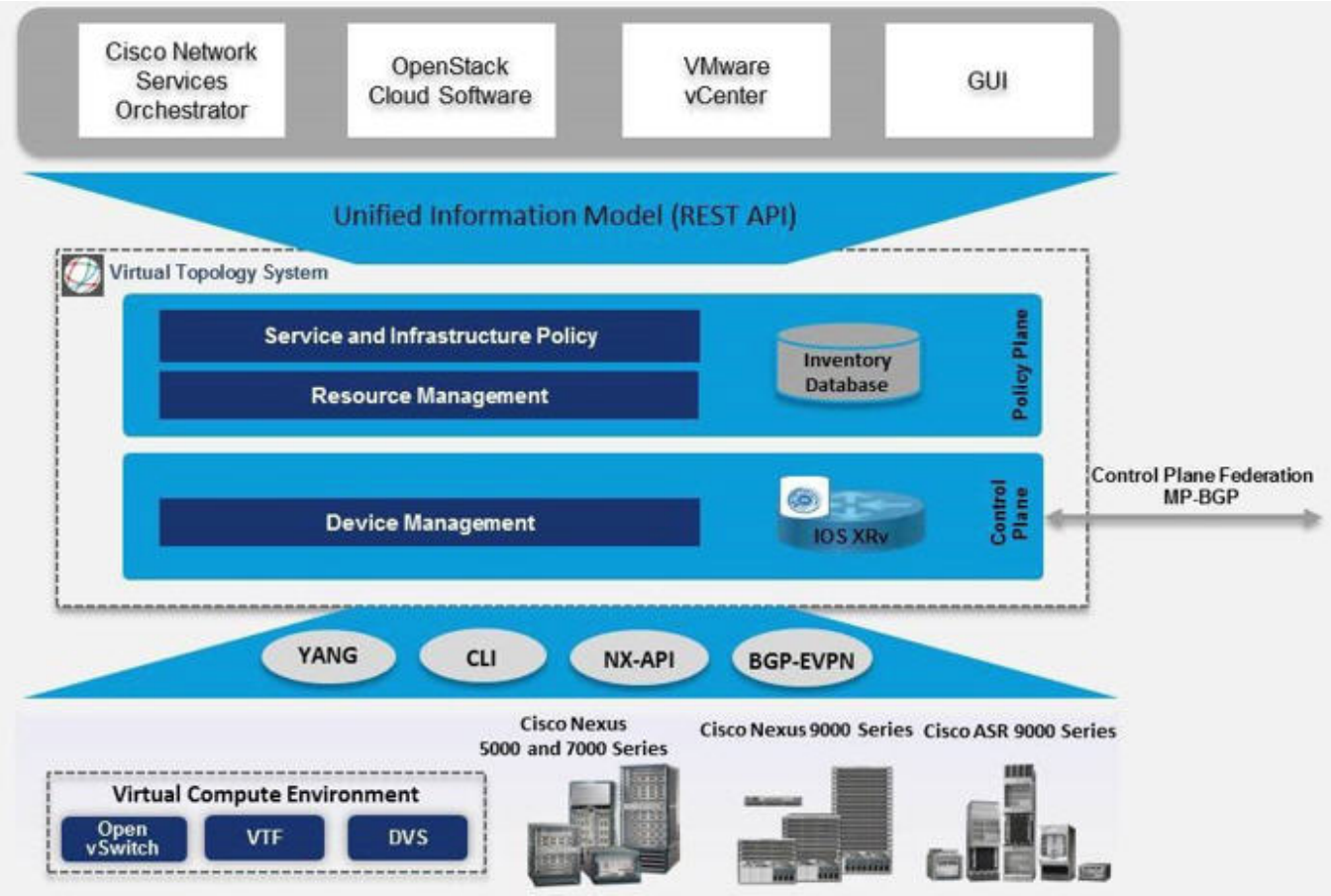
- Provides open, scalable and standards-based solution.
- Automates the data center overlay fabric provisioning for both physical and virtual workloads.
- Provides a network virtualization architecture and software-defined networking (SDN) framework that meets the requirements of multi-tenant data centers for cloud services.
- Enables a policy-based approach for overlay provisioning.
- Automates complex network overlay provisioning and management tasks through integration with cloud orchestration systems such as OpenStack and VMware vCenter.
- Reduces the complexity involved in managing heterogeneous network environments.
- Supports Cisco Nexus 2000, 3000, 5000, 7000, and 9000 series switches.
- Provides software forwarder like Virtual Topology Forwarder (VTF).

You can manage the solution in the following ways:

- Using the embedded Cisco VTS GUI.
- Using a set of northbound Representational State Transfer (REST) APIs that can be consumed by orchestration and cloud management systems.

Architecture

Cisco VTS architecture includes two main components namely the policy plane and the control plane. These components perform core functions such as SDN control, resource allocation, and core management function.



- **Policy Plane:** The policy plane enables Cisco VTS to implement a declarative policy model that is designed to capture the intent of the user into a specific device-level construct. The solution exposes a set of modular policy constructs that can be flexibly organized into user-defined services for use cases across service providers and cloud environments. These policy constructs are exposed using REST APIs that are consumed by orchestrators and applications or using the Cisco VTS GUI. The policy models are exposed as system policies or service policies.

  System policies allow administrators to logically group devices into pods within or across data centers to define admin domains with common system parameters. For example, BGP-EVPN control plane with distributed Layer 2 and Layer 3 gateways.

  The inventory module maintains a database of the available physical entities such as data center interconnect (DCI) routers, top-of-rack leaf, spine, and border-leaf switches, and virtual entities like VTF in the VTS domain. The database includes interconnections between these entities and details about the services instantiated within a VTS domain.

  The resource management module manages the available resource pools in the VTS domain including VLANs, VXLAN Network Identifiers (VNIs), IP addresses, and multicast groups.

- **Control Plane:** The control plane module serves as the SDN control subsystem that programs various data planes including VTFs residing on the x86 servers, hardware leafs, and DCI gateways. This plane hosts Service Routing (SR) module which provides routing services to Cisco VTS. The SR module calculates the L2 and L3 tables and routes, to provide connectivity between different VMs for a given tenant and service chaining. The main components of this module are Virtual Topology Service Routing (VTSR) and VTF. VTSR is the controller and VTF runs on each compute server hosting the tenant Virtual Machines (VMs).

Cisco VTS Usernames and Passwords

The following table lists the Cisco VTS usernames and passwords that are deployed after you install Cisco VTS in Cisco NFVI.

Configuration Location	Value Requirements	Description/Comments

Cisco VIM: openstack-configs /setup_data.yaml VTS_PARAMETERS: VTS_USERNAME VTS_PASSWORD VTS_SITE_UUID The following parameters are optional, only required if VTS_DAY0 is enabled. VTC_SSH_PASSWORD VTC_SSH_USERNAME VTS_SITE_UUID Optional: MANAGED	VTS_USERNAME must be admin. VTS_PASSWORD must match VTC UI login password for the admin user. Password must have a minimum of 8 characters and at least one uppercase letter, one digit, and one special character. VTS_SITE_UUID is unique UUID of VTS SITE controlled by Cisco VIM. The VTS_SITE_UUID must be in a generic UUID format (Unique Pod UUID to indicate which pod the VTS is controlling) The VTC_SSH_PASSWORD and VTC_SSH_USERNAME are ssh credentials to login to VTC VMs. MANAGED is either True or False. By default, it is false. If it is True, VTS deployment mode is managed.	Used by VTF to register with the VTC / VTSR.
VTC ISO config.txt : vts-admin Password Administrative User Administrative Password	Must match the Cisco VIM setup_data.yaml VTC_SSH_PASSWORD parameter. Administrative User must match with setup_data.yml VTC_SSH_USERNAME parameter. Administrative Password matches with VTC_SSH_PASSWORD parameter.	Configures VTC admin user's initial password. SSH username/password for VTC VM.
VTSR ISO: USERNAME PASSWORD		VTSR VM SSH username/password The VTSR adds this in **VTS Inventory > Authorization Group> vtsgroup** Device User Name associated with VTC admin user

Modes of ToR Configuration with VTS

Cisco VTS supports two modes of ToR configuration:

- Unmanaged ToR: It is the default mode of operation for VTS with Cisco VIM. VTS network inventory is added as *Unmanaged* device instead of actual ToR switches. BGP EVPN ingress replication mode mechanism is used for admin domain, but the port configuration does not push configuration to the ToR switches.
- Managed ToR: VTS network inventory is added with actual TOR switches. Control and compute nodes information is added with their corresponding interfaces connected with ToR in the VTS host inventory. BGP EVPN multicast replication mode is used for admin domain, while the port configuration enables multicast Internet Group Management Protocol (IGMP) snooping and PIM configuration for Tenant VLAN on actual ToR switches.

As the storage nodes do not have VTF, the switch ports hanging off the storage nodes are configured statically.

To maintain consistency, add the tor_info to the storage nodes in the setup_data of the pod.
Listed below is the snippet of the Multicast configuration push to Cisco Nexus 9000, when the port is configured with Tenant VLAN ID 111:

```
interface Vlan111
no shutdown
no ip redirects
ip address 22.22.22.200/24
no ipv6 redirects
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
ip igmp version 3
ip igmp static-oif 239.0.0.1
hsrp 22
ip 22.22.22.1
vlan configuration 111
ip igmp snooping static-group 239.0.0.1 interface port-channel12
ip igmp snooping static-group 239.0.0.1 interface port-channel13
ip igmp snooping static-group 239.0.0.1 interface port-channel14
```

⚠ Due to the limitation of VTS, Tenant VLAN ID needs to be selected as the lowest number in the ToR interface. If not, the multicast configuration is pushed incorrectly.

The following table lists the configurations required to enable the functionality of ToRs managed through VTS.

Configuration Location	Value Requirements	Description
CVIMmercury: openstack-configs /setup_data. yaml VTS_PARAMET ERS: MANAGED:	MANAGED: Set to True or False. By default, it is False.	MANAGED: Must be configured as True, when VTS deployment mode is managed. It is a Day 0 configuration, and cannot be enabled as a reconfigure option.
TORSWITCHINF O: CONFIGURE_T ORS	CONFIGURE_TORS: False	CONFIGURE_TORS value must be False to indicate that Cisco VIM is not configuring the ToRs. This enables the VTC to access and manage switches.
SWITCHDETAIL S:	Hostname, ssh_ip, username, and password of the switches for VTC to manage {switch_a_hostname: ethx/y, switch_b_hostname: ethx/y}	Need minimum switch details to access it.
SERVERS: <SERVER_NAM E>: tor_info:		For each server, list the tor_info associated with the server, so that VTC can manage the switch ports. Note that the storage nodes do not have VTF and hence switch ports hanging off the storage nodes are configured statically. To maintain consistency, add the tor_info to the storage nodes in the setup_data of the pod.

From an architecture point of view, the following are configured automatically in VTC node when managed ToR mode is selected in *setup_data.yaml:*

- VTS System settings and route reflectors are configured in VTC.
- Openstack Virtual Machine Manager is configured.
- Global VNI POOL is configured.
- Multicast pools are created to allocate a multicast IP address for Tenant VLAN ID.
- Authentication group is created for a device.
- ToR switches are configured under Network Inventory.
- Admin domain is created with BGP EVPN multicast replication mode for L2 and L3 Gateway.
- ToR switches and VTSR are added to L2 and L3 Gateway in the admin domain.
- Controller and Compute Node are added under host inventory with corresponding ToR interfaces.
- All VTFs are registered with VTSRs and appear under Virtual Forwarding Groups.

High Availability

The VTS solution supports redundancy with two instances running on separate hosts in an active/standby configuration.

During the initial setup, configure each instance with an underlay IP address and a virtual IP address, and use Virtual Router Redundancy Protocol (VRRP) to determine the active instance.

To ensure consistency of the control plane information and accelerate failover after a failure, synchronize the data from the active-instance with the standby instance after each transaction. Establish BGP peering based on both VTS instances for the distribution of tenant-specific routes. During the switchover, you must perform a Nonstop Forwarding (NSF) and a graceful restart to ensure that services are not disrupted.

System Requirements

System Requirements

VTC VM

The following table provides information about the minimum system requirements for the VTC virtual machine:

Requirement	Details
Disk space	48 GB
CPU	8
Memory	32 GB
Computing host	Certified with Cisco UCS B-series, Cisco UCS C-series Rack Servers

VTSR VM

The VTSR VM serves two purposes. It is required to enable VTS High Availability. It also acts as the control plane for the VTF. You need to install VTSR only if you consider enabling High Availability or if you plan to have a VTF in your set up.

The following table gives details about the minimum system requirements for the VTSR virtual machine:

Requirement	Details
Disk Space	Primary disk must be 77 GB.
CPUs	14
Memory	48 GB RAM
Computing Host	Certified with Cisco UCS B-series, Cisco UCS C-series Rack Servers

Supported VM Managers

Supported Virtual Machine Managers

You can install Cisco VTS on the following supported versions of Virtual Machine manager (VMM):

	OpenStack Liberty	OpenStack Newton/Queens
On RHEL	12.0.0; 12.0.1; 12.0.2; 12.0.3; 12.0.4; 12.0.5; 12.0.6	14.0.3 On CentOS
On CentOS	12.0.0; 12.0.1; 12.0.2	N/A

Supported Platforms

Supported Platforms

The following table provide information about the Cisco VTS supported platforms and their role.

> ⚠ VTS supports VXLAN overlays using the BGP EVPN control plane.

Role	Platform Supported
Top-of-rack (ToR) leaf switch	• Cisco Nexus 9300TX and 9300PX platform switches • Cisco Nexus 9332PQ and 93128TX switches • Cisco Nexus 9200 platform switches • Cisco Nexus 9500 platform switches
Data center spine	• Cisco Nexus 9300TX and 9300PX platform switches • Cisco Nexus 9500 platform switches • Cisco Nexus 9200 platform switches
Border leaf	• Cisco Nexus 9300TX and 9300PX platform switches • Cisco Nexus 9500 platform switches • Cisco Nexus 9200 platform switches
Data center interconnect (DCI)	• Cisco ASR 9000 Series Aggregation Services routers • Cisco Nexus 9300 platform switches
Virtual machine manager (VMM)	OpenStack Queens on RHEL versions
Hypervisor	• Red Hat Enterprise Linux 7.3 with KVM • Red Hat Enterprise Linux 7.6 • CentOS
Virtual forwarders	Cisco Virtual Topology Forwarder (VTF)

The following table lists the software images supported for the different devices.

Cisco Nexus 93xx	NX OS Release 7.0.3.I7.2 or 9.2(1)
Cisco Nexus 95xx	NX OS Release 7.0.3.I7.2 or 9.2(1)
Cisco ASR 9000	Cisco IOS XR Software Release 6.5.1.

The following table lists the VPC modes supported for different devices.

> ⚠ If Cisco Nexus 9000 series ToR is not configured with vPC related configuration, including peer-link (Multichassis EtherChannel Trunk (MCT), you must not configure vpc on the ToR. This may bring loopback interface used for NVE to admin down state.

The following table shows the supported VPC modes:

Cisco Nexus 93xx	Server VPC
Cisco Nexus 95xx	Server VPC

Virtual Topology Forwarder

Virtual Topology Forwarder

Overview

Virtual Topology Forwarder (VTF) runs on each compute server in the DC and provides connectivity to all tenant VMs hosted on the compute server. It supports both intra and inter DC/WAN connectivity. It allows Cisco VTS to terminate the VXLAN tunnels on host servers when VTF is used as a software VXLAN Tunnel Endpoint (VTEP). It is deployed as a virtual machine or in vhost mode, to deliver a high-performance software data plane on a host server.

Cisco VTS supports hybrid overlays by combining the physical and virtual endpoints into a single VXLAN segment.

VTF includes two major components namely Cisco Vector Packet Processing (VPP) and VPFA. VPFA is a Cisco agent running on each VM compute resource. VPFA is the FIB agent that receives the L2/L3 table forwarding information from VTSR to provide connectivity to the local tenant VMs that are hosted on its compute, and programs them in the VPP.

VTF/VPP Integration

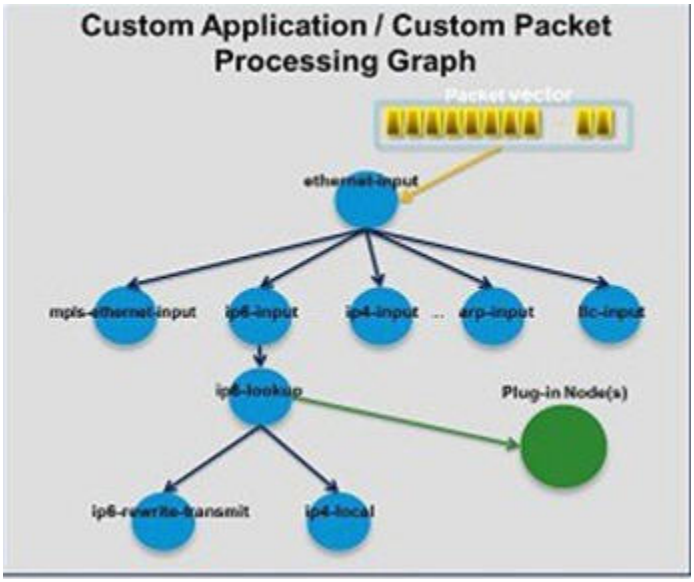
Cisco VTF is a Cisco soft switch that is built on the Cisco Vector Packet Processing (VPP) technology.

The VPP platform is an extensible framework that provides productive and quality switch or router functionality. It is the open-source version of the Cisco VPP technology which is a high performance, packet-processing stack that can run on commodity CPUs.

The benefits of VPP are its high performance, proven technology, modularity, flexibility, and rich feature set.

The VPP platform is built on a packet-processing graph. This modular approach allows you to plugin new graph nodes which improves extensibility and to customize the plugins for specific purposes.

The image below illustrates the custom packet processing graph for the VPP platform.



The VPP platform grabs all available packets from RX rings to form a vector of packets. A packet-processing graph is applied node by node (including plugins) to the entire packet vector. Graph nodes are small and modular, and loosely coupled which makes it easy to include new graph nodes and rewire the existing graph nodes.

A plugin can introduce new graph nodes or rearrange the packet-processing graph. You can also build a plugin independent of the VPP source and consider it as an independent component. You can install a plugin by adding it to a plugin directory.

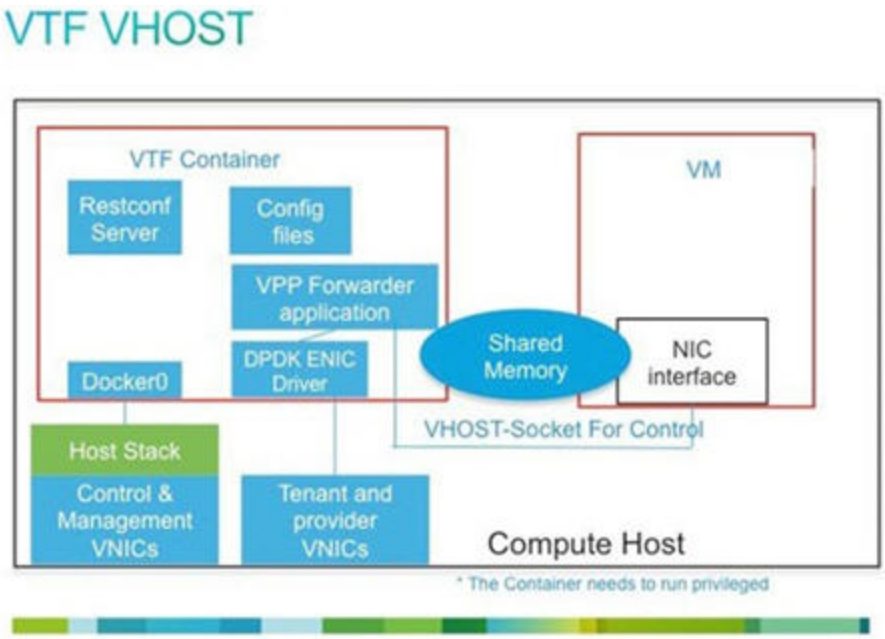
VTF uses remote plugin that binds into VPP using VPF agent (VPFA). The VPFA interacts with VPP application using low-level API. The VPFA exposes *ne tconf* or *yang* based API for remote devices to program the VTF through the VPFA.

Vhost

Vhost is a solution that allows the user space process to share a number of virtqueues directly with a Kernel driver. This solution acts as a transport mechanism for the kernel to access the user space application memory while allowing a number of *ioeventfds* and *irqfds* to serve as the kick mechanism. A QEMU guest uses an emulated PCI device as the control plane, to handle the QEMU. Once a virtqueue is set up, the QEMU guest uses the Vhost API to pass direct control of a virtqueue to a Kernel driver.

In this model, a vhost_net driver directly passes the guest network traffic to a TUN device directly from the Kernel side, thereby improving the performance significantly.

The figure below shows the VTF VHOST.



In the above implementation, the guest NFV application directly writes the packets into the TX rings which are shared through a common vhost socket as the RX ring on the VPP. The VPP grabs these packets from the RX ring buffer and forwards the packets using the vector graphs it maintains.

VTS Installation

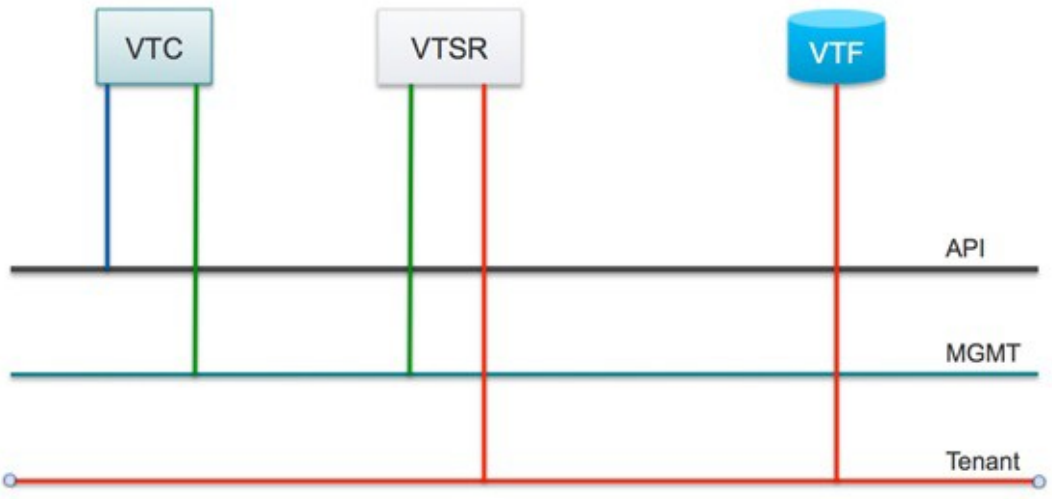
VTS Installation

If your Cisco NFVI package includes VTS, follow the Cisco VTS installation procedures which are customized for Cisco NFVI from the standard Cisco VTS 2.6.2 installation procedures located on the Cisco VTS product site. You must install Cisco VTS before you install Cisco VIM.

To install Cisco VTS with Cisco NFVI:

1. You must manually install the Cisco VTS Virtual Topology Controller (VTC) and its VTSR VMs before you start the Cisco VIM installation.
2. Run the VTC and VTSR VMs on an independent pair of servers, and not on a Cisco NFVI control, compute, storage, or management node.
3. You can set up the networking on those servers as described in the installation procedures.
4. When you run the Cisco VIM installer, you have to provide the VTC VIP and appropriate VTS credentials.

The following figure shows the connectivity of Cisco VTS VTC and VTSR VMs with the Cisco NFVI networks.



The following table shows the mapping of Cisco VTS network names with Cisco VIM network names.

Cisco VTS VM	Cisco VTS Network Name	Cisco VIM Network Name
VTC	Management Network	API (a)
VTC	Underlay Network	Management or Provision (mx)
VTSR	Management Network	Management or Provision (mx)
VTSR	Underlay Network	Tenant (t)

The following table describes the required IP address allocations for VTS components:

Cisco VIM Network	Required Cisco VTS IP Addresses	Description
API (a)	3 total (1 VIP + 1 IP per VTC VM)	Set up in the VTC config.iso and cluster.conf
Management or Provisioning (mx)	• 5 total—Three for VTC (one VTC VIP called as VTS_NCS_IP in setup_data and one IP per VTC VM) • Two for VTSR: one IP per VTSR VM.	Set up in *VTSR config.iso.* ⚠ VTS component IP addresses cannot overlap with the pool ranges configured in the Cisco VIM *setup_data.yaml* .
Tenant (t)	2 total—(one IP address VTSR VM.	Set up in *VTSR config.iso* ⚠ The VTS component IPs cannot overlap with pool ranges that are configured in the Cisco VIM setup_data.yaml.

The following is the VTS IP distribution and setup mechanism.

VIM API network:

- VTC1—api (a) network IP1 (associated through the VTC1 config ISO)
- VTC2—api (a) network IP2 (associated through the VTC2 config ISO)
- VTC VIP—api (a) network IP3 (associated through the HA step cluster.conf)

VIM Management/Provisioning network:

- VTC1—management/provisioning (mx) network IP1 (associated through the VTC1 config ISO)
- VTC2—management/provisioning (mx) network IP2 (associated through the VTC2 config ISO)
- VTC VIP—management/provisioning (mx) network IP3 (associated through the HA step cluster.conf)
- VTSR 1—management/provisioning (mx) network IP4 (associated through the VTSR-1 config ISO)
- VTSR 2—management/provisioning (mx) network IP5 (associated through the VTSR-2 config ISO)

VIM Tenant network:

- VTSR 1—tenant (t) network IP1 (associated through the VTSR-1 config ISO)
- VTSR 2—tenant (t) network IP2 (associated through the VTSR-2 config ISO)

VTC VM Installation

VTC VM Installation

To install VTS within Cisco NFVI, you must install the Virtual Topology Controller (VTC) VM using either the automatic or manual configuration option.

Installing VTC VM - Automatic Configuration Using ISO File

To install a VTC VM and enable configuration using an ISO file, create a text file with the VM settings, wrap the text file in an ISO file, and then attach the ISO file to the VM CD drive.

1. Connect to the controller node via SSH, and copy the *vtc.qcow2* file to */var/lib/libvirt/images/* folder.
2. Copy the *vtc.sample.xml* file to your controller.
3. Create a *config.txt* file containing the following parameters:

```
Hostname=vtc
ManagementIPv4Method=Static
ManagementIPv4Address= <VM's a-net IP address in a.b.c.d form>
ManagementIPv4Netmask= <a-net IP mask in a.b.c.d form>
ManagementIPv4Gateway= <a-net gateway IP address in a.b.c.d form>
UnderlayIPv4Method=Static
UnderlayIPv4Address= <VM's mx-net IP address in a.b.c.d form>
UnderlayIPv4Netmask=<mx-net IP mask in a.b.c.d form>
DNSv4=<DNS server--ie. setup_data.yaml::NETWORKING['domain_name_servers'][0]>
Domain=<domain name--ie. setup_data.yaml::NETWORKING['domain_name']>
NTP=<NTP server--ie. setup_data.yaml::NETWORKING['ntp_servers'][0]>
vts-adminPassword=<password for user 'admin'--setup_data.yaml::VTS_PARAMETERS['VTC_SSH_PASSWORD']>
AdministrativeUser=<VM ssh login user--can be setup_data.yaml::VTS_PARAMETERS['VTC_SSH_USERNAME']>
AdministrativePassword=<VM ssh login user--can be setup_data.yaml::VTS_PARAMETERS['VTC_SSH_PASSWORD']>
ManagementIPv6Method: Unused by NFVI
UnderlayIPv6Method: Ununsed by NFVI
```


- *config.txt* file must have a blank line at the end.
- Before entering the VTS_PASSWORD, review Cisco VTS Username and Password

Parameter descriptions:

- Hostname—The VM hostname.
- ManagementPv4Method—Whether to use DHCP or static addressing for the Cisco NFVI API network (a-net) interface (eth0).
- ManagementIPv4Address—The api (a) network IPv4 address of the VM (required only for static addressing).
- ManagementIPv4Netmask—The a network IPv4 net mask of the VM (required only for static addressing).
- ManagementIPv4Gateway—The a network API IPv4 gateway of the VM (required only for static addressing).
- UnderlayIPv4Method—Whether to use DHCP or static addressing for the Cisco NFVI management/provisioning (mx) network interface (eth1).
- UnderlayIPv4Address—The mx network IPv4 address of the VM (required only for static addressing).
- UnderlayIPv4Netmask—The mx network IPv4 net mask of the VM (required only for static addressing).
- DNSv4—DNS IPv4 address (required only for static addressing).
- Domain—DNS search domain (required only for static addressing).
- NTPv4—NTP IPv4 address or FQDN (required only for static addressing).
- vts-admin Password—Password for the vts-admin user. This should match the value in setup_data.yaml::VTS_PARAMETERS ['VTS_PASSWORD'] or subsequently changed through the VTC UI to match the value in setup_data.yaml::VTS_PARAMETERS ['VTS_PASSWORD']
- Administrative User—New administrative user for login using SSH.
- Administrative Password—Sudo password for the administrative user.

4. Use **mkisofs** to create an ISO file, for example:

```
mkisofs -o config.iso config.txt
```

5. Create the VTC VM using following command:

```
virsh create vtc.sample.xml
```

Installing VTC VM - Manual Configuration Using Virt-Manager

To install VTC VM, configure it manually using the virt-manager application:

1. Connect to the controller node through SSH, and copy the *vtc.qcow2* file *to /var/lib/libvirt/images/* folder.
2. Copy the Cisco NFVI *vtc.sample.xml* file to your controller. Modify it as per your setup. See Sample Configuration, for examples.
3. Create the VTC VM using the following command:

   ```
   virsh create vtc.sample.xml
   ```

4. Run the command:

   ```
   virsh list --all
   ```

   Output:

   ```
   Id     Name      State
   --------------------------------
   2      VTC      running
   ```

5. Start **virt-manager**. Run:

   ```
   virt-manager
   ```

6. After the virt-manager window opens, click the VTC VM to open up the VTC VM console.

   The console displays an installation wizard that takes you through the initial VTC VM configuration.
7. Enter the following:

   For items that take multiple values such as DNS and NTP, each value must be separated by a space.

   - VTS Hostname
   - DHCP / Static IP configuration for static IP
   - Management IP address for VTC—This is the Cisco NFVI api (a) network IP address.
   - Management IP Netmask (api network)
   - Management Gateway address (api network)
   - DNS Address—One of the DNS servers in setup_data.yaml::NETWORKING['domain_name_servers'
   - DNS Search domain—setup_data.yaml::NETWORKING['domain_name']
   - Underlay IP address—This is the IP address for Cisco NFVI management/provisioning (mx) network.
   - Underlay IP Netmask (mx network)
   - NTP address—One of the setup_data.yaml::NETWORKING['ntp_servers'] addresses
   - Password change for user vts-admin—Enter the default user vts-admin password. The vts-admin user is used for password recovery and to revisit a configuration screen for editing the information. If you log in to the VTC VM using vts-admin username and password again, you get the same dialog to go through the VTC VM setup again. The password must match the value in setup_data.yaml:: VTS_PARAMETERS['VTS_PASSWORD'] or subsequently changed through the VTC UI to match the value in setup_data.yaml:: VTS_PARAMETERS['VTS_PASSWORD']

     Before entering the VTS_PASSWORD, we recommend that you review Cisco VTS Username and Password.
   - Administrator User: Enter administrative username and password. This username and password are used to login to the VM via SSH.
   - Password for administrator user

     VTC VM reboots at this time. Wait for two minutes for the VTC VM to be up. You can ping the IP address given for VTC VM in the setup process, to verify whether the VTC VM is up.
8. SSH into VTC VM using the IP address, administrative username/password given in the setup process (not vts-admin user).

Installing VTC VM - Manual Configuration using VNC

If the server where you install VTC is in a remote location with network latency or low bandwidth, you can use VNC to access the VTC VM and manually configure it using the CTC VM graphic console. To do this:

1. Connect to the controller node via SSH, and copy the vtc.qcow2 file to /var/lib/libvirt/images/ folder.
2. Copy the *vtc.sample.xml* file to your controller. Modify it as per your setup. The sample VTC XML file output is provided in Sample Configuration.
3. Replace the following sections of the *vtc.sample.xml* file:

```
<graphics type='spice' port='5900' autoport='yes' listen='127.0.0.1'>
<listen type='address' address='127.0.0.1'/>
</graphics>
```

with the following:

```
<graphics type='vnc' port='5900' autoport='yes' listen='0.0.0.0'>
<listen type='address' address='0.0.0.0'/>
</graphics>
```


Setting the listen address to 0.0.0.0 allows external clients to connect to the VNC port (5900). You have to make sure that iptables configuration (if any) allows inbound TCP port 5900 connections.

4. Create the VTC VM using following command:

```
virsh create vtc.sample.xml
```

You should now be able to use a VNC client to connect to the VTC VM graphic console and continue the setup.

5. Enter the following:

For items that take multiple values, such as DNS and NTP, use a space to separate each value.

- VTS Hostname
- DHCP/Static IP configuration for static IP
- Management IP address for VTC—This is the Cisco NFVI api (a) network IP address.
- Management IP Netmask (api network)
- Management Gateway address (api network)
- DNS Address—One of the DNS servers in setup_data.yaml::NETWORKING['domain_name_servers'
- DNS Search domain—-- setup_data.yaml::NETWORKING['domain_name']
- Underlay IP address—This is the IP address for Cisco NFVI management/provisioning (mx) network.
- Underlay IP Netmask (mx network)
- NTP address—One of the setup_data.yaml::NETWORKING['ntp_servers'] addresses
- Password change for user vts-admin—Enter the default user vts-admin password. The vts-admin user is used for password recovery and to revisit a configuration screen if you make a mistake or need to change the information. If you log into the VTC VM using vts-admin username and password again, you get the same dialog to go through the VTC VM setup again. This should match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD'] or subsequently changed through the VTC UI to match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD']
- Administrator User—Enter administrative username and password. This username and password are used to login to the VM via SSH.
- Password for administrator user.

  When VTC VM reboots at this time, wait for two minutes for the VTC VM to come up. You can ping the IP address given for VTC VM in the setup process to verify whether the VTC VM is up.

6. SSH into VTC VM using the IP address, administrative username/password given in the setup process (not vts-admin user).

Installing VTSR VMs

Installing VTSR VMs

Before you can install Cisco VTS for Cisco NFVI, you must install the VTSR VM and register it to VTS. VTSR VM is the control plane VM. Installing and registering the VTSR VM requires you to complete the following procedures:

Creating VTSR VM

The VTSR VM is essential to the Virtual VTEP topology. As VTSR VM contains a nested VM, the VTSR must enable nesting.

Before you Begin

You must complete VTS VM installation and change the VTC UI initial password to the password that you enter for Cisco VIM when you install Cisco VIM. This password is set in setup_data.yaml or Cisco VIM Insight. Login to VTC UI and create a site with Unique UUID and EVPN VxLAN Type. Then, update the site UUID in setup_data.yaml as VTS_SITE_UUID.

Bringing up the KVM-based VTSR VM

1. Create the VTSR VM XML referring to the Cisco NFVI sample (VTSR.XML).
2. Generate an ISO file for the VTSR. See Creating ISO for IOS VTSR.
3. Create the VM using the XML.

```
virsh create VTSR.xml
```

Creating ISO for IOS VTSR

To create an ISO file for VTSR:

1. Create the *system.cfg* file based on the sample below

Verify that the configuration file has no space or extra characters.

Before you enter the VTS_USERNAME and VTS_PASSWORD, review Cisco VTS Usernames and Passwords.

```
# This is a sample VTSR configuration file
# Copyright (c) 2015 cisco Systems
# Protect the generated ISO, as it contains authentication data
# in plain text.
# The following are the common configurations for VTSR
# VTS Registration Information:
# VTS_ADDRESS should be the VTS IP. The value must be either an IP or a mask.
# VTS_ADDRESS is mandatory. If only the V4 version is specified,
# the V4 management interface for the VTSR (NODE1_MGMT_NETWORK_IP_ADDRESS)
# will be used. If the V6 version is specified, the V6 management interface
# for the VTSR (NODE1_MGMT_NETWORK_IPV6_ADDRESS) must be specified and will be used.
VTS_ADDRESS="10.85.88.152"
#VTS_IPV6_ADDRESS="a1::10"
# VTS_REGISTRATION_USERNAME used to login to VTS.
VTS_REGISTRATION_USERNAME="admin"
# VTS_REGISTRATION_PASSWORD is in plaintext.
VTS_REGISTRATION_PASSWORD="Cisco123!"
# VTSR VM Admin user/password
USERNAME="cisco"
PASSWORD="cisco123"
# Mandatory Management-VRF name for VTSR.
VTS_MANAGEMENT_VRF="vtsr-mgmt-vrf"
# VTSR VM Network Configuration for Node 1:
# NETWORK_IP_ADDRESS, NETWORK_IP_NETMASK, and NETWORK_IP_GATEWAY
# are required to complete the setup. Netmask can be in the form of
# "24" or "255.255.255.0"
```

```
# The first network interface configured with the VTC VM is used for
# underlay connectivity, while the second interface is used for the management network.
# For both MGMT and UNDERLAY networks, a <net-name>_NETWORK_IP_GATEWAY
# variable is mandatory and used for monitoring purposes.
##
V6 is only supported on the mgmt network and dual stack is
# not supported. If both are specified, V6 will take priority (and
# requires VTS_IPV6_ADDRESS to be set).
# The *V6* parameters for the mgmt network are optional. Note that if V6 is used for mgmt
# it must be V6 on both nodes. Netmask must be the prefix length for V6.
NODE1_MGMT_NETWORK_IP_ADDRESS="19.1.0.20"
NODE1_MGMT_NETWORK_IP_NETMASK="255.255.255.0"
NODE1_MGMT_NETWORK_IP_GATEWAY="19.1.0.1"
#NODE1_MGMT_NETWORK_IPV6_ADDRESS="a1::20"
#NODE1_MGMT_NETWORK_IPV6_NETMASK="64"
#NODE1_MGMT_NETWORK_IPV6_GATEWAY="a1::1"
NODE1_UNDERLAY_NETWORK_IP_ADDRESS="19.0.128.20"
NODE1_UNDERLAY_NETWORK_IP_NETMASK="255.255.255.0"
NODE1_UNDERLAY_NETWORK_IP_GATEWAY="19.0.128.1"
# AUX network is optional
#NODE1_AUX_NETWORK_IP_ADDRESS="169.254.20.100"
#NODE1_AUX_NETWORK_IP_NETMASK="255.255.255.0"
#NODE1_AUX_NETWORK_IP_GATEWAY="169.254.20.1"
# XR Hostname
NODE1_XR_HOSTNAME="vtsr01"
# Loopback IP and netmask
NODE1_LOOPBACK_IP_ADDRESS="128.0.0.10"
NODE1_LOOPBACK_IP_NETMASK="255.255.255.255"
# Operational username and password - optional
# These need to be configured to start monit on VTSR
#VTSR_OPER_USERNAME="monit-ro-oper"
# Password needs an encrypted value
# Example : "openssl passwd -1 -salt <salt-string> <password>"
#VTSR_OPER_PASSWORD="$1$cisco$b88M8bkCN2ZpXgEEc2sG9/"
# VTSR monit interval - optional - default is 30 seconds
#VTSR_MONIT_INTERVAL="30"
# VTSR VM Network Configuration for Node 2:
# If there is no HA, the following Node 2 configurations will remain commented and
# will not be used and Node 1 configurations alone will be applied.
# For HA , the following Node 2 configurations has to be uncommented
# VTSR VM Network Configuration for Node 2
# NETWORK_IP_ADDRESS, NETWORK_IP_NETMASK, and NETWORK_IP_GATEWAY
# are required to complete the setup. Netmask can be in the form of
# "24" or "255.255.255.0"
#
The first network interface configured with the VTC VM is used for
# underlay connectivity, while the second interface is used for the management network.
# For both MGMT and UNDERLAY networks, a <net-name>_NETWORK_IP_GATEWAY
# variable is mandatory and used for monitoring purposes.
##
V6 is only supported on the mgmt network and dual stack is
# not supported.If both are specified, V6 will take priority (and
# requires VTS_IPV6_ADDRESS to be set).
# The *V6* parameters for the mgmt network are optional. Note that if V6 is used for mgmt
# it must be V6 on both nodes. Netmask must be the prefix length for V6.
#NODE2_MGMT_NETWORK_IP_ADDRESS="19.1.0.21"
#NODE2_MGMT_NETWORK_IP_NETMASK="255.255.255.0"
#NODE2_MGMT_NETWORK_IP_GATEWAY="19.1.0.1"
##NODE2_MGMT_NETWORK_IPV6_ADDRESS="a1::21"
##NODE2_MGMT_NETWORK_IPV6_NETMASK="64"
##NODE2_MGMT_NETWORK_IPV6_GATEWAY="a1::1"
#NODE2_UNDERLAY_NETWORK_IP_ADDRESS="19.0.128.21"
#NODE2_UNDERLAY_NETWORK_IP_NETMASK="255.255.255.0"
#NODE2_UNDERLAY_NETWORK_IP_GATEWAY="19.0.128.1"
# AUX network is optional
# Although Aux network is optional it should be either present in both nodes
# or not present in both nodes.
# It cannot be present on Node1 and not present on Node2 and vice versa
#NODE2_AUX_NETWORK_IP_ADDRESS="179.254.20.200"
#NODE2_AUX_NETWORK_IP_NETMASK="255.255.255.0"
#NODE2_AUX_NETWORK_IP_GATEWAY="179.254.20.1"
```

```
# XR Hostname
#NODE2_XR_HOSTNAME="vtsr02"
# Loopback IP and netmask
#NODE2_LOOPBACK_IP_ADDRESS="130.0.0.1"
#NODE2_LOOPBACK_IP_NETMASK="255.255.255.255"
# VTS site uuid
VTS_SITE_UUID="abcdefab-abcd-abcd-abcd-abcdefabcdef"
```

2. Copy your VTSR *system.cfg* files to the same path where the script resides. For example:

```
admin:/opt/cisco/package/vts/bin$ ls -l
total 1432
-rwxr-xr-x 1 vts-admin vts-admin 4767 Sep 29 16:40 build_vts_config_iso.sh
-rw-r--r-- 1 root root 1242 Sep 29 23:54 system.cfg
```

3. Create the ISO file as shown below (you need to log in as root):

```
root:/opt/cisco/package/vts/bin# ./build_vts_config_iso.sh vtsr system.cfg.
Validating input.
Generating ISO File. Done!
```

4. Spawn the VTSR VM with the ISO connected to it.
5. Power on the VM.
   In case you spawn a new VTSR VM later, it comes up with VTSR Day Zero configuration and get re-registered with the VTC. Use the *sync-to* option available in the Config Sync feature to synchronize the configuration with the latest VTC configuration.

Verifying Cisco VTS Installation

Verifying Cisco VTS Installation

Verifying VTSR VM Installation

To verify VTSR VM installation:

Before you begin

Ensure that the tenant network (t) gateway and management network (mx) gateway are reachable from the VTSR server.

1. Log into the VTSR VM using the VTC VM console. If you had installed the VTC VM in an RedHat KVM based-OpenStack environment, use virt-manager or VNC console to log into the VM. See Installing VTC VM Manual Configuration using VNC
2. Ping the Cisco NFVI tenant (t) network gateway IP address. In case ping fails, verify Cisco NFVI tenant network.
3. Ping the VTC Cisco NFVI management/provisioning (mx) network IP address. In case ping fails, verify the mx network.

   You should be able to ping the gateway IP address for both Cisco NFVI mx and t networks, as VTSR registers to the VTC using the VTC mx network IP address.

Verifying VTC VM Installation

To verify VTC VM installation:

1. Log into the VTC VM just created using the VTC VM console.
   a. If you installed the VTC VM in an RedHat KVM based-OpenStack environment, - telnet 0 <*console-port*> (The console port is the Telnet port in the VTC.xml file.)
2. Ping the Cisco NFVI api network gateway. If ping fails, verify the VM networking to the Cisco NFVI api network.
3. For the VTC VM CLI, ping the Cisco NFVI management/provisioning (mx) network gateway. If ping fails, verify VM networking to the mx network.

   Underlay network gateway is the switched virtual interface (SVI) created for IOSXRv and VTF on the leaf where the controller is connected.

   After few minutes, verify whether the VTS UI is reachable by typing in the VTS api network IP in the browser.

Troubleshooting VTF Registration

If VTF registration issues arise, you can use the following commands to find the VTF registration logs on each Cisco NFVI compute node:

```
[root@devstack-71 neutron]# docker exec -it neutron_vtf_4269 bash
[root@devstack-71 /]# cd /var/log/vpfa
[root@devstack-71 vpfa]# ls
vpfa_err.log vpfa_med.log vpfa_server.log vpfa_server_frequent.log vpfa_stdout.log
vpfa_freq.log vpfa_reg.log vpfa_server_errors.log vpfa_server_slow.log
[root@devstack-71 vpfa]# tail vpfa_reg.log
2016-06-23 02:47:22,860:INFO:VTF-REG: Sent PATCH {"vtf": {"username": "admin",
"vpp-client-name": "devstack-71", "ip": "34.34.34.5", "binding-host-name": "devstack-71",
"gateway-ip": "34.34.34.1", "local-mac": "00:3a:7d:6a:13:c9"}} to
https://172.18.96.15:8888/api/running/cisco-vts/vtfs/vtf
2016-06-23 02:47:23,050:INFO:VTF-REG-ERR: Failure:400!!!
```

A successful log example is shown below:

```
[root@devstack-71 vpfa]# tail vpfa_reg.log
2016-06-23 15:27:57,338:INFO:AUTH: Successful Login - User: admin
URI:/yang-api/datastore/interfaces Host:IPv4Address(TCP, '34.34.34.5', 21345) Method:GET
2016-06-23 15:28:07,340:INFO:AUTH: Successful Login - User: admin
URI:/yang-api/datastore/interfaces Host:IPv4Address(TCP, '34.34.34.5', 21345) Method:GET
```

If a VTF registration fails, check the following:

- IP network connectivity between the compute nodes and the VTC and VTSR VMs (Cisco NFVI tenant and management/provisioning networks)
- VTS_PARAMETERS—The VTS_USERNAME must be admin.
- The VTC and VTSR must be up and the VTS configurations must be applied. The VTSR must be registered with VTC.
- VTS UI must show "vtsgroup3" in Inventory->Authorization Groups.
- VTC Admin Username is admin and Device Username is the one set for XRVR_USERNAME in the VTSR config ISO.

Configuring Cisco VTS and VTSR

Configuring Cisco VTS and VTSR Post Installation

For providing Cisco VTS configurations post installation, follow the below steps:

1. If you have changed the Cisco VTS username/password while configuring VTS HA configuration, continue with Step 3. If not, log into the Cisco VTS GUI using the default username/password admin/admin.
2. Change the Cisco VTS password using the **UI Change Password** tab.

   > ⚠ Before you enter the Cisco VTS password, see Cisco VTS Usernames and Passwords.

3. Log into the VTC VM using the following command:

```
cd /opt/vts/bin
sudo ./vts-cli.sh -applyTemplate vtsr-underlay-loopback-template
./vts-cli.sh -applyTemplate vtsr-underlay-loopback-template command is applyTemplate and template
name is vtsr-underlay-loopback-template
Enter device name: <hostname of vtsr>
Enter loopback-interface: <loopback interface name>
Enter ipaddress: <loopback interface ip>
Enter netmask: <loopback interface netmask>
```

4. Similarly, configure IGP in VTSR. Log into the VTC VM using the following command:

```
cd /opt/vts/bin
sudo ./vts-cli.sh -applyTemplate vtsr-underlay-ospf-template
./vts-cli.sh -applyTemplate vtsr-underlay-ospf-template command is applyTemplate and template name
is vtsr-underlay-ospf-template
Enter device name: <hostname of vtsr>
Enter process-name: <ospf process id >
Enter router-id: <ospf router id>
Enter area-address: <ospf area address>
Enter physical-interface: <VTSR interface connected to NFVI t-network>
Enter loopback-interface: <vtsr loopback interface>
Enter default-cost: <ospf default >
```

VTS in HA Configuration

Installing VTS in HA Configuration

Procedure

Complete the following steps to install Cisco VTS in a Layer 2 HA configuration.

1. Create two VTC VMs namely VTC1 and VTC2. When you create VMs, reserve three IP addresses for each Cisco VIM network to which the VTC VM are connected as described in VTS Overview.
2. If you changed the initial VTC password in a previous installation step, proceed to Step 4. If not, log into the VTC GUI using the default username /password admin/admin.
3. Change the VTC password using the UI Change Password tab. For information on Cisco VTS username and password, see Cisco VTS Usernames and Passwords.
4. Edit the cluster.conf file on VTC1 and VTC2 located in /opt/vts/etc/. Both VTCs must have identical information in the cluster.conf file. Parameters include:
    - vip_public—VIP address used for the Cisco VIM API (a) network.
    - vip_private—VIP address used for VTS on the Cisco VIM management/provisioning (mx) network. Cisco VIM uses VTFs, so this field must be entered. The vip_private field is the VIP for the VTS master private interface.
    - master_name—Enter the name of the primary VTC in the HA configuration.
    - master_ip—The master VTC IP address used for the Cisco NFVI API network.
    - slave_name—Enter the name of the secondary VTC in the HA configuration.
    - slave_ip—The secondary VTC IP address used for the Cisco NFVI API network.
    - external_ip—The external IP address. This comes from the Cisco VIM setup_data.yaml file after you complete the Cisco VIM installation and Cisco VIM configuration for the Cisco VTS installation. For VTS installation on Cisco VIM, see Cisco VTS Mechanism.

```
###Virtual Ip of VTC Master on the public interface. Must fill in at least 1
vip_public=
vip_public_ipv6=
###VTC1 Information. Must fill in at least 1 ip address
master_name=
master_ip=
master_ipv6=
###VTC2 Information. Must fill in at least 1 ip address
slave_name=
slave_ip=
slave_ipv6=
###In the event that a network failure occurs evenly between the two routers, the cluster needs an
outside ip to determine where the failure lies
###This can be any external ip such as your vmm ip or a dns but it is recommended to be a stable ip
within your environment
###Must fill in at least 1 ip address
external_ip=
external_ipv6=
############################
### Non-mandatory fields ###
############################
###If you intend to use a virtual topology forwarder (VTF) in your environment, please fill in the
vip for the underlay as well as the underlay gateway. Otherwise leave blank.
###Virtual Ip of VTC Master on the private interface. You can fill in ipv4 configuration, ipv6, or
both if you use both
vip_private=
private_gateway=
vip_private_ipv6=
private_gateway_ipv6=
###If you have your vtc's in different subnets, xrvr needs to be configured to route traffic and the
below section needs to be filled in
###If you have your vtc's on the same subnet, the below section has be skipped
###Name of your vrf. Example: VTS_VIP
vrf_name=
###Ip of your first Xrvr. Example: 11.1.1.5
xrvr1_mgmt_ip=
###List of neighbors for xrvr1, separated by comma. Example: 11.1.1.1,11.1.1.2
xrvr1_bgp_neighbors=
xrvr1_bgp_neighbors_ipv6=
```

```
###Ip of your second Xrvr. Example: 12.1.1.5
xrvr2_mgmt_ip=
###List of neighbors for xrvr2, separated by comma. Example: 12.1.1.1,12.1.1.2
xrvr2_bgp_neighbors=
xrvr2_bgp_neighbors_ipv6=
###Username for Xrvr
xrvr_user=
###Xrvr ASN information
remote_ASN=
local_ASN=
###Xrvr BGP information
bgp_keepalive=
bgp_hold=
###Update source for Xrvr1 (i.e. loopback)
xrvr1_update_source=
###Update source for Xrvr2 (i.e. loopback)
xrvr2_update_source=
###Router BGP Id for Xrvr1
xrvr1_router_id=
###Router BGP Id for Xrvr2
xrvr2_router_id=
###XRVR1 name
xrvr1_name=
###XRVR2 name
xrvr2_name=
###If you plan on having your VTC's on different subnets and intend to use a virtual topology forwarder
(VTF) in your environment,
### please fill out the following fields. Otherwise, leave blank
###List of neighbors for xrvr1, separated by comma. Example: 2.2.2.2,2.2.2.3
xrvr1_underlay_neighbors=
xrvr1_underlay_neighbors_ipv6=
###List of neighbors for xrvr2, separated by comma. Example: 3.3.3.2,3.3.3.3
xrvr2_underlay_neighbors=
xrvr2_underlay_neighbors_ipv6=
###Directly connected Tor information for Xrvr1
xrvr1_directly_connected_device_ip=
xrvr1_directly_connected_device_ipv6=
xrvr1_directly_connected_device_user=
xrvr1_directly_connected_device_neighbors=
xrvr1_directly_connected_device_neighbors_ipv6=
xrvr1_directly_connected_ospf=
xrvr1_directly_connected_router_id=
xrvr1_directly_connected_update_source=
###Directly connected Tor information for Xrvr2
xrvr2_directly_connected_device_ip=
xrvr2_directly_connected_device_user=
xrvr2_directly_connected_device_neighbors=
xrvr2_directly_connected_device_neighbors_ipv6=
xrvr2_directly_connected_ospf=
xrvr2_directly_connected_router_id=
xrvr2_directly_connected_update_source=
###VPC Peer information if any. Otherwise leave blank
xrvr1_vpc_peer_ip=
xrvr1_vpc_peer_user=
xrvr1_vpc_peer_ospf=
xrvr1_vpc_peer_router_id=
xrvr1_vpc_peer_update_source=
xrvr2_vpc_peer_ip=
xrvr2_vpc_peer_user=
xrvr2_vpc_peer_ospf=
xrvr2_vpc_peer_router_id=
xrvr2_vpc_peer_update_source=
###VTC Underlay Addresses
vtc1_underlay=
vtc2_underlay=
vtc1_underlay_ipv6=
vtc2_underlay_ipv6=
##Gateway of secondary L3 underlay
vtc2_private_gateway=
vtc2_private_gateway_ipv6=
```

5. Execute the cluster installer script, cluster_install.sh, located in */opt/vts/bin/* on VTC1 and VTC2. Do not run the script until you have completed Steps 1-5.

```
admin@vtc1:/opt/vts/bin$ sudo ./cluster_install.sh
[sudo] password for admin:
Change made to ncs.conf file.
Need to restart ncs
Created symlink from /etc/systemd/system/multi-user.target.wants/pacemaker.service to
/lib/systemd/system/pacemaker.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/corosync.service to
/lib/systemd/system/corosync.service.
Cisco Virtualized Infrastructure Manager Installation Guide, 3.0.0
127
Installing Cisco VTS
Installing VTS in an HA Configuration
Please run cluster_install.sh on vtc2.waits until finished Both nodes are online.
Configuring master Configuring Pacemaker resources
Master node configuration finished
HA cluster is installed
```


For HA to run, the *cluster_install.sh* script updates */etc/hosts* with the VTC information. If run on the node specified as a master, it completes the basic cluster setup, then wait for the slave to complete. Once the slave is finished, the master completes the remainder of the setup. When the cluster_install script is finished on the master, you can see both the public and private VIP using *ip addr*. If you use VTFs, now that the VIP is up, both VTSRs completes their auto-registration.

6. Verify the HA status.

```
admin@vtc1:/opt/cisco/package/vtc/bin$ sudo crm status
Last updated: Wed May 4 00:00:28 2016
Last change: Wed May 4 00:00:10 2016 via crm_attribute on vtc2
Stack: corosync
Current DC: vtc2 (739533872) - partition with quorum
Version: 1.1.10-42f2063
2 Nodes configured
4 Resources configured
Online: [ vtc1 vtc2 ]
ClusterIP (ocf::heartbeat:IPaddr2): Started vtc1
Master/Slave Set: ms_vtc_ha [vtc_ha]
Masters: [ vtc1 ]
Slaves: [ vtc2 ]
ClusterIP2 (ocf::heartbeat:IPaddr2): Started vtc1
admin@vtc1:/opt/cisco/package/vtc/bin$ sudo ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 52:54:00:00:bd:0f brd ff:ff:ff:ff:ff:ff
inet 11.1.1.4/24 brd 11.1.1.255 scope global eth0
valid_lft forever preferred_lft forever
inet 11.1.1.2/32 brd 11.1.1.2 scope global eth0
valid_lft forever preferred_lft forever
inet6 2001:420:10e:2010:5054:ff:fe00:bd0f/64 scope global dynamic
valid_lft 2591955sec preferred_lft 604755sec
inet6 fe80::5054:ff:fe00:bd0f/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 52:54:00:4c:11:13 brd ff:ff:ff:ff:ff:ff
inet 15.15.15.4/24 brd 11.1.1.255 scope global eth1
valid_lft forever preferred_lft forever
inet 15.15.15.20/32 brd 11.1.1.20 scope global eth1
```

Completing VTSR HA Configuration

Follow the below steps to set up the VTSR HA configuration:

> **Before you begin**
>
> You must complete VTS VM installation and change the VTC UI initial password to the password that you enter for Cisco VIM, when you install Cisco VIM. This password is set in *setup_data.yaml* or the Cisco VIM Insight.

1. Login to VTC UI and create a site with Unique UUID and EVPN VxLAN Type. Update this UUID as VTS_SITE_UUID in *setup_data.yaml*.
2. Ensure the tenant network (t) gateway and management network (mx) gateway are reachable from the VTSR server.
3. Power ON the 2 VTSR VMs as per the VTSR installation step. The VTSR VM comes up in active/active HA mode.

Uninstalling VTC HA

To move VTC back to its original pre-HA state, run the following script on both the active and standby nodes.

```
sudo /opt/vts/bin/cluster_uninstall.sh
```

Sample Configuration

Sample Cisco VTS Configuration

Sample VTC VM libvert Domain Configuration

```
<domain type='kvm' id='1332'>
<name>VTC-release2.1</name>
<uuid>5789b2bb-df35-4154-a1d3-e38cefc856a3</uuid>
<memory unit='KiB'>32389120</memory>
<currentMemory unit='KiB'>32388608</currentMemory>
<vcpu placement='static'>8</vcpu>
<resource>
<partition>/machine</partition>
</resource>
<os>
<type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
<boot dev='hd'/>
</os>
<features>
<acpi/>
<apic/>
<pae/>
</features>
<cpu mode='custom' match='exact'>
<model fallback='allow'>Westmere</model>
<feature policy='require' name='vmx'/>
</cpu>
<clock offset='utc'/>
<on_poweroff>destroy</on_poweroff>
<on_reboot>restart</on_reboot>
<on_crash>restart</on_crash>
<devices>
<emulator>/usr/libexec/qemu-kvm</emulator>
<disk type='file' device='disk'>
<driver name='qemu' type='qcow2' cache='none'/>
<source file='/home/cisco/VTS2.1/vtc.qcow2'/>
<target dev='vda' bus='virtio'/>
<alias name='virtio-disk0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0'/>
</disk>
<controller type='usb' index='0'>
<alias name='usb0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
</controller>
<controller type='pci' index='0' model='pci-root'>
<alias name='pci.0'/>
</controller>
<controller type='virtio-serial' index='0'>
<alias name='virtio-serial0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
</controller>
<interface type='bridge'>
<mac address='52:54:00:5b:12:3a'/>
<source bridge='br-ex'/>
<virtualport type='openvswitch'>
<parameters interfaceid='263c1aa6-8f7d-46f0-b0a3-bdbdad40fe41'/>
</virtualport>
<target dev='vnet0'/>
<model type='virtio'/>
<alias name='net0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
</interface>
```

```
<interface type='bridge'>
<mac address='52:54:00:8d:75:75'/>
<source bridge='br-control'/>
<virtualport type='openvswitch'>
<parameters interfaceid='d0b0020d-7898-419e-93c8-15dd7a08eebd'/>
</virtualport>
<target dev='vnet1'/>
<model type='virtio'/>
<alias name='net1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x0b' function='0x0'/>
</interface>
<serial type='tcp'>
<source mode='bind' host='127.0.0.1' service='4888'/>
<protocol type='telnet'/>
<target port='0'/>
<alias name='serial0'/>
</serial>
<console type='tcp'>
<source mode='bind' host='127.0.0.1' service='4888'/>
<protocol type='telnet'/>
<target type='serial' port='0'/>
<alias name='serial0'/>
</console>
<channel type='spicevmc'>
<target type='virtio' name='com.redhat.spice.0'/>
<alias name='channel0'/>
<address type='virtio-serial' controller='0' bus='0' port='1'/>
</channel>
<input type='mouse' bus='ps2'/>
<graphics type='spice' port='5900' autoport='yes' listen='127.0.0.1'>
<listen type='address' address='127.0.0.1'/>
</graphics>
<sound model='ich6'>
<alias name='sound0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</sound>
<video>
<model type='qxl' ram='65536' vram='65536' heads='1'/>
<alias name='video0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0'/>
</video>
<memballoon model='virtio'>
<alias name='balloon0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
</memballoon>
</devices>
<seclabel type='dynamic' model='selinux' relabel='yes'>
<label>system_u:system_r:svirt_t:s0:c26,c784</label>
<imagelabel>system_u:object_r:svirt_image_t:s0:c26,c784</imagelabel>
</seclabel>
</domain>
```

Sample VTSR VM libvirt Domain Configuration

```
<domain type='kvm' id='20'>
<name>SAMPLE-VTSR-1</name>
<memory unit='GiB'>48</memory>
<cpu mode='host-passthrough'/>
<vcpu placement='static'>14</vcpu>
<resource>
<partition>/machine</partition>
</resource>
<os>
<type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
<boot dev='hd'/>
<boot dev='cdrom'/>
</os>
```

```
<features>
<acpi/>
<apic/>
<pae/>
</features>
<clock offset='localtime'/>
<on_poweroff>destroy</on_poweroff>
<on_reboot>restart</on_reboot>
<on_crash>restart</on_crash>
<devices>
<emulator>/usr/libexec/qemu-kvm</emulator>
<disk type='file' device='cdrom'>
<driver name='qemu'/>
<source file='/home/admin/VTS20/images/vtsr_node1_cfg.iso'/>
<target dev='hda' bus='ide'/>
<readonly/>
</disk>
<disk type='file' device='disk'>
<driver name='qemu' type='qcow2'/>
<source file='/home/admin/VTS20/images/vtsr.qcow2'/>
<target dev='vda' bus='virtio'/>
<alias name='virtio-disk0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x09' function='0x0'/>
</disk>
<controller type='usb' index='0'>
<alias name='usb0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
</controller>
<controller type='ide' index='0'>
<alias name='ide0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
</controller>
<controller type='pci' index='0' model='pci-root'>
<alias name='pci.0'/>
</controller>
<interface type='bridge'>
<source bridge='br-ex'/>
<virtualport type='openvswitch'>
<parameters interfaceid='4ffa64df-0d57-4d63-b85c-78b17fcac60a'/>
</virtualport>
<target dev='vtsr-dummy-mgmt'/>
<model type='virtio'/>
<alias name='vnet1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0'/>
</interface>
<interface type='bridge'>
<source bridge='br-inst'/>
<virtualport type='openvswitch'>
<parameters interfaceid='4ffa64df-0d67-4d63-b85c-68b17fcac60a'/>
</virtualport>
<target dev='vtsr-dummy-2'/>
<model type='virtio'/>
<alias name='vnet1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
</interface>
<interface type='bridge'>
<source bridge='br-inst'/>
<virtualport type='openvswitch'>
<parameters interfaceid='4ffa64df-0f47-4d63-b85c-68b17fcac70a'/>
</virtualport>
<target dev='vtsr-dummy-3'/>
<model type='virtio'/>
<alias name='vnet1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</interface>
<interface type='bridge'>
<source bridge='br-inst'/>
<virtualport type='openvswitch'>
<parameters interfaceid='4ffa64df-0d47-4d63-b85c-58b17fcac60a'/>
</virtualport>
<vlan>
```

```
<tag id='800'/>
</vlan>
<target dev='vtsr-gig-0'/>
<model type='virtio'/>
<alias name='vnet1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
</interface>
<interface type='bridge'>
<source bridge='br-ex'/>
<virtualport type='openvswitch'>
<parameters interfaceid='3ffa64df-0d47-4d63-b85c-58b17fcac60a'/>
</virtualport>
<target dev='vtsr-gig-1'/>
<model type='virtio'/>
<alias name='vnet1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0'/>
</interface>
<interface type='bridge'>
<source bridge='br-inst'/>
<virtualport type='openvswitch'>
<parameters interfaceid='a2f3e85a-4de3-4ca9-b3df-3277136c4054'/>
</virtualport>
<vlan>
<tag id='800'/>
</vlan>
<target dev='vtsr-gig-2'/>
<model type='virtio'/>
<alias name='vnet3'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
</interface>
<serial type='pty'>
<source path='/dev/pts/0'/>
<target port='0'/>
<alias name='serial0'/>
</serial>
<console type='pty' tty='/dev/pts/0'>
<source path='/dev/pts/0'/>
<target type='serial' port='0'/>
<alias name='serial0'/>
</console>
<input type='tablet' bus='usb'>
<alias name='input0'/>
</input>
<input type='mouse' bus='ps2'/>
<graphics type='vnc' port='5900' autoport='yes' listen='0.0.0.0' keymap='en-us'>
<listen type='address' address='0.0.0.0'/>
</graphics>
<video>
<model type='cirrus' vram='9216' heads='1'/>
<alias name='video0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
</video>
<memballoon model='virtio'>
<alias name='balloon0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x0a' function='0x0'/>
</memballoon>
</devices>
</domain>
```

Cisco VIM

Cisco VIM

Installation Sequence

Installation Sequence

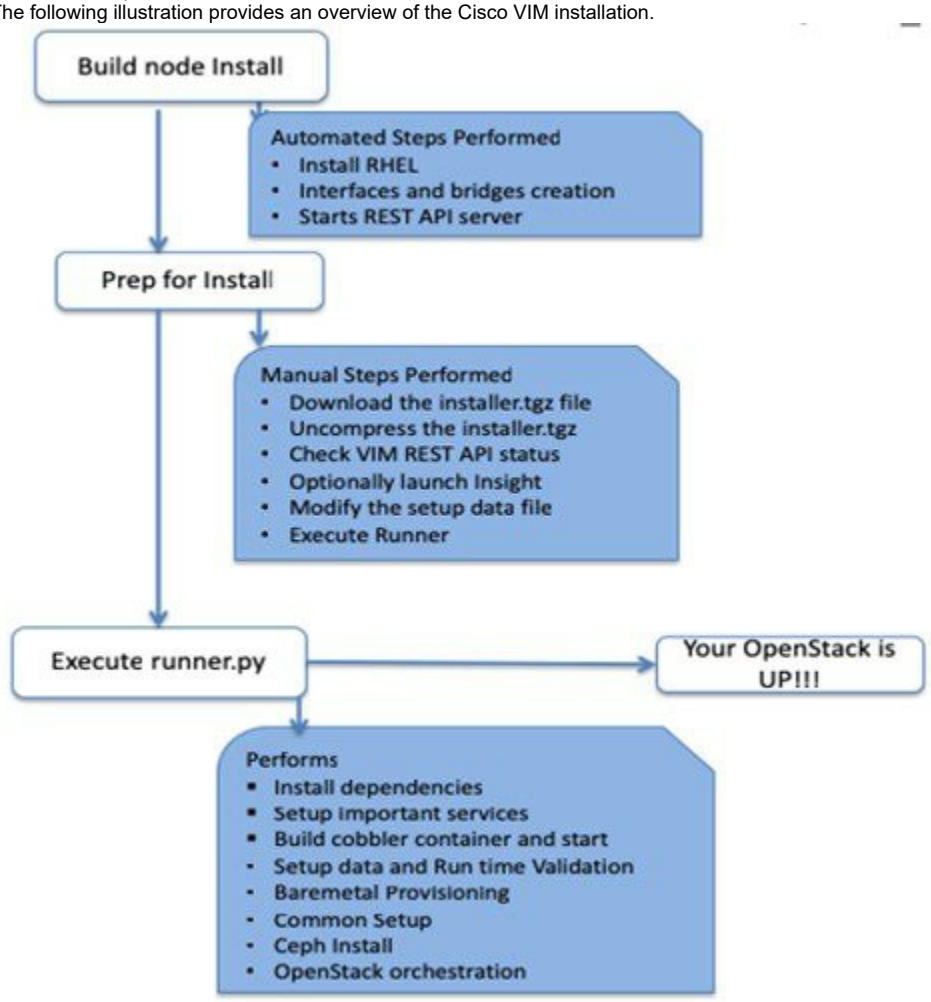
Before you install Cisco VIM, complete the procedures in Preparing for Cisco NFVI Installation and ensure that Cisco NFVI network infrastructure is set up. If your management node does not have internet access, complete the procedure in Installation Preparation Without Internet Access. You can download and install the Cisco VIM installation files from the Internet, Cisco VIM software Hub, or the USB drive prepared for installation.

The bootstrap script is then kicked off to download the installer repository for installing Docker and its dependencies and starting the installer web service.

Ciso VIM installation is a multi-step process, with tests embedded in each step, to allow fixing user or environment errors and continue from the failure point of the installation. To start off, the Cisco VIM installer validates the intent file *(setup_data.yaml)* from a syntax and semantic point of view. It also validates the correctness of the management node orchestration and the hardware BOM (bill of materials) along with its BIOS settings. The orchestrator then sets up the docker registry on the management node along with other essential services, for example, cobbler, EFK in respective containers in the management node. It then creates new vNICs (for Cisco VIC) or sub-interfaces (for Intel NIC) on the controller, compute, and dedicated storage nodes based on the configuration provided in the *setup_data.yaml* file. This is followed by the Pxeboot Execution Environment (PXE) boot of RHEL onto the target nodes (control, compute and storage) through the Cobbler server set up on the management node. Post PXE boot, the orchestrator carries out layer 2 and 3 ping checks to test out connectivity with target frame sizes.
After the installation, the Cisco VIM installer performs common steps across all the Cisco NFVI nodes.

Next, the Ceph related packages required for managing the cluster and creating Object Storage Daemon (OSD) and monitor nodes are installed on the control and storage nodes. Three Ceph monitor nodes are installed at the host level on the control nodes. These serve as management nodes and have the administration keyring. Ceph configurations such as ceph.conf and Ceph client keyrings files are stored under */etc/ceph* on each controller. Each Ceph storage node associates an OSD to a physical hard drive with a write journal on a separate SSD, to support small block random I/O.

Next Openstack services are installed on the target servers, along with the target mechanism driver. An integrated cloud sanity is then executed to make sure that the cloud is up and running. Based on the setup_data input, an optional control and data plane check with VMs is then run, to validate the end-to-end connectivity of the cloud from a cloud user point of view.
The following illustration provides an overview of the Cisco VIM installation.



If you have Cisco Unified Management (UM), complete only part of the Cisco VIM installation procedure and proceed to the Installing UM with Internet Access procedure to complete the configuration and setup of Cisco VIM. If you do not have Cisco VIM UM, configure Cisco VIM by editing the *setup_data.yaml* file as described in the Cisco VIM installation.

Deployment of Management Node

Deployment of Management Node

This procedure allows you to install Cisco VIM on a Cisco NFVI management node:

Before you begin

- You must get Cisco NFVI installation file download site credentials from your Cisco account representative.
  For management nodes with no Internet access, you need a USB drive containing the Cisco NFVI installation files. To prepare the USB drive, see Installation Preparation Without Internet Access.
- The private networks 192.168.1.0/24 and 192.168.2.0/24 are internally reserved for testing the cloud from a control and data plane point of view. We recommend that you do not use these reserved networks while preparing network layouts.
- You need to provide a valid certificate signed by a trusted certificate authority for Cisco VIM deployment. It needs to be a server certificate with a common name matching the IP address and DNS name specified in the setup data file under *external_lb_vip_address* and *external_lb_vip_fqdn.* To ensure security, use only the valid certificate signed by a trusted certificate authority in a production environment. For details on generating a self-signed certificate, see OpenStack Configuration.

1. If your management node does not have Internet access, use the prepared USB drive and complete the following steps:
   a. Insert the USB drive into the management node.
   b. Run the *import_artifacts.sh* script to copy all artifacts onto the management node, for example:

   ```
   cd ~/installer-<tag_id>/tools
    ./import_artifacts.sh
   ```

   All the installation artifacts are copied *to* /var/cisco/artifacts/ on the management node.
2. If you are installing Cisco VIM Insight, navigate to Unified Management and complete the Cisco VIM Insight installation. If you are not installing Cisco VIM Insight, complete the following steps, irrespective of the fact that it is an air-gapped or connected installation.
3. Change to the installer directory by running the following command:

   ```
   cd ~/installer-<tag_id>
   ```

4. Create a directory (for example, ~/Save/) to store a copy of the *setup_data.yaml* file that configures the Cisco NFVI for your particular implementation.
5. Change to openstack-configs directory and copy the example Cisco VIM *setup_data.yaml* file into the directory that you just created:

   ```
   cd openstack-configs/
   cp setup_data.yaml.<C_or_B>_Series_EXAMPLE setup_data.yaml
   ~/Save/setup_data.yaml
   ```

   Based on your requirements, you must change the CPU and MEM allocation ratio for the target pod. Update the following parameters located in */root/installer-<xxx>/openstack-configs/openstack_config.yaml* to your target value:

   NOVA_RAM_ALLOCATION_RATIO: 1.5 # range of 1.0 to 4.0

   NOVA_CPU_ALLOCATION_RATIO: 16.0 # range of 1.0 to 16.0

   In case this setting is not done on Day 0, see Memory/CPU Usage on how to set these variables.
6. With a yaml editor, modify the copied example *setup_data.yaml* file as the data setup file for your implementation. This includes both Cisco NFVI data and OpenStack parameters.
7. If you intend to run the cloud over TLS, see OpenStack Configuration for TLS certificate generation.
8. Run the installation:

   ```
   ciscovim --setupfile ~/Save/setup_data.yaml run
   ```

   After the installation is complete, you can view the installation logs at */var/log/mercury/<UUID>.*

Cisco VIM Client Details

Cisco VIM Client Details

Cisco VIM combines the CLI and API so that you can use the CLI or API installer transparently.

> ⚠ For a complete list of Cisco VIM REST API commands, see Cisco VIM REST API

Before you use Cisco VIM CLI, check that the installer API server is up and pointing to the right installer directory. You can execute the following command to validate the state of the API server and the installer directory that is used :

```
# cd installer-<tagid>/tools
#./restapi.py -a status
Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h ago
REST API launch directory: /root/installer-<tagid>/
```

Verify whether the server status is active and the restapi launch directory is the same as the directory from where the installation is launched. If the installer directory or the REST API state is not correct, go to the target installer directory and execute the following commands:

```
# cd new-installer-<tagid>/tools
#./restapi.py -a setup

Check if the REST API server is running from the correct target directory
#./restapi.py -a status


Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h ago
REST API launch directory: /root/new-installer-<tagid>/
```

The REST API tool provides the options to restart, tear down, and reset password for the REST API server as listed:

```
# ./restapi.py --h
usage:
restapi.py [-h] --action ACTION [--yes] [--verbose]

REST API setup helper optional arguments:

-h, --help           show this help message and exit
--action ACTION, -a  ACTION
                setup - Install and Start the REST API server.
                teardown -Stop and uninstall the REST API server.
                restart - Restart the REST API server.
                regenerate-password - Regenerate the password for REST API server.
                reconfigure-tls - Reconfigure SSL certificates and key.
                upgrade - Upgrade to new workspace.
                reset-password - Reset the REST API password with user given password.
                status - Check the status of the REST API server.

--yes, -y Skip the dialog. Yes to the action.
--verbose, -v  Perform the action in verbose mode.
```

If the REST API server is not running, executing *ciscovim* shows the following error message:

```
ciscovim -setupfile ~/Save/<setup_data.yaml> run
```

If the installer directory or the REST API state is not correct, or is pointing to an incorrect REST API launch directory, go to the *installer-<tagid>/tools* directory and execute the following commands:

```
./restapi.py --action setup
```

To confirm that the Rest API server state and launch directory is correct, execute the following command:

```
./restapi.py --action status
```

If you run the REST API recovery step on an existing pod, run the following command to ensure that the REST API server continues to manage the existing pod:

```
ciscovim --setup_file <setup_data_file_path> --perform 7 -y
```

From the CLI, enter the following command:

```
ciscovim --help

usage: ciscovim [--setupfile <setupdata_file>] <subcommand> ...

Command-line interface to the Cisco Virtualized manager

Positional arguments:
<subcommand>

run                           Perform/terminate an install operation
install-status               Status of installation of the Openstack cloud
list-steps                          List steps
add-computes                  Add compute-nodes to the Openstack cloud
add-storage                   Add a storage-node to the Openstack cloud
list-nodes                    List the nodes in the Openstack cloud
remove-computes              Remove compute-nodes from the Openstack cloud
remove-storage              Remove a storage-node from the Openstack cloud
replace-controller           Replace a controller in the Openstack cloud
list-openstack-configs  List of Openstack configs that can be changed using reconfigure
list-password-keys      List of password keys that can be changed using reconfigure
reconfigure             Reconfigure the Openstack cloud
cluster-recovery        Recover the Openstack cluster after a network partition or power outage
mgmtnode-health         Show health of the Management node
commit                  Commit an update
rollback                Rollback an update
update                  Update the Openstack cloud
update-status           Status of the update operation
upgrade                 Upgrade the Openstack cloud
check-fernet-keys       Check whether the fernet keys are successfully synchronized across keystone nodes
NFVbench                Launch NFVbench Flows
nfvimon                 NFVI Monitoring / Zenoss management operations
resync-fernet-keys      Resynchronize the fernet keys across all the keystone nodes
rotate-fernet-keys      Trigger rotation of the fernet keys on keystone
client-version          Show Virtualized Infrastructure Manager Version
version                 Show Virtualized Infrastructure Manager Version
help                    Display help about this program or one of its

Optional arguments:

--setupfile <setupdata_file>

See "ciscovim help COMMAND" for help on a specific command.
To look at the help for a sub-command (e.g. run) execute the following:

# ciscovim help run

usage:
ciscovim run [--join] [--perform <perform>] [--skip <skip>] [-y] Perform a install operation

Optional arguments:
--join                                Join the installation process
--perform <perform> Perform the following steps.
--skip <skip> Skip the following steps.
-y, --yes Yes option to skip steps without prompt
[root@MercRegTB1 installer]#
You can also run the installer in multiple smaller steps. To understand the steps involved during installation
```

```
execute the following command:
# ciscovim list-steps
Virtualized Infrastructure Manager:
===================================
+-------------------------+--------------+
| Operations                | Operation ID |
+-------------------------+--------------+
| INPUT_VALIDATION                |      1                  |
| MGMTNODE_ORCHESTRATION  |      2       |
| VALIDATION              |      3       |
| BAREMETAL               |      4       |
| COMMONSETUP             |      5                  |
| CEPH                    |      6       |
| ORCHESTRATION           |      7       |
| VMTP                    |      8       |
+-------------------------+--------------+
```

To execute the installer in steps, include specific steps from above. For example:

```
$ ciscovim run --perform 1,3 -y
```

Similarly, you can execute the installation using the skip option, where you explicitly indicate which options to skip. For example:

```
$ ciscovim run --skip 1,3 -y
```


When using the step-by-step installation, keep a track of the steps that are already completed to avoid the occurrence of unpredictable results. *ci scovim install-status* also indicates the current state of the installation process.

While the installation time varies from pod to pod, typical installation time through the Internet for a UCS C-series with three controllers, nine computes, and three storage components is listed in the following table.

Operation ID	Operation	Estimated Time
1	Input validation	6 minutes
2	Management node orchestration	40 minutes
3	Run time Validation	30 seconds
4	Bare metal	60 minutes
5	Host setup	10 minutes
6	Ceph	5 minutes
7	Orchestration	25 minutes
8	VMTP (external and provider networks)	14 minutes

Pod Reinstallation

Pod Reinstallation

You might need to reinstall the pod with the same image version. To alleviate the need for reimaging the management node followed by re-install, you can re-install the pod on assuming that the management node is compatible with the same tag.

> ⚠ For reinstallation, ensure that you use the servers in which the original installation is done. If you are using a different set of servers for reinstallation, power-off the servers in which the previous installation is done, to prevent floating of duplicate IPs in the network.

Listed below are the steps to reinstall the pod without reimaging the management node:

1. Copy the *setup_data.yaml* from */root/openstack-configs/* directory to *~/Save/*

```
cd ~/installer-<x.x.x>
 ./unbootstrap.sh -k
```

> ⚠
> - If you use Auto-TOR with ACI API, execute *./unbootstrap.sh -sk*.
> - If you use NCS-55xx as a ToR, then you must execute *./unbootstrap.sh -k* before any reimage or reinstallation of the pod to a new tag.

2. To verify that no docker containers are running, use the command:

```
docker ps -a docker ps -a
```

3. To verify that no docker images are present, use the command:

```
docker images
```

4. To setup RestAPI, use the command:

```
cd ~/installer-<xxx>/tools
./restapi -a setup
```

5. To regenerate the TLS certificate, when needed or TLS is enabled, use the command:

```
cd ~/installer-<xxx>
tools/tls_cert_gen.sh -f ~/Save/setup_data.yaml
```

6. To re-run Cisco VIM installation, use the command:

```
ciscovim run --setupfile ~/Save/setup_data.yaml
```

Control and Data Plane Testing

Control and Data Plane Testing

Cisco VIM offers an optional integrated test to validate the control and data plane sanity of the cloud from an end-user point of view. Virtual Machine Through Put (VMTP) is an optional test available to check the Layer 2 and Layer 3 data plane traffic between Cisco NFVI compute nodes. VMTP performs ping connectivity, round trip time measurement (latency), and TCP throughput measurement for the following Cisco NFVI east to west VM-to-VM flows:

- Same network (private fixed IP, flow number 1).
- Different network using fixed IP (same as intra-tenant L3 fixed IP, flow number 2).
- Different network using floating IP and NAT (same as floating IP inter-tenant L3, flow number 3.)

To enable VMTP for basic Cisco VIM installation, update the setup_data with the following commands:

```
VMTP_VALIDATION:
 EXT_NET:# Option applicable for V4 with external network with floating IP, min of 5 cont. IP; and a min of 3
VLANS need to be defined in TENANT_VLAN_RANGES
   NET_NAME: <name of external network>
   NET_SUBNET: <external cidr>
   NET_IP_START: <floating ip start>
   NET_IP_END: <floating ip end>
   NET_GATEWAY: <external net gateway>
   DNS_SERVER: <dns server for external net>

 PROV_NET:# Either for V4 or V6 for provider network
   NET_NAME: <provider network name>
   NET_SUBNET: <provider net cidr>
   NET_IP_START: <starting IP for provider net>
   NET_IP_END: <end IP for provider net>
   NET_GATEWAY: <provider net gateway>
   DNS_SERVER: <dns server for provider net>
   SEGMENTATION_ID: <segmentation id for provider net> # Needs to match a vlan defined under
PROVIDER_VLAN_RANGES
   IPV6_MODE: <"slaac" or "dhcpv6-stateless" or "dhcpv6-stateful"> # only for IPv6;
   VNIC_TYPE: <"direct" or normal># use value of direct for SRIOV, default is over virtio (value of normal)
   PHYSNET_NAME: <physnet_name># needed for SRIOV, entry has to be of the name: phys_sriov0, or phys_sriov1,
... phys_sriovn, where n is total num of SRIOV port-1
```


A minimum of four continuous IP is needed for VMTP (ideally have 8 IPs). For IPv6, it is recommended to iterate over the last group to get the start and end IP addresses.

For provider network, IPv4 or IPv6 is supported, but not both at the same time. Ensure that you do not enable external network for IPv6.

Updating Cisco VIM Software

Updating Cisco VIM Software

The Cisco VIM installer provides a mechanism to update all OpenStack services and some infrastructure services such as RabbitMQ, MariaDB, HAProxy, and VMTP.

⚠ Updating host-level packages and management node ELK and Cobbler containers are not supported

As Cisco NFVI software update runs serially, component-by-component, one node at a time, the service impact is minimal. If errors occur during an update, an automatic rollback brings the cloud back to its previous state. After an update is completed, check for any functional cloud impacts. If everything is fine, you can commit the update which clears the old containers from the system. Cisco recommends that you commit the update before you perform any other pod management functions. Skipping the commit option might lead to double faults. If you see any functional impact on the cloud, perform a manual rollback to start the old containers again.

⚠

- Cisco NFVI software updates are not supported for registry related containers and authorized_keys.
- When the management node repo containers are updated, they cannot be rolled back to the older versions as this requires node packages to be deleted, which might destabilize the cloud.
- Update of Cisco NFVI software is done within the same major version, that is, from 3.2.0 to 3.2.1, and not from 2.4 to 3.0.

To prevent double faults, a cloud sanity check is done both before and after the update.
To complete the software update, perform the steps listed in Deployment of Management Node. If your management node does not have Internet, fetch the target software bits by completing the steps listed in Installation Preparation Without Internet Access first, then follow the Cisco VIM installation instructions. Differences between a software update and regular Cisco VIM installation:

- You do not need to modify setup_data.yaml like you did during the first installation. In most cases, no modifications are needed.
- You do not need to repeat the Cisco VIM Insight installation.
- Minor differences between NFVI software installation and updates are listed in the installation procedure.

⚠

- After you complete a software update and before you perform any pod management operation, you must execute ciscovim commit.
- During the software update, the following operations are locked: add/remove compute/storage node, replace controllers, reconfigure, power off/on, and rotate fernet key.
- Before you commit, you can roll back the update to return the node to its previous software version.

Unified Management

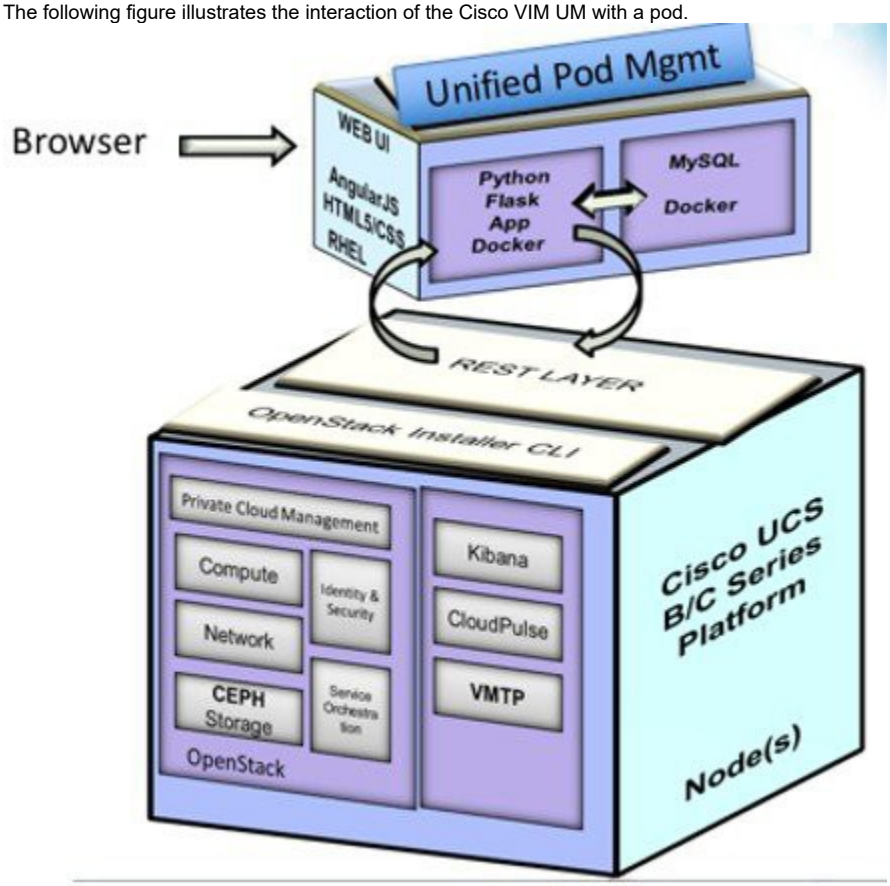
Installing Cisco VIM Unified Management

UM Overview

UM Overview

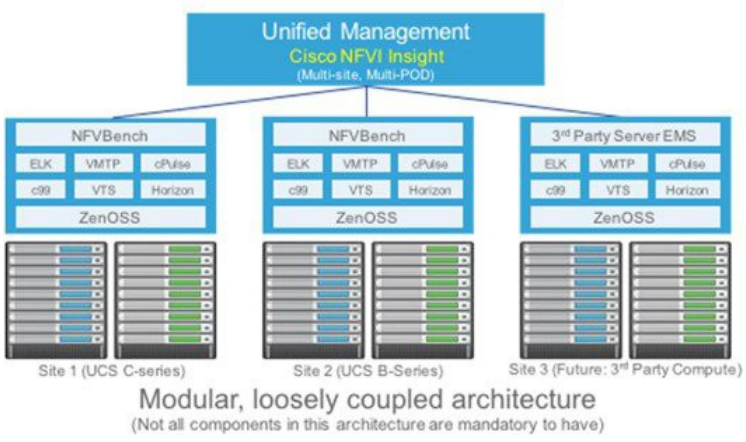
Unified Management (UM) also known as Cisco VIM Insight is a light-weight UI introduced to ease the deployment and management of the NFVI platform. This feature is available as an add-on from both commercial and feature point of view. Cisco VIM Insight offers a single pane of glass service to provide deployment visualization and to manage multiple Cisco VIM pods, thereby reducing user-errors.

The following figure illustrates the interaction of the Cisco VIM UM with a pod.



The architecture of the Cisco VIM UM is light-weight, hierarchical and scalable. It simplifies the management from the global UI. Each local site is autonomous with localized toolsets. The global UM UI provides ease of management with multi-site multi-pod capability for distributed NFV deployment at scale. Cisco VIM UM is designed to operate in HA as an option.

UM is integrated with Cisco VIM REST layer, to support multi-tenancy with local RBAC support. The container-based UI platform is loosely coupled, and can help manage multiple Cisco VIM pods right from day-0 or later in the lifecycle of the cloud as shown in the following figure.



You can install UM on a standalone (BOM same as the management node) dedicated node to manage one or more Cisco VIM pods. As the UI interacts with the REST API, it is not necessary that the pod must be managed by UM node from Day 0. The UI interacts with each pod through REST API and Role Based Access Control (RBAC) information stored in the DB.

The UI has two types of views:

- UI Admin: UI Admin can add users as UI admin or pod admin.
- Pod Admin: Pod admin has the privilege only at the pod level, unless Pod admin is also a UI admin.

Admin UI

Admin UI is responsible for managing the UI and Pod admin, which includes adding and revoking user privileges. The UI admin can delete an existing pod from the management pane.

Pod UI

The pod UI is responsible for managing each pod. UM provides easy access to switch between multiple pods. Through pod UI, a pod admin can manage users and their respective roles and responsibilities.

You can execute Day 0 (installation) and Day n activities such as pod management, software update, and so on seamlessly, where n is an integer greater than 1. ELK, Horizon web UI, and so on, are also cross-launched and visible for each pod through the pod UI.

UM with Internet Access

Installing UM with Internet Access

Overview

Complete the following steps to install Cisco VIM Insight on the Cisco NFVI management node. As security is paramount to pod management, the web-service hosting the single pane of glass is protected through TLS. Following are the steps to get the TLS certificate setup going.
You can select one of the following approaches for the TLS certificate configurations:

- Provide your own certificate: You can bring in your certificate on the management node and provide the absolute path of .pem and CA certificate files in the *insight_setup_data.yaml* file. The path must be provided as a value for the key PEM_PATH in the *insight_setup_data.yaml* file.
- Generate a new certificate on the node. You can create a new certificate on the node by running the following command:

```
# cd /root/Insight-<tag_id>/insight/ #./tls_insight_cert_gen.py -f <path_to_insight_setup_data.yaml>
/insight_setup_data.yaml.
```

This script searches for the 'PEM_PATH' inside the *insight_setup_data.yaml*. As the path is not provided, it creates a new certificate inside *install-dir/openstack-configs*.

The self-signed certificate generation utility script is provided for lab/testing deployment only. Ensure that you do not use self-signed certificate generated by this utility for the production deployment.

Installation

Before you begin

Complete all the preparation tasks that are described in Preparing for Cisco NFVI Installation. The procedure to bootstrap the node hosting Insight is the same as installing the buildnode.iso. Ensure that you plan for a standalone unified management node for production. Click Yes if the node is to be used in the production.

1. Enter *ip a* to verify the br_mgmt and br_api interfaces are up and are bound to bond0 and bond1 respectively. For example:

```
$ ip a
br_api: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP link/ether 00:42:68:6f:79:f2
brd ff:ff:ff:ff:ff:ff
inet nnn.nnn.nnn.nnn/25 brd nnn.nnn.nnn.nnn scope global br_api valid_lft forever preferred_lft
forever
inet6 fe80::3c67:7aff:fef9:6035/64 scope link valid_lft forever preferred_lft forever
bond1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue master br_api state UP link/ether
00:42:68:6f:79:f2 brd ff:ff:ff:ff:ff:ff
br_mgmt: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP link/ether 00:78:88:46:ee:6e
brd ff:ff:ff:ff:ff:ff
inet nnn.nnn.nnn.nnn/24 brd nnn.nnn.nnn.nnn scope global br_mgmt valid_lft forever preferred_lft
forever
inet6 fe80::278:88ff:fe46:ee6e/64 scope link valid_lft forever preferred_lft forever
bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue master br_mgmt state UP
link/ether 00:78:88:46:ee:6e brd ff:ff:ff:ff:ff:ff
```


The br_mgmt and br_api interfaces are created when you install the RHEL on the management node as in Management Node on UCS C-series (M4/M5).

2. Run the following commands to copy the installer directory and the standalone *insight_setup_data_yaml.*

   a. Copy the installer directory to a directory in */root/.* Start the name of the new directory with *Insight-tag_id.*

```
# cd /root/
# cp -pr installer-<tag_id> <Insight-tag_id>
```

b. Copy the standalone *insight_setup_data.yaml*. Standalone_EXAMPLE file from the *Insight-dir/openstack-configs* to any other location on the management node or the BOM.

```
# cp /root/Insight-<tag_id>/openstack-configs/insight_setup_data.yaml.
Standalone_EXAMPLE /root/insight_setup_data.yaml
```

3. Modify the insight setup data according to your requirements.

a. For releases prior to Cisco VIM 3.4.5, run the following commands:

```
#Configuration File:
#########################################################
# User Defined Configuration File.
# Information in this file is specific to the user setup.
#########################################################
# This file is used as an inventory file to setup Insight Container.
#########################################################
# Registry credentials
#########################################################
REGISTRY_USERNAME: '<username>'
REGISTRY_PASSWORD: '<password>'
# Install Mode: connected/disconnected, Optional parameter; default is connected
INSTALL_MODE: connected
# https_proxy: <Name of the proxy server without https://> ; Optional Parameter for INSTALL_MODE
# Needed for connected install only and not required for disconnected mode.
#########################################################
# Super Admin Username Password
#########################################################
# This user is the default Super Admin of the system and can grant Access to all other users
getting
registered to PODs.
# This is a mandatory field and is required to be filled every time.
UI_ADMIN_USERNAME: '<username>'
UI_ADMIN_EMAIL_ID: '<email_id@domain.com>'
# Please define the mail server off which the Insight email alias works;
# For example, outbound.cisco.com
# Optional: Valid SMTP Server is required for sending mails to the customers. By default, it is set
as True.
INSIGHT_SMTP_SERVER: <smtp.domain.com>
#INSIGHT_SMTP_PORT: <port no.>
#optional, defaults to 25, if undefined
# for Insight UI, customer needs to create a mailer, so that automated mails come from that alias;
# For example, vim-insight-admin@cisco.com
# Mandatory: You need to create a valid email alias that would be responsible for sending email
notification for users and UI Admin.
INSIGHT_EMAIL_ALIAS: <Email-Alias@domain.com>
# Optional: Insight Email Alias Password is required if log in on a SMTP server requires
authentication.
INSIGHT_EMAIL_ALIAS_PASSWORD: <password> #Optional
#########################################################
# LDAP Configuration
#########################################################
LDAP_MODE: <True or False> # Required, True when LDAP server is available.
##
Following LDAP settings are required only when LDAP_MODE is True.
LDAP_SERVER: <IP Address of the LDAP Server>
LDAP_PORT: <port no.>
LDAP_ADMIN: '<user-DN for admin>' # e.g Complete DN of admin user for bind and search. <cn=admin,
dc=example, dc=com>
LDAP_ADMIN_PASSWORD: '<password>' # e.g. password of bind user
LDAP_BASE_DN: '<DN tree for Groups>' # e.g. 'ou=Groups,dc=cisco,dc=com'
LDAP_SECURE: '<True or False> # For protocol to be followed. True is for ldaps and False is for
ldap
# LDAP certificate path for self-signed certificates only;
# Required when LDAP_SECURE is True for self-signed certificate.
# In case of trusted Root-CA-Certificate, this key in not required.
LDAP_CERT_PATH: '<abs_location_for_cert_path>'
LDAP_USER_ID_ATTRIBUTE: 'LDAP attribute which can be used as user-id'
```

```
# e.g. <'uid' or 'cn' or 'mail'>
LDAP_GROUP_SEARCH_FILTER: 'LDAP search filter to search groups on LDAP'
# e.g. <LDAP_GROUP_SEARCH_FILTER: "(objectClass=posixGroup)">
LDAP_GROUP_USER_SEARCH_FILTER: 'LDAP search filter to search group-members on LDAP' # e.g.
<LDAP_GROUP_USER_SEARCH_FILTER: "(objectClass=posixAccount)">
#
#
##############################
# LDAP AUTHORIZATION
##############################

LDAP_AUTHORIZATION: <True or False>     #Optional, Default is False

##############################
# Role Mapping keys
##############################
UM_ADMIN_GROUP: <LDAP group to be mapped as Insight UM-Admins> #Optional, Default is CVIM-UM-ADMIN
POD_ADMIN_GROUP: <LDAP group to be mapped as Insight Pod-Admins> #Optional, Default is CVIM-POD-
ADMIN
POD_USER_GROUP: <LDAP group to be mapped as Insight Pod-Users[Write and Read Permissions]>
#Optional, Default is CVIM-POD-USER
READ_ONLY_POD_USER_GROUP: <LDAP group to be mapped as Insight Pod-Users[Read Only]> #Optional,
Default is CVIM-READ-ONLY

#TLS certificate path;
#Absolute TLS certificate path, can also be generated using the script tls_insight_cert_gen.py
located
at
# installer-<tagid>/insight/; if generated by: tls_insight_cert_gen.py, then entry of the info is
optional;
# the script copies the certs to installer-<tagid>/openstack-configs/ dir
PEM_PATH: <abs_location_for_cert_path>
SSL_CERT_CHAIN_FILE: <abs_location_for_cert_chain_file of x509 certificate> #Mandatory if PEM_PATH
is defined in the setupdata.
#If using tls_insight_cert_gen.py to create the cert, please define the following:
CERT_IP_ADDR: <br_api of the insight node> # Mandatory
CERT_HOSTNAME: <Domain name for Cert> # Optional
And then execute:
# cd installer-<tagid>/insight
# ./tls_insight_cert_gen.py --file <absolute path of insight_setup_data.yaml>
The script generates the certs at installer-<tagid>/openstack-configs/ dir
If bringing in a 3rd part Cert, skip the above step and define the following
CERT_IP_ADDR: <br_api of the insight node> # Mandatory
CERT_HOSTNAME: <Domain name for Cert> # Optional
PEM_PATH in insight_setup_data.yaml, and go to step 4 instead of executing # .
/tls_insight_cert_gen.py
As part of insight bootstrap the script copy the certs to installer-<tagid>/openstack-configs/ dir
```

b. For release Cisco VIM 3.4.5, run the following commands:

```
################################################################################
#                     !! INSIGHT SETUP CONFIGURATIONS !!                       #
#                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~                        #

# User Defined Configuration File
# Information in this file is specific to the user setup
# UM -> Unified Management (Insight)

################################################################################
#                           REGISTRY INFORMATION                               #
################################################################################
# Mandatory parameters
REGISTRY_USERNAME: '<username>'
REGISTRY_PASSWORD: '<password>'

# Mandatory Parameter when SDS is enabled
# Not required when SDS is disabled
# Example registry FQDN name [your.domain.com]
```

```
REGISTRY_NAME: '<registry_name>'

################################################################################
#                            INSTALLATION MODE                                 #
################################################################################
# Optional parameter
# Valid options:
# a) connected (default): Node has connectivity to https://cvim-registry.com
#
# b) disconnected: Node has NO connectivity to https://cvim-registry.com
# For details, see Installing UM without Internet Access section
#
INSTALL_MODE: connected

################################################################################
#                           NETWORKING INFORMATION                             #
################################################################################
# Optional, must have at least one sub key defined.
NETWORKING:

  # Optional, needed if the pod is behind a proxy
  # Name of the proxy server without 'https://'
  # Not required for INSTALL_MODE: disconnected
  https_proxy_server: '<proxy.domain.com:8080>'

  # Optional; max of 4 enteries in the list
  ntp_servers:
    - <1.pool.ntp.org>
  # OR
  # Support for IPv6 address
  ntp_servers: ['2001:c5c0:1234:5678:1002::1', 15.0.0.254]

################################################################################
#                           INSIGHT SUPER ADMIN                                #
################################################################################
# User will be the default Super Admin of the system and can grant access to
# all other users getting registered to Cisco VIM pods.
# Mandatory parameters
UI_ADMIN_USERNAME: '<username>'
UI_ADMIN_EMAIL_ID: '<email_id@domain.com>'

################################################################################
#                            SMTP CONFIGURATIONS                               #
################################################################################
# Set this to False, if there is no access to SMTP server
# Optional, valid options are True and False (default)
SMTP_MODE: False

# Following SMTP/EMAIL settings are mandatory "ONLY when" SMTP_MODE is True
# Skip the below keys, if SMTP_MODE is False


# Define the mail server off which the Insight email alias works.
# For example, outbound.cisco.com
# Mandatory: Valid SMTP Server is required for sending mails to the customers.
INSIGHT_SMTP_SERVER: <smtp.domain.com>


# Optional, defaults to 25 if undefined
INSIGHT_SMTP_PORT: <port no.>


# For Insight UI, you must create a mailer, so that all automated mails are sent
# from that alias.
# For example: 'vim-insight-admin@cisco.com'
# Mandatory
INSIGHT_EMAIL_ALIAS: <email-alias@domain.com>


# Optional: Insight Email Alias Password is required if login on a SMTP server
# requires authentication.
```

```
INSIGHT_EMAIL_ALIAS_PASSWORD: <password>

################################################################################
#                       TLS CERT AND HOST INFORMATION                          #
################################################################################
# TLS certificate for INSIGHT UI.
# Absolute TLS certificate path, can also be generated using the script
# tls_insight_cert_gen.py located at insight-<tag_id>/insight/.
# If generated by: tls_insight_cert_gen.py, then below entry is optional.
PEM_PATH: <abs_location_for_cert_path>


# Mandatory in case PEM_PATH is defined.
SSL_CERT_CHAIN_FILE: <abs_location_for_cert_chain_file of x509 certificate>


# If using tls_insight_cert_gen.py to create the cert, define the following:
# Mandatory
CERT_IP_ADDR: <br_api_of_the_UM_node>

# Optional
CERT_HOSTNAME: <domain_name_for_cert>


################################################################################
#                            LDAP CONFIGURATIONS                               #
################################################################################
# LDAP Configurations to enable LDAP users to manage Insight UI.
# Optional, valid options are True and False (default)
LDAP_MODE: False


# Following LDAP settings are required "ONLY when" LDAP_MODE is True.
# Skip the below keys if LDAP_MODE is False

# Mandatory, valid options are True and False.
# True is for secure connection(ldaps).
LDAP_SECURE: <True or False>

# Mandatory, IP address of the LDAP Server or Hostname when LDAP_SECURE is
# True with a trusted Root CA certificate.
LDAP_SERVER: <ip|hostname_of_ldap_server>

# Mandatory, LDAP configured port.
LDAP_PORT: <port no.>

# Mandatory, Base DN of the LDAP server.
# E.g. 'dc=cisco,dc=com'
LDAP_BASE_DN: '<Base_DN_of_ldap_server>'

# Optional, LDAP search filter to search groups on LDAP.
# Defaults to '(objectClass=posixGroup)'
LDAP_GROUP_SEARCH_FILTER: '<ldap_group_search_filter>'

# Optional, LDAP search filter to search group-members on LDAP.
# Defaults to '(objectClass=posixAccount)'
LDAP_GROUP_USER_SEARCH_FILTER: '<ldap_group_user_search_filter>'

# TLS certificate path.
# Required when LDAP_SECURE is True for self-signed certificates only.
# In case of trusted Root-CA-signed certificate, this key is not required.
LDAP_CERT_PATH: '<abs_location_for_cert_path>'

# Mandatory, LDAP attribute which can be used as user-id
# E.g. '<'uid' or 'cn' or 'mail'>'
LDAP_USER_ID_ATTRIBUTE: <ldap_user_id_attribute>

# Optional, complete DN of the admin user for bind and search.
# E.g. '<dn=admin, dc=example, dc=com>'
LDAP_ADMIN: '<user-DN for admin>'
```

```
# Optional, password of the bind admin user: LDAP_ADMIN
LDAP_ADMIN_PASSWORD: '<password>'

# Optional, attribute on the LDAP server used to define group members.
LDAP_GROUP_MEMBER: '< memberUid >'

# Optional, attribute on the LDAP server used to define role associated members.
LDAP_ROLE_MEMBER: '< member >'

# Optional, valid options are True and False (default)
# Enable this to use Insight permissions mapping keys with LDAP group/role.
LDAP_AUTHORIZATION: False

# Following are the optional keys to map Insight permissions with LDAP group/role
# These Group/Role-DN value and LDAP_BASE_DN are used to create full Group/Role-DN.
# UM_ADMIN_GROUP: 'cn=cvim-um-admin,ou=Roles'
# LDAP_BASE_DN: 'dc=cisco,dc=com'
# Full-DN mapped as UM-Admins:- UM_ADMIN_GROUP + LDAP_BASE_DN

# Optional, LDAP Group-DN to be mapped as Insight UM-Admins.
# Defaults to 'cn=cvim-um-admin,ou=Roles'
UM_ADMIN_GROUP: <um_admin_group>

# Optional, LDAP Group-DN to be mapped as Insight Pod-Admins
# Defaults to 'cn=cvim-pod-admin,ou=Roles'
POD_ADMIN_GROUP: <pod_admin_group>

# Optional, LDAP Group-DN to be mapped as Insight Pod-Users[Write and Read Permissions]
# Defaults to 'cn=cvim-pod-user,ou=Roles'
POD_USER_GROUP: <pod_user_group>


# Optional, LDAP Group to be mapped as Insight Pod-Users[Read Only]
# Defaults to 'cn=cvim-read-only,ou=Roles'
READ_ONLY_POD_USER_GROUP: <read_only_pod_user_group>

################################################################################
#                            OPTIONAL FEATURES                                 #
################################################################################
# Automatically assigns the pod_user permissions to um_admin during pod
# registration with default role 'full-pod-access'.
# Optional, valid options are True and False (default)
UM_ADMIN_WITH_FULL_POD_ACCESS: False

# Display all pod-users as suggestion at new pod-user registration.
# Optional, valid options are True and False (default)
DISPLAY_ALL_POD_USERS: False

################################################################################
#                                 UM ADMINS                                    #
################################################################################
# Optional, options for non root user.
# Can have one or more admins.
# Each vim admin must have a vim_admin_password_hash, a vim_admin_public_key,
# or both.

## 1. vim_admin_username: ADMIN USER NAME                                      |
##---------------------------------------------------------------------------
## vim admin user names should satisfy following criteria:
##     a. Required
##     b. Unique
##     c. ASCII chars
##     d. No space allowed
##     e. 1 <= Length <=32
##     f. Only lower case letters
##     g. Digits, underscores, or dashes
##     h. First character must be a letter or an underscore

## 2. vim_admin_password_hash: ADMIN USER PASSWORD HASH                        |
##---------------------------------------------------------------------------
## Optional, to generate a password hash:
```

```
## -> python -c 'import crypt; print crypt.crypt ("<plaintxt_strong_pwd>")'


## 3. vim_admin_public_key: ADMIN USER PUBLIC KEY                          |
##-------------------------------------------------------------------------
## Optional,, vim_admin_public_key is a user's public key.
## It can be generated with 'ssh-keygen'.
## Should be a string that starts with "ssh-rsa AAAA" or "ssh-ed25519 AAAA"


# Optional, must have at least one sub key defined.
vim_admins:
     # vim admin with only password hash.
  -  vim_admin_username: non_root_admin_1
     vim_admin_password_hash: $6.....


     # vim admin with password hash and public key
  -  vim_admin_username: non_root_admin_2
     vim_admin_password_hash: $6.....
     vim_admin_public_key: ssh-rsa AAAA... or ssh-ed25519 AAAA...


     # vim admin with only public key
  -  vim_admin_username: non_root_admin_3
     vim_admin_public_key: ssh-rsa AAAA... or ssh-ed25519 AAAA...

###############################################################################
#                         SSH ACCESS CONFIGURATIONS                           #
###############################################################################
# Optional, valid options are True and False (default)
# True: root can SSH to the UM management node.
# False: root cannot SSH to the UM management node.
#        At least one vim_admin must be configured if this is False
permit_root_login: False

# Optional
# Eg.
# WARNING: Unauthorized access to this system is forbidden and will be
# prosecuted by law. By accessing this system, you agree that your actions
# may be monitored if unauthorized usage is suspected.
ssh_banner: <warning_msg>

###############################################################################
#                               UM LDAP ADMINS                                #
###############################################################################
# Optional, enable LDAP users to SSH to the UM management node.
# Can be added as day-0 or day-1 as part of reconfigure.
# During reconfigure, all but domain_name can be changed.
# New domain_name can be added as part of reconfigure, but once configured
# cannot be changed.

# Optional, contains list of ldap mappings
# Must have at least one element defined in its list
UM_LDAP_ADMINS:
    # All below keys are mandatory
  - domain_name: corp_ldap2
    ldap_search_base: "dc=cisco,dc=com"
    ldap_cert_path: "<cert_path>"
    # For multiple ldap server pass comma separated value.
    ldap_uri: "ldaps://172.29.84.231"

    # All below keys are optional
    ldap_schema: rfc2307
    ldap_user_object_class: posixAccount
    ldap_user_uid_number: uidNumber
    ldap_user_gid_number: uidNumber
    ldap_group_member: memberUid
    ldap_default_bind_dn: "<string>"
    ldap_default_authtok: "<string>"
```

```
    # (password|obfuscated_password)
    ldap_default_authtok_type: "<string>"
    ldap_group_search_base: "<string>"
    ldap_user_search_base: "<string>"
    access_provider: "<string>"
    simple_allow_groups: "<string>"
    ldap_id_use_start_tls: <boolean>

    # never|allow|try|demand)
    ldap_tls_reqcert: "<string>"


    # (ldap|krb5|ad|none)
    chpass_provider: "<string>"

################################################################################
```

4. Save the edited *insight_setup_data.yaml* file.
5. Start the insight installation process:

    a. For releases prior to Cisco VIM 3.4.5, execute the following commands:

```
$ cd /root/Insight-<tag_id>/insight/
$./bootstrap_insight.py --help
usage: bootstrap_insight.py [-h] --action ACTION [--regenerate_secrets]
                            [--setpassword] [--file INSIGHTSETUPDATA] [--keep]
                            [--verbose] [--backupdir BACKUPDIR] [-y]

Insight install setup helper.

optional arguments:

  -h, --help            show this help message and exit
  --action ACTION, -a ACTION
                        install - Install Insight UI
                        install-status - Display Insight Install Status
                        reconfigure - Reconfigure Insight DB, TLS and UI
                        list-reconfigure-keys - List setup data reconfigurable keys
                        update - Update Insight UI
                        update-status - Display Insight Update Status
                        rollback - Rollback Insight UI update
                        commit - Commit Insight UI update
                        backup - Backup Insight UI
                        uninstall - Uninstall Insight UI

  --regenerate_secrets, -r
                        System generated INSIGHT_DB_PASSWORD
  --setpassword, -s     User supplied INSIGHT_DB_PASSWORD,
  --file INSIGHTSETUPDATA, -f INSIGHTSETUPDATA
                        Location of insight_setup_data.yaml
  --keep, -k            Preserve Insight artifacts during uninstall on UM Node only.
  --verbose, -v         Verbose on/off
  --backupdir BACKUPDIR, -b BACKUPDIR
                        Path to backup Insight
  -y, --yes             Option to skip reconfigure or uninstall steps without prompt


$ ./bootstrap_insight.py -a install -f </root/insight_setup_data.yaml>
VIM Insight install logs are at: /var/log/insight/bootstrap_insight
/bootstrap_insight_<date>_<time>.log
Management Node validation!
+-------------------------------+--------+------+
| Rule                                    | Status | Error|
+-------------------------------+--------+------+
| Check Kernel Version                  | PASS          | None |
| Check Ansible Version             | PASS   | None |
| Check Docker Version                    | PASS   | None |
| Check Management Node Tag         | PASS   | None |
```

```
| Check Bond Intf. Settings         | PASS   | None |
| Root Password Check                    | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings            | PASS   | None |
| Check Docker Pool Settings        | PASS   | None |
| Check Home Dir Partition            | PASS   | None |
| Check Root Dir Partition            | PASS   | None |
| Check /var Partition                    | PASS   | None |
| Check LVM partition                   | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+-------------------------------+--------+------+

Insight standalone Input validation!
+-----------------------------------------+--------+-------+
| Rule                                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone Schema Validation      | PASS   | None  |
| Valid Key Check in Insight Setup Data     | PASS   | None  |
| Duplicate Key Check In Insight Setup Data | PASS   | None  |
| CVIM/Insight Workspace Conflict Check     | PASS   | None  |
| Check Registry Connectivity               | PASS   | None  |
| Check LDAP Connectivity                             | PASS   | None  |
| Test Email Server for Insight             | PASS   | None  |
+-----------------------------------------+--------+-------+

Downloading VIM Insight Artifacts, takes time!!!

Cisco VIM Insight Installed successfully!
+----------------------+--------+-------------------------------------------------------------+
| Description                    | Status |
Details                                          |
+----------------------+--------+-------------------------------------------------------------+
| VIM Insight UI URL         | PASS   | https://<br_api:9000>                                       |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml> |
|                                |        |                                                             |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml        |
| VIM Insight Workspace | PASS   | /root/Insight-<tag_id>/insight/                         |
+----------------------+--------+-------------------------------------------------------------+

Cisco VIM Insight backup Info!
+----------------------+--------
+-------------------------------------------------------------------------------------+
| Description                    | Status |
Details                                                                    |
+----------------------+--------
+-------------------------------------------------------------------------------------+
| Insight backup Status | PASS   | Backup done @/var/cisco/insight_backup
/insight_backup_<release_tag>_<date_time>   |
+----------------------+--------
+-------------------------------------------------------------------------------------+

Cisco VIM Insight Autobackup Service Info!
+----------------------+--------+-----------------------------------------------+
| Description                    | Status | Details                                          |
+----------------------+--------+-----------------------------------------------+
| VIM Insight Autobackup | PASS   | [ACTIVE]: Running 'insight-autobackup.service' |
+----------------------+--------+-----------------------------------------------+
Done with VIM Insight install!

VIM Insight install logs are at: "/var/log/insight/bootstrap_insight/"

Logs of Insight Bootstrap are generated at : /var/log/insight/bootstrap_insight/ on the management
node.
Log file name for Insight Bootstrap are in the following format :
bootstrap_insight_<date>_<time>.log. Only ten bootstrap Insight log files are displayed at a time.

Once the bootstrap process is completed a summary table preceding provides the information of the
UI
URL and the corresponding login credentials. After first login, for security reasons, we recommend
you to change the Password.
```

```
Insight autobackup takes place after the installation, and is located at default backup location
/var/cisco/insight_backup; details of which is provided in the backup summary table.

To add a new UI Admin in a setup that just got created, login to VIM insight and add a new UI admin
user from the Manage UI Admin Users menu. Without doing a fresh install (that is un-bootstrap,
followed by bootstrap) of the insight application, the UI admin that was bootstrapped cannot be
changed.
Refer Cisco VIM Insight Post Bootstrap Validation Checks section, to verify the bootstrap status of
Cisco VIM Insight.
```

b. For release Cisco VIM 3.4.5, execute the following commands:

```
$ cd /root/Insight-<tag_id>/
$ ./insight/insight_runner.py -h
usage: insight_runner.py [-h] [-f SETUPFILE] [-y] [-s SKIP_STEPS]
                         [-p PERFORM_STEPS] [-l] [-v]
                         [--update] [--dry-run] [--commit] [--rollback]
                         [--reconfigure] [--regenerate_secrets]
                         [--setpassword] [-i] [-u] [--list-reconfigure-keys]

INSIGHT ORCHESTRATOR

optional arguments:
  -h, --help            show this help message and exit
  -f SETUPFILE, --setupfile SETUPFILE
                        User input file, default is insight_setup_data.yaml
  -y, --yes             Yes option to skip steps without prompt
  -s SKIP_STEPS, --skip_steps SKIP_STEPS
                        Comma separated list of steps to skip. eg -s 1
  -p PERFORM_STEPS, --perform_steps PERFORM_STEPS
                        Comma separated list of steps to perform. eg -p 2
  -l, --list_steps      List steps
  -v, --version         Display version info
  --update              Update Insight
  --dry-run             Dry Run to find all containers marked for update
  --commit              Commit Insight Update
  --rollback            Rollback Insight Update
  --reconfigure         Reconfigure Insight DB, TLS and UI
  --regenerate_secrets  System generated Insight DB_ROOT_PASSWORD
  --setpassword         User supplied Insight DB_ROOT_PASSWORD
  -i, --install-status  Display Insight install status
  -u, --update-status   Display Insight update status
  --list-reconfigure-keys
                        List setup data reconfigurable keys


$ ./insight/insight_runner.py -l

           !! INSIGHT !!
CISCO VIM UNIFIED MANAGEMENT ORCHESTRATOR
=========================================
 +--------------------+----------------+
 |     Operations     |  Operation ID  |
 +--------------------+----------------+
 |  INPUT_VALIDATION  |       1        |
 |  BOOTSTRAP_INFRA   |       2        |
 +--------------------+----------------+


$ ./insight/insight_runner.py -p 1,2 -f </root/insight_setup_data.yaml>

Perform steps ['1', '2']. Continue (Y/N)y

The logs for this run are available at /var/log/insight/bootstrap/<date>_<time>

                ##############################
                 CISCO INSIGHT ORCHESTRATOR
                ##############################
```

```
[1/2][INPUT_VALIDATION: INIT]                                                    [   \   ]    0min
1sec


Management Node validation!
+-------------------------------+--------+------+
| Rule                                    | Status | Error|
+-------------------------------+--------+------+
| Check Kernel Version                  | PASS          | None |
| Check Ansible Version             | PASS   | None |
| Check Docker Version                    | PASS   | None |
| Check Management Node Tag         | PASS   | None |
| Check Bond Intf. Settings         | PASS   | None |
| Root Password Check                   | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings            | PASS   | None |
| Check Docker Pool Settings        | PASS   | None |
| Check Home Dir Partition            | PASS   | None |
| Check Root Dir Partition            | PASS   | None |
| Check /var Partition                    | PASS   | None |
| Check LVM partition                   | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+-------------------------------+--------+------+

Insight standalone Input validation!
+-----------------------------------------+--------+-------+
| Rule                                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone Schema Validation      | PASS   | None  |
| Valid Key Check in Insight Setup Data     | PASS   | None  |
| Duplicate Key Check In Insight Setup Data | PASS   | None  |
| CVIM/Insight Workspace Conflict Check     | PASS   | None  |
| Check Registry Connectivity               | PASS   | None  |
| Check LDAP Connectivity                     | PASS   | None  |
| Test Email Server for Insight             | PASS   | None  |
+-----------------------------------------+--------+-------+
.

[2/2][BOOTSTRAP_INFRA: vim-admins-Restart and enable sss daemon]              [ DONE! ]    1min
23secs

.
.

Cisco VIM Insight Installed successfully!
+------------------+--------+-------------------------------------------------------------+
| Description      | Status | Details                                                     |
+------------------+--------+-------------------------------------------------------------+
| Insight UI URL   | PASS   | https://<br_api>:9000                                       |
| UI Admin Email ID | PASS   | Check for info @: /root/insight-openstack-                  |
|                  |        | configs/insight_setup_data.yaml                             |
| UI Admin Password | PASS   | Check for info @: /opt/cisco/insight/secrets.yaml           |
+------------------+--------+-------------------------------------------------------------+

Backup Validation Passed
[***][AUTOBACKUP: Completed Step 1 of backup, backupdir:... /var/cisco/insight_backup
/insight_autobackup_3.4.5_<date>_<time>]
[***][AUTOBACKUP: Starting post-backup..please wait!!]
[***][AUTOBACKUP: Completed Cisco UM backup ... /var/cisco/insight_backup/insight_autobackup_3.4.5
_<date>_<time>

Ended Installation [BOOTSTRAP_INFRA] [Success]

The logs for this run are available at /var/log/insight/bootstrap/<date>_<time>

Logs of Insight Bootstrap are generated at : /var/log/insight/bootstrap/ on the UM management
node.
Log file name for Insight Bootstrap are in the following tar format: insight_<date>_<time>.tar.gz

Once the bootstrap process is completed a summary table preceding provides the information of the
```

UI URL and the corresponding login credentials. After first login, for security reasons, we recommend you to change the Password.

Insight autobackup takes place after the installation, and is located at default backup location /var/cisco/insight_backup; details of which is provided below the bootstrap summary table.

To add a new UI Admin in a setup that just got created, login to VIM insight and add a new UI admin user from the Manage UI Admin Users menu. Without doing a fresh installation (that is un-bootstrap, followed by bootstrap) of the insight application, the UI admin that was bootstrapped cannot be changed.

Refer Cisco VIM Insight Post Bootstrap Validation Checks section, to verify the bootstrap status of Cisco VIM Insight.

UM with Cisco VIM Software Hub

UM with Cisco VIM Software Hub

To reduce the logistics of the artifact distribution during an air-gapped installation, use Cisco VIM Software Hub. To download the artifacts to the Cisco VIM Software Hub server, follow the instructions available at Cisco VIM Software Hub. Then, you can use the connected way of installing Unified Management (UM) on the UM node.

To install UM on the UM node through Cisco VIM Software Hub, you need REGISTRY_NAME as an additional field in the setup data for the UM node.

```
# Mandatory parameter when SDS is enabled.
REGISTRY_NAME: '<registry_name>'
```

Here, the registry name is fully qualified domain name (FQDN) or your domain.com. When Cisco VIM Software Hub is not enabled, you must not use this parameter.
Once REGISTRY_NAME is defined in the setup data, the UM software fetches the artifacts from the Cisco VIM Software Hub server as long as the INSTALL_MODE is defined to be connected or not defined in the *insight_setup_data.yaml* file. By default, it is assumed to be connected.

UM with LDAP

Installing UM with LDAP

Insight supports both LDAP and LDAPs (Secure over SSL) for an AD (Active Directory) environment. You can choose only one at a time.

LDAPs supports connection using both self-signed and CA-signed certificate. You can choose any type of certificate for LDAPs.

- Selecting self-signed certificate option will require a certificate for verification over LDAPs and to make a secure connection to LDAP over SSL.
- No certificate is required when selecting CA-signed certificate option.

The following are the required keys in setup data for LDAP support:

- LDAP_MODE: < True or False >
- LDAP_SERVER: < IP address of LDAP server >
- LDAP_PORT: < Port no. >
- LDAP_BASE_DN: <DN tree for Groups>
- LDAP_SECURE: < True or False >
- LDAP_USER_ID_ATTRIBUTE: <'uid' or 'cn' or 'mail'>

Following optional key is required in the setup_data file, when LDAP_SECURE is True and a self-signed certificate is used:
LDAP_CERT_PATH: < Path of cert file >
Following optional keys are required in the setup_data file, when LDAP server is configured to support simple binding:

- LDAP_ADMIN: < User-Name of Admin user >
- LDAP_ADMIN_PASSWORD: < Password of user Admin >
- LDAP_GROUP_SEARCH_FILTER: < Filter to search LDAP-Group on Server >
- LDAP_GROUP_USER_SEARCH_FILTER: < Filter to search user in LDAP-Group >
- LDAP_GROUP_MEMBER: < Attribute used for defining group-member association with LDAP server>

Following optional key is required in the setup_data file, to setup Insight authorization via LDAP server.:

LDAP_AUTHORIZATION: < True or False >

This key is non-reconfigurable, that is, this functionality can only be set ON/OFF at the time of fresh-installation.

Following optional keys are required in the setup_data file, when LDAP authorization is True:

- UM_ADMIN_GROUP: <LDAP group-dn to be mapped as Insight UM-Admins>
- POD_ADMIN_GROUP: <LDAP group-dn to be mapped as Insight Pod-Admins>
- POD_USER_GROUP: <LDAP group-dn to be mapped as Insight Pod-Users[Write and Read Permissions]>
- READ_ONLY_POD_USER_GROUP: <LDAP group-dn to be mapped as Insight Pod-Users[Read Only]>
- LDAP_ROLE_MEMBER: < Attribute used for defining association of role to user/group on LDAP server>

The group-DN values must exclude LDAP_BASE_DN value. For example: UM_ADMIN_GROUP: “cn=cvim-um-admin,ou=Group”

UM Without SMTP

Installing UM Without SMTP

By default, a SMTP infrastructure is required for Cisco VIM UM service.
For releases starting from Cisco VIM 2.4.2, the UM service is supported in the absence of SMTP.

> ⚠ The migration of the UM service to SMTP-enabled mode from the mode which does not require SMTP is not supported.

To install UM without SMTP, follow the below steps:

1. Modify the *insight_setup_data.yaml* file and add the following key:

   ```
   SMTP_MODE: False
   ```

2. Remove the following keys from the *insight_setup_data.yaml:*

   ```
   INSIGHT_SMTP_SERVER
   INSIGHT_EMAIL_ALIAS
   INSIGHT_SMTP_PORT and
   INSIGHT_EMAIL_ALIAS_PASSWORD
   ```

3. Save the yaml file and begin the installation from the Insight directory:

   ```
   #./bootstrap_insight.py -a install -f <path to insight_setup_data.yaml>
   ```

   With SMTP disabled, bootstrap Insight sets both the Super Admin and Pod Admin as the default user. The default user can login and register the pod, but cannot perform the following:

   - Add new user at pod level.
   - Add new Pod Admin.
   - Add new Super Admin.

To add new user or update password for the existing user for Insight without SMTP, use the below script:

```
# ./user_populate.py --help
usage: user_populate.py [-h] [--username USERNAME] [--emailid EMAILID]
[--usertype USERTYPE] [--updatepass UPDATEPASS]

Optional arguments:
-h, --help
show the help message and exit
--username USERNAME, -u USERNAME
name of the user.
--emailid EMAILID, -e EMAILID
Email ID of the user.
--usertype USERTYPE, -t USERTYPE
User Type:
super_admin - User is Super User for Insight
pod_admin - User allowed to register new PODS
pod_user - User can only get associated with PODS
--updatepass UPDATEPASS, -p UPDATEPASS
Email ID of user whose password needs to be updated.
```

To add a user, enter the below command:

```
#./user_populate.py -u abc -e abc@abc.com -t pod_user
```

- *-t* can take one of the following values such as *super_admin, pod_admin,* and *pod_user* as an argument.
- If the user already exists, an error stating **User already exists** is displayed. If the user is new, the script prompts to enter a new password and confirmation password.

To use forgot password functionality, use the below command:

```
#./user_populate.py -p abc@abc.com
```

If you add a user or change a password using *-p* option, you are redirected to the **Change Password** page on first login through UM.

UM Without Internet Access

Installing UM without Internet Access

Overview

Complete the following steps to install Cisco VIM Insight on the Cisco NFVI management node. As security is paramount to pod management, the web-service hosting the single pane of glass is protected through TLS. Following are the steps to get the TLS certificate setup going.

You can select one of the following approaches for the TLS certificate configurations:

- Provide your own certificate: You can bring in your certificate on the management node and provide the absolute path of .pem and CA certificate files in the *insight_setup_data.yaml* file. The path must be provided as a value for the key PEM_PATH in the *insight_setup_data.yaml* file.
- Generate a new certificate on the node. You can create a new certificate on the node by running the following command:

```
# cd /root/Insight-<tag_id>/insight/
#./tls_insight_cert_gen.py -f <path_to_insight_setup_data.yaml>/insight_setup_data.yaml
```

This script searches for the PEM_PATH inside the *insight_setup_data.yaml.* As the path is not provided, it creates a new certificate inside *install-dir /openstack-configs.*

The self-signed certificate generation utility script is provided for lab/testing deployment only. Ensure that you do not use a self-signed certificate generated by this utility for the production deployment.

The UM node is installed in the air-gapped mode, when the data center does not have internet connectivity. You can use the USB drive to load the installation files on the UM node. Downloading them to the USB drive may take several hours depending on the speed of your internet connection.

⚠ Only Insight installation on a standalone UM node is supported. Attempt to install Insight on Cisco VIM management node causes unexpected behavior.

Installation

The procedure to bootstrap the node hosting Insight is the same as installing the *buildnode.iso.* Ensure that you plan for a standalone UM node for production. Click **Yes** if the node is to be used in the production.

Before you begin

- Ensure that you have set up a CentOS 7 staging server (VM, laptop, or UCS server) with a 64 GB USB 2.0 drive.
- Ensure that you have internet, preferably a wired connection, to download the Cisco VIM installation files on the USB drive.
- Ensure that you have disabled the CentOS sleep mode.

1. On the staging server, use yum to install the following packages:
   a) PyYAML

   b) python-requests

   c) Python 3.6 (rh-python36))

   Check if python 3.6 binary is located at */opt/rh/rh-python36/root/bin/*, if not copy the python 3.6 binary to */opt/rh/rh-python36/root/bin/.*
2. Access the Cisco VIM software download website using a web browser.
3. Log in with the credentials provided by your account representative and download the ***getartifacts.py*** script from the external registry.

   ```
   # download the new getartifacts.py file
   curl -o getartifacts.py
   https://username:password@cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/<3.4.x>
   /getartifacts.py
   # Change the permission of getartifacts.py
   chmod +x getartifacts.py
   ```

4. Run the ***getartifacts.py*** script. The script formats the USB 2.0 drive (or USB 3.0 drive for M5-based management node) and downloads the installation files. You must provide the registry username and password, tag ID, and USB partition on the staging server.

```
./getartifacts.py -h
usage: getartifacts.py [-h] -t TAG -u USERNAME -p PASSWORD [--proxy PROXY]
                       [--retry] (-d DRIVE | -f FILE)
                       [--mgmtk8s | --argus | --insight | --sds | -U]

Script to pull container images en masse.

optional arguments:
  -h, --help            show this help message and exit
  -t TAG, --tag TAG     Installer version to pull
  -u USERNAME, --username USERNAME
                        Registry username
  -p PASSWORD, --password PASSWORD
                        Registry password
  --proxy PROXY         https_proxy if needed
  --retry               Try to complete a previous fetch
  -d DRIVE, --drive DRIVE
                        Provide usb drive path
  -f FILE, --file FILE  location of image file
  --mgmtk8s             Additionally download CVIM MON HA artifacts
  --argus               Additionally download argus artifacts
  --insight             Additionally download insight artifacts
  --sds                 Additionally download sds artifacts
  -U, --upgrade         Additionally download artifacts for upgrade from 2.4.x

This script pulls images from remote registry then copies the contents to USB
drive or image file based on the user supplied option
```

The *getartifacts.py* script gets the images from the remote registry and copies the contents to the USB drive.

5. To identify the USB drive, execute the *lsblk* command before and after inserting the USB drive. The command displays a list of available block devices. You can use the output data to find the location of the USB drive. You must provide the entire drive path in the `-d` option instead of any partition.
   For example:

   ```
   sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> --insight [--proxy proxy.
   example.com]
   ```

6. Verify the integrity of the downloaded artifacts and container images.

```
# create a directory sudo mkdir -p /mnt/Cisco
# /dev/sdc is the USB drive, same as supplied in getartifacts.py python script sudo mount /dev/sdc1
/mnt/Cisco
cd /mnt/Cisco
# execute the test-usb help to look at the options
./test-usb -h

usage: ./test-usb [-h] -- Show this program to check integrity of artifacts in this USB drive/image file
                  [-a] -- Check integrity of all (core and all) artifacts in this USB drive/image File
                  [-l] -- Location of artifacts
                  [-f] -- Location of image file
                  [-U] -- test upgrade artifacts from 2.4.x to 3.4.y
# execute the verification script
./test-usb
# failures will be explicitly displayed on screen, sample success output below
# sample output of ./test-usb execution with 3.0.0 release
#./test-usb
INFO: Checking the integrity of this USB drive
INFO: Checking artifact buildnode-K9.iso
INFO: Checking artifact registry-3.0.0.tar.gz
INFO: Checking the integrity of this USB drive
INFO: Checking artifact buildnode-K9.iso
INFO: Checking artifact registry-3.0.0.tar.gz
INFO: Checking artifact mariadb-app-K9.tar.gz
INFO: Checking artifact haproxy-K9.tar.gz
INFO: Checking artifact insight-K9.tar.gz
Node
INFO: Checking required layers:
INFO: 548 layer files passed checksum.
If a failure occurs, an error message is displayed. For example:
# ./test-usb
INFO: Checking the integrity of this USB drive
INFO: Checking artifact buildnode-K9.iso
ERROR: Checksum for artifact buildnode-K9.iso does not match ('SHA512 (buildnode-K9.iso) =
96ec62a0932a0d69daf60acc6b8af2dc4e5eca132cd3781fc17a494592feb52a7f171eda25e59c0d326fbb09194eeda66036cbdc3
870dafe74f59cf1f2dce225'
!= 'SHA512 (buildnode-K9.iso) =
a6a9e79fa08254e720a80868555679baeea2dd8f26a0360ad47540eda831617bea0514a117b12ee5f36415b7540afa112a1c904cd
69e40d704a8f25d78867acf')
INFO: Checking artifact registry-3.4.2.tar.gz
ERROR: Artifact registry-3.4.2.tar.gz is not present INFO: Checking required layers:
ERROR: Layer file sha256:002aa1f0fbdaea7ea25da1d906e732fe9a9b7458d45f8ef7216d1b4314e05207 has a bad
checksum
ERROR: Layer file sha256:5be3293a81773938cdb18f7174bf595fe7323fdc018c715914ad41434d995799 has a bad
checksum
ERROR: Layer file sha256:8009d9e798d9acea2d5a3005be39bcbfe77b9a928e8d6c84374768ed19c97059 has a bad
checksum
Cisco Virtualized Infrastructure Manager Installation Guide, 3.4.x
97
Preparing for Cisco NFVI Installation
Installing Cisco VIM Software Hub in Air-Gapped Mode
ERROR: Layer file sha256:ea55b2fc29b95d835d16d7eeac42fa82f17e985161ca94a0f61846defff1a9c8 has a bad
checksum
INFO: 544 layer files passed checksum.
```

7. To resolve failure in downloading artifacts, unmount the USB and run the ***getartifacts*** command again with the ***--retry*** option.

```
sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> --insight --retry
```

8. Mount the USB and then run the ***test-usb*** command to validate if all the files are downloaded.

```
# /dev/sdc is the USB drive, same as supplied in getartifacts.py python script
sudo mount /dev/sda1 /mnt/Cisco
cd /mnt/Cisco
```

9. Execute the verification script.

```
# ./test-usb
# In case of failures the out of the command displays a message indicating the same on the screen
```

10. When the USB integrity test completes, unmount the USB.

```
sudo umount /mnt/Cisco
```

11. After the artifacts of a target release are saved on the USB, you must unplug the USB from the staging server, connect it to the UM node, and then perform the following steps on the UM node:

    a. Provision your UM node with the build node ISO of that release and then connect the USB to UM node.
    b. To copy the contents of the USB to UM node navigate to the */root/insight-<tag>* directory, and then execute the import artifacts command:

```
# cd ~/insight-<tag>/tools
# ./import_artifacts.sh
```

> ⚠ To update UM, do not proceed beyond Step 11 and continue with *Step 5* of Upgrade/Update UM

12. To create *insight_setup_data.yaml*, see *Step 2 and Step 3 of Installation* under UM with Internet Access
13. Save the edited *insight_setup_data.yaml* file.
14. Start the insight installation process:

    a. For releases earlier to Cisco 3.4.5:

```
$ cd /root/insight-<tag_id>/insight/
$./bootstrap_insight.py --help

usage: bootstrap_insight.py [-h] --action ACTION [--regenerate_secrets]
                            [--setpassword] [--file INSIGHTSETUPDATA] [--keep]
                            [--verbose] [--backupdir BACKUPDIR] [-y]

Insight install setup helper.

optional arguments:

  -h, --help            show this help message and exit
  --action ACTION, -a ACTION
                        install - Install Insight UI
                        install-status - Display Insight Install Status
                        reconfigure - Reconfigure Insight DB, TLS and UI
                        list-reconfigure-keys - List setup data reconfigurable keys
                        update - Update Insight UI
                        update-status - Display Insight Update Status
                        rollback - Rollback Insight UI update
                        commit - Commit Insight UI update
                        backup - Backup Insight UI
                        uninstall - Uninstall Insight UI

  --regenerate_secrets, -r
                        System generated INSIGHT_DB_PASSWORD
  --setpassword, -s     User supplied INSIGHT_DB_PASSWORD,
  --file INSIGHTSETUPDATA, -f INSIGHTSETUPDATA
                        Location of insight_setup_data.yaml
  --keep, -k            Preserve Insight artifacts during uninstall on UM Node only.
  --verbose, -v         Verbose on/off
  --backupdir BACKUPDIR, -b BACKUPDIR
                        Path to backup Insight
  -y, --yes             Option to skip reconfigure or uninstall steps without prompt


$ ./bootstrap_insight.py -a install -f </root/insight_setup_data.yaml>
# Insight Schema Validation would be initiated:
```

```
VIM Insight install logs are at: / var/log/insight/<bootstrap_insight_<date>_<time>.log
Management Node Validations!
+-------------------------------+--------+------+
| Rule                                    | Status | Error|
+-------------------------------+--------+------+
| Check Kernel Version                   | PASS   | None |
| Check Ansible Version                   | PASS   | None |
| Check Docker Version                    | PASS   | None |
| Check Management Node Tag     | PASS   | None |
| Check Bond Intf. Settings     | PASS   | None |
| Root Password Check                     | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings              | PASS   | None |
| Check Docker Pool Settings        | PASS   | None |
| Check Home Dir Partition      | PASS   | None |
| Check Root Dir Partition      | PASS   | None |
| Check /var Partition          | PASS   | None |
| Check LVM partition           | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+-------------------------------+--------+------+

Insight standalone Input Validations!
+-----------------------------------------+--------+-------+
| Rule                                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone Schema Validation             | PASS   | None  |
| Valid Key Check in Insight Setup Data            | PASS   | None  |
| Duplicate Key Check In Insight Setup Data | PASS   | None  |
| CVIM/Insight Workspace Conflict Check     | PASS   | None  |
| Check Registry Connectivity                       | PASS   | None  |
| Check LDAP Connectivity                           | PASS   | None  |
| Test Email Server for Insight                | PASS   | None  |
+-----------------------------------------+--------+-------+

Setting up Insight, Kindly wait!!!
Cisco VIM Insight Installed successfully!

+----------------------+--------+-------------------------------------------------------------+
| Description                    | Status |
Details                                                |
+----------------------+--------+-------------------------------------------------------------+
| VIM Insight UI URL         | PASS          | https://<br_api:
9000>                                  |
| VIM UI Admin Email ID | PASS          | Check for info @: <abs path of insight_setup_data.yaml>
|
| VIM UI Admin Password | PASS          | Check for info @ /opt/cisco/insight/secrets.yaml
|
| VIM Insight Workspace | PASS          | /root/Insight_<tag_id>/insight/
|
+----------------------+--------+-------------------------------------------------------------+
Cisco VIM Insight backup Info!

+----------------------+-------
+-------------------------------------------------------------------------------+
| Description              | Status|
Details                                                                        |
+----------------------+-------
+-------------------------------------------------------------------------------+
| Insight backup Status| PASS  | Backup done @/var/cisco/insight_backup
/insight_backup_<release_tag>_<date_time>|
+----------------------+-------
+-------------------------------------------------------------------------------+
Done with VIM Insight install!

VIM Insight install logs are at: /var/log/insight/bootstrap_insight/
Logs of Insight Bootstrap is generated at : /var/log/insight/bootstrap_insight/ on the management
node.
Log file name for Insight Bootstrap is in the following format :
bootstrap_insight_<date>_<time>.log. Only ten bootstrap Insight log files are displayed at a time.
```

```
Once the bootstrap process is completed a summary table preceding provides the information of the
UI
URL and the corresponding login credentials. After first login, for security reasons, we recommend
you to change the Password.

Insight autobackup takes place after an install and is located at default backup location
/var/cisco/insight_backup; details of which is provided in the backup summary table.

To add a new UI Admin in a setup that just got created, login to VIM insight and add a new UI admin
user from the Manage UI Admin Users menu. Without doing a fresh install (that is un-bootstrap,
followed by bootstrap) of the insight application, the UI admin that was bootstrapped with cannot
be
changed.
Refer Cisco VIM Insight Post Bootstrap Validation Checks, to verify the bootstrap status
of Cisco VIM Insight.
```

b. For Cisco VIM 3.4.5, execute the following commands:

```
$ cd /root/Insight-<tag_id>/
$ ./insight/insight_runner.py -h
usage: insight_runner.py [-h] [-f SETUPFILE] [-y] [-s SKIP_STEPS]
                         [-p PERFORM_STEPS] [-l] [-v]
                         [--update] [--dry-run] [--commit] [--rollback]
                         [--reconfigure] [--regenerate_secrets]
                         [--setpassword] [-i] [-u] [--list-reconfigure-keys]


INSIGHT ORCHESTRATOR


optional arguments:
  -h, --help            show this help message and exit
  -f SETUPFILE, --setupfile SETUPFILE
                        User input file, default is insight_setup_data.yaml
  -y, --yes             Yes option to skip steps without prompt
  -s SKIP_STEPS, --skip_steps SKIP_STEPS
                        Comma separated list of steps to skip. eg -s 1
  -p PERFORM_STEPS, --perform_steps PERFORM_STEPS
                        Comma separated list of steps to perform. eg -p 2
  -l, --list_steps      List steps
  -v, --version         Display version info
  --update              Update Insight
  --dry-run             Dry Run to find all containers marked for update
  --commit              Commit Insight Update
  --rollback            Rollback Insight Update
  --reconfigure         Reconfigure Insight DB, TLS and UI
  --regenerate_secrets  System generated Insight DB_ROOT_PASSWORD
  --setpassword         User supplied Insight DB_ROOT_PASSWORD
  -i, --install-status  Display Insight install status
  -u, --update-status   Display Insight update status
  --list-reconfigure-keys
                        List setup data reconfigurable keys


$ ./insight/insight_runner.py -l

           !! INSIGHT !!
CISCO VIM UNIFIED MANAGEMENT ORCHESTRATOR
=========================================
 +--------------------+----------------+
 |     Operations     |  Operation ID  |
 +--------------------+----------------+
 |  INPUT_VALIDATION  |       1        |
 |  BOOTSTRAP_INFRA   |       2        |
 +--------------------+----------------+
```

```
$ ./insight/insight_runner.py -p 1,2 -f </root/insight_setup_data.yaml>

Perform steps ['1', '2']. Continue (Y/N)y

The logs for this run are available at /var/log/insight/bootstrap/<date>_<time>

                ##############################
                 CISCO INSIGHT ORCHESTRATOR
                ##############################

[1/2][INPUT_VALIDATION: INIT]                                                [   \   ]    0min
1sec


Management node validation!
+------------------------------+--------+------+
| Rule                         | Status | Error|
+------------------------------+--------+------+
| Check Kernel Version         | PASS   | None |
| Check Ansible Version        | PASS   | None |
| Check Docker Version         | PASS   | None |
| Check Management Node Tag    | PASS   | None |
| Check Bond Intf. Settings    | PASS   | None |
| Root Password Check          | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings       | PASS   | None |
| Check Docker Pool Settings   | PASS   | None |
| Check Home Dir Partition     | PASS   | None |
| Check Root Dir Partition     | PASS   | None |
| Check /var Partition         | PASS   | None |
| Check LVM partition          | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+------------------------------+--------+------+

Insight standalone input validation!
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone Schema Validation    | PASS   | None  |
| Valid Key Check in Insight Setup Data   | PASS   | None  |
| Duplicate Key Check In Insight Setup Data | PASS   | None  |
| CVIM/Insight Workspace Conflict Check   | PASS   | None  |
| Check Registry Connectivity             | PASS   | None  |
| Check LDAP Connectivity                 | PASS   | None  |
| Test Email Server for Insight           | PASS   | None  |
+-----------------------------------------+--------+-------+
.
.

[2/2][BOOTSTRAP_INFRA: vim-admins-Restart and enable sss daemon]             [ DONE! ]    1min
23secs

.
.

Cisco VIM Insight Installed successfully!
+-------------------+--------+-------------------------------------------------------------+
| Description       | Status | Details                                                     |
+-------------------+--------+-------------------------------------------------------------+
| Insight UI URL    | PASS   | https://<br_api>:9000                                       |
| UI Admin Email ID | PASS   | Check for info @: /root/insight-openstack-                  |
|                   |        | configs/insight_setup_data.yaml                             |
| UI Admin Password | PASS   | Check for info @: /opt/cisco/insight/secrets.yaml           |
+-------------------+--------+-------------------------------------------------------------+

Backup Validation Passed
[***][AUTOBACKUP: Completed Step 1 of backup, backupdir:... /var/cisco/insight_backup
/insight_autobackup_3.4.6_<date>_<time>]
[***][AUTOBACKUP: Starting post-backup..please wait!!]
[***][AUTOBACKUP: Completed Cisco UM backup ... /var/cisco/insight_backup/insight_autobackup_3.4.6
_2020-<date>_<time>
```

```
Ended Installation [BOOTSTRAP_INFRA] [Success]

The logs for this run are available at /var/log/insight/bootstrap/<date>_<time>

Logs of Insight Bootstrap are generated at : /var/log/insight/bootstrap/ on the UM management node.
Log file name for Insight Bootstrap are in the following tar format: insight_<date>_<time>.tar.gz

Once the bootstrap process is completed a summary table preceding provides the information of the
UI URL and the corresponding login credentials. After first login, for security reasons, we
recommend you to change the Password.

Insight autobackup takes place after the installation, and is located at default backup location
/var/cisco/insight_backup; details of which is provided below the bootstrap summary table.

To add a new UI Admin in a setup that just got created, login to VIM insight and add a new UI
admin user from the Manage UI Admin Users menu. Without doing a fresh install (that is un-
bootstrap, followed by bootstrap) of the insight application, the UI admin that was bootstrapped
cannot be changed.

Refer Cisco VIM Insight Post Bootstrap Validation Checks section, to verify the bootstrap status
of Cisco VIM Insight.
```

UM Optional Services

UM Optional Services

For releases from Cisco VIM 3.2.0, Cisco VIM UM service provides the following optional features:

- Automatically add each UM-admin as the default pod-user with Full-Pod-Access to a pod during pod-registration.
- Display all the pod-users as suggested users, while registering a new pod-user.

> ⚠ By default, these features are set to False. To use these features, change the value of corresponding keys to **True** in Insight setup data file.

To install UM with these features, follow the below steps:

1. Modify the insight_setup_data.yaml file and add following key:
    a. To automatically add each UM admin to pod with Full-Pod-Access during pod registration, set the following key with **True** as value:

    ```
    UM_ADMIN_AS_POD_ADMIN: True
    ```

    b. To display the suggested users during pod-user registration, set the following key with **True** as value:

    ```
    DISPLAY_ALL_POD_USERS: True
    ```

2. Save the yaml file and begin the installation from the insight directory:
    a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

    ```
    # cd /root/Insight-<tag_id>/
    #./bootstrap_insight.py -a install -f <path to insight_setup_data.yaml>
    ```

    b. For Cisco VIM 3.4.5, enter the following commands:

    ```
    # cd /root/Insight-<tag_id>/
    # ./insight/insight_runner.py -p 1,2 -f </root/insight_setup_data.yaml>
    ```

Insight Post Bootstrap Validation Checks

Insight Post Bootstrap Validation Checks

Follow the below steps to check the Cisco VIM Insight bootstrap validation:

1. Check Cisco Insight installation workspace:

```
# cd $HOME
# ll
Look for path pointed by symlink 'insight-openstack-configs'
# lrwxrwxrwx.  1 root root   38 May 20 23:59 insight-openstack-configs -> /root/insight-<tag_id>
/openstack-configs
```

> ⚠ The above step is applicable only for release Cisco VIM 3.4.5.

2. After the Cisco VIM Insight bootstrap, you can view the status of Insight installation through *install-status* action using bootstrap:

   a. For releases prior to Cisco VIM 3.4.5:

```
# cd Insight-<tag_id>/insight
# ./bootstrap_insight.py -a install-status

$ Cisco VIM Insight Install Status!
+-----------------------+--------+-----------------------------------------------+
| Description                    |Status         |   Details                      |
|
+-----------------------+--------+-----------------------------------------------+
| VIM Insight Setup            | PASS          |
Success                                                          |
| VIM Insight Version         | PASS   | <release_tag>                                  |
| VIM Insight UI URL         | PASS   | https://<br_api:9000>                          |
| VIM Insight Container | PASS   | insight_<tag_id>                                |
| VIM Mariadb Container | PASS   | mariadb_<tag_id>                                |
| VIM Insight Autobackup| PASS   | [ACTIVE]: Running 'insight-autobackup.service' |
| VIM Insight Workspace | PASS   | /root/installer-<tag_id>/insight                |
+-----------------------+--------+-----------------------------------------------+
```

   b. For Cisco VIM 3.4.5, enter the following commands:

```
# cd Insight-<tag_id>
# ./insight/insight_runner.py --install-status
Fetching Insight install status..

Cisco VIM Insight Install Status!
+--------------------+--------+-----------------------------------------------+
| Description        | Status | Details                                       |
+--------------------+--------+-----------------------------------------------+
| Insight Setup      | PASS   | Success                                       |
| Insight Version    | PASS   | OG: <release_tag>                             |
| Insight UI URL     | PASS   | https://<br_api>:9000                         |
| Mariadb Container  | PASS   | mariadb_<tag_id>                              |
| Insight Container  | PASS   | insight_<tag_id>                              |
| Insight Autobackup | PASS   | [ACTIVE]: Running 'insight-autobackup.service' |
+--------------------+--------+-----------------------------------------------+
```

3. You can also verify whether the Insight and MySQL containers are up or not, by running the following command:

```
$ source ~/.bashrc
$ dp

   NAMES             STATUS
insight_26349       Up 8 days
mariadb_26349       Up 8 days
```

4. Check the status of Insight by running the following command:

```
$ systemctl status docker-insight
docker-insight.service - Insight Docker Service
Loaded: loaded (/usr/lib/systemd/system/docker-insight.service; enabled; vendor preset:
disabled)
Active: active (running) since Fri 2017-04-07 13:09:25 PDT; 36s ago Main PID: 30768
(docker-current)
Memory: 15.2M
CGroup: /system.slice/docker-insight.service
30768 /usr/bin/docker-current start -a insight_<tag-id>
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: Tables_in_rbac
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: buildnode_master
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: permission_master
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: role_master
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: role_permission
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: user_master
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: user_role
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: user_session
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: Starting the apache httpd
Apr 07 13:09:26 i11-tb2-ins-3 docker[30768]: AH00558: httpd: Could not reliably determine
the server's fully qualified domain name, using 2.2.2.6.
Set the 'ServerName' directive gl... this message
Hint: Some lines were ellipsized, use -l to show in full.
```

5. Check if the Insight is up by running the following command:

```
$curl https://br_api:9000 -k (or --insecure)
Your response of curl should show the DOCTYPE HTML:
<!DOCTYPE html>
<!--[if lt IE 7]> <html lang="en" ng-app="myApp" class="no-js lt-ie9 lt-ie8 lt-ie7">
<![endif]-->
<!--[if IE 7]> <html lang="en" ng-app="myApp" class="no-js lt-ie9 lt-ie8">
<![endif]-->
<!--[if IE 8]> <html lang="en" ng-app="myApp" class="no-js lt-ie9"> <![endif]-->
<!--[if gt IE 8]><!--> <html lang="en" ng-app="mercuryInstaller" class="no-js">
<!--<![endif]-->
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Cisco VIM Installer</title>
<meta name="description" content="">
<meta name="viewport" content="width=device-width, initial-scale=1,
maximum-scale=1, user-scalable=0"/>
<link rel="stylesheet"
href="../static/lib/html5-boilerplate/dist/css/normalize.css">
<link rel="stylesheet" href="../static/lib/html5-boilerplate/dist/css/main.css">
<link rel="stylesheet" href="../static/lib/bootstrap/bootstrap.min.css">
<link rel="stylesheet" href="../static/lib/font-awesome/font-awesome.min.css">
<!--<link
href="http://maxcdn.bootstrapcdn.com/font-awesome/4.1.0/css/font-awesome.min.css"
rel="stylesheet">-->
<link rel="stylesheet" href="../static/lib/bootstrap/bootstrap-theme.min.css">
<link rel="stylesheet" href="../static/lib/uigrid/ui-grid.min.css">
<link rel="stylesheet" href="../static/lib/chart/angular-chart.min.css">
<script
src="../static/lib/html5-boilerplate/dist/js/vendor/modernizr-2.8.3.min.js"></script>
<link rel="stylesheet" href="../static/css/app.css">
```

```
<!--new dashboard css starts-->
<link rel="stylesheet" href="../static/css/dashboard.css">
<!--new dashboard css end-->
</head>
<body class="skin-blue sidebar-collapse" ng-controller="DashboardCtrl"
id="ToggleNavbar">
<div class="wrapper" id="wrapper">
<div class="content-wrapper" id="contentclass">
<mi-header></mi-header>
<mi-left-side-navbar></mi-left-side-navbar>
<message-box> </message-box>
<div class=" viewheight" ng-view autoscroll="true"></div>
</div>
<mi-footer></mi-footer>
</div>
<!--new dashboard js starts-->
<script src="../static/lib/bootstrap/jquery.min.js"></script>
<script src="../static/lib/jquery/jquery-ui.js"></script>
<script src="../static/lib/bootstrap/progressbar.js"></script>
<!--new dashboard js ends-->
<script src="../static/lib/chart/Chart.min.js"></script>
<script src="../static/lib/bootstrap/bootstrap.min.js"></script>
<script src="../static/lib/angular/angular.js"></script>
<script src="../static/lib/chart/angular-chart.min.js"></script>
<script src="../static/lib/uigrid/angular-touch.js"></script>
<script src="../static/lib/uigrid/angular-animate.js"></script>
<script src="../static/lib/uigrid/csv.js"></script>
<script src="../static/lib/uigrid/pdfmake.js"></script>
<script src="../static/lib/uigrid/vfs_fonts.js"></script>
<script src="../static/lib/uigrid/ui-grid.js"></script>
<script src="../static/lib/angular/smart-table.min.js"></script>
<script src="../static/lib/angular-route/angular-route.js"></script>
<script src="../static/lib/angular-cookies/angular-cookies.js"></script>
<script src="../static/lib/angular/angular-translate.js"></script>
<script
src="../static/lib/angular/angular-translate-loader-static-files.min.js"></script>
<script
src="../static/lib/angular/angular-translate-storage-cookie.min.js"></script>
<script
src="../static/lib/angular/angular-translate-storage-local.min.js"></script>
<script src="../static/lib/yamltojson/yaml.js"></script>
<script src="../static/lib/yaml/js-yaml.min.js"></script>
<script src="../static/lib/d3/d3min.js"></script>
<script src="../static/utility/utility.js"></script>
<script src="../static/widgets/widgets.js"></script>
<script src="../static/app.js"></script>
<script src="../static/layout/layout.js"></script>
<script src="../static/login/login.js"></script>
<script src="../static/globals/globals.js"></script>
<script src="../static/dashboard/dashboard.js"></script>
<script src="../static/cloudpulse/cloudpulse.js"></script>
<script src="../static/blueprintsetup/physicalsetupwizard/ucsmcommon.js"></script>
<script src="../static/blueprintsetup/physicalsetupwizard/cimccommon.js"></script>
<script src="../static/vmtp/runvmtp.js"></script>
<script src="../static/blueprintsetup/physicalsetupwizard/networking.js"></script>
<script
src="../static/blueprintsetup/physicalsetupwizard/serverandroles.js"></script>
<script src="../static/blueprintsetup/openstacksetupwizard/cephsetup.js"></script>
<script
src="../static/blueprintsetup/openstacksetupwizard/cindersetup.js"></script>
<script
src="../static/blueprintsetup/openstacksetupwizard/glancesetup.js"></script>
<script src="../static/blueprintsetup/openstacksetupwizard/haproxy.js"></script>
<script
src="../static/blueprintsetup/openstacksetupwizard/keystonesetup.js"></script>
<script
src="../static/blueprintsetup/openstacksetupwizard/swiftstack.js"></script>
<script
src="../static/blueprintsetup/openstacksetupwizard/neutronsetup.js"></script>
<script src="../static/blueprintsetup/openstacksetupwizard/vmtpsetup.js"></script>
<script
```

```
src="../static/blueprintsetup/physicalsetupwizard/physicalsetupwizard.js"></script>
<script src="../static/blueprintsetup/servicesSetupWizard/systemlog.js"></script>
<script src="../static/blueprintsetup/servicesSetupWizard/NFVbench.js"></script>
<script
src="../static/blueprintsetup/servicesSetupWizard/servicesSetupWizard.js"></script>
<script
src="../static/blueprintsetup/openstacksetupwizard/openstacksetupwizard.js"></script>
<script src="../static/blueprintsetup/blueprintsetup.js"></script>
<script src="../static/blueprintmanagement/blueprintmanagement.js"></script>
<script src="../static/topology/topology.js"></script>
<script src="../static/monitoring/monitoring.js"></script>
<script src="../static/horizon/horizon.js"></script>
<script src="../static/podmanagement/podmanagement.js"></script>
<script
src="../static/blueprintsetup/openstacksetupwizard/tlssupport.js"></script>
<script src="../static/blueprintsetup/openstacksetupwizard/elksetup.js"></script>
<script src="../static/systemupdate/systemupdate.js"></script>
<script
src="../static/blueprintsetup/physicalsetupwizard/registrysetup.js"></script>
<script src="../static/registertestbed/registertestbed.js"></script>
<script src="../static/registersaas/registersaas.js"></script>
<script src="../static/useradministration/manageusers.js"></script>
<script src="../static/useradministration/rolemanagement.js"></script>
<script src="../static/saasadmindashboard/saasadmindashboard.js"></script>
<script src="../static/saasadmindashboard/buildnodes.js"></script>
<script src="../static/saasadmindashboard/buildnodeusers.js"></script>
<script src="../static/saasadmindashboard/managesaasuser.js"></script>
<script src="../static/saasadminusermanagement/saasadminusermgmt.js"></script>
<script src="../static/blueprintsetup/physicalsetupwizard/nfvisetup.js"></script>
<script src="../static/blueprintsetup/physicalsetupwizard/torswitch.js"></script>
<script src="../static/blueprintsetup/openstacksetupwizard/vtssetup.js"></script>
<script src="../static/rbacutilities/rbacutility.js"></script>
<script src="../static/forgotpassword/forgotpassword.js"></script>
<script src="../static/changepassword/changepassword.js"></script>
<script src="../static/passwordreconfigure/passwordreconfigure.js"></script>
<script
src="../static/openstackconfigreconfigure/openstackconfigreconfigure.js"></script>
<script
src="../static/reconfigureoptionalservices/reconfigureoptionalservices.js"></script>
</body>
```

6. You can check the status of Insight autobackup service that is invoked as a daemon process. Incremental autobackup is taken from the database and */opt/cisco/insight/mgmt_certs* directory if there is any change.

```
systemctl status insight-autobackup
insight-autobackup.service - Insight Autobackup Service
Loaded: loaded (/usr/lib/systemd/system/insight-autobackup.service; enabled; vendor
preset: disabled)
Active: active (running) since Mon 2017-09-04 05:53:22 PDT; 19h ago
Process: 21246 ExecStop=/bin/kill ${MAINPID} (code=exited, status=0/SUCCESS)
Main PID: 21287 (python)
Memory: 9.2M
CGroup: /system.slice/insight-autobackup.service
21287 /usr/bin/python
/var/cisco/insight_backup/insight_backup_2.1.10_2017-08-31_03:02:06/root
/rohan/installer-10416/insight/playbooks/../insight_autobackup.py
Sep 04 05:53:22 F23-insight-4 systemd[1]: Started Insight Autobackup Service.
Sep 04 05:53:22 F23-insight-4 systemd[1]: Starting Insight Autobackup Service...
```

UM Admin Login for Standalone Setup

UM Admin Login for Standalone Setup

For security reasons, the Insight Admin logs into the UI with which UM is bootstrapped. Insight Admin needs to add new users as Pod Admin.

Registration of UM Admin to UM

1. Enter the following address on the browser: https://<br_api>:9000.
2. Enter the **Email ID** and **Password**. The Email ID should be the one specified as UI_ADMIN_EMAIL_ID in **insight_setup_data.yaml** during bootstrap. The Password for UI Admins are generated at:

   ```
   /opt/cisco/insight/secrets.yaml
   ```

   where key is UI_ADMIN_PASSWORD.
3. If LDAP mode is True and LDAP user attribute is set to uid, login with LDAP user id credentials.
4. Click **Login as UI Admin User**. You will be redirected to Insight UI Admin Dashboard.

UM Pod Admin Login for Standalone Setup

UM Pod Admin Login for Standalone Setup

Follow the below steps:

1. Log in as Insight UM.
2. Navigate to **Manage Pod Admin** and click **Add Pod Admin**.
3. Enter a new Email ID in **Add Pod Admin** pop-up.
4. Enter the username of the Pod Admin.
5. Click **Save**. The user registration mail is sent to a newly added Pod Admin with a token.
6. Click the URL with token and if token is valid the Pod Admin is redirected to **Insight-Update Password** page.
7. Enter new password and then confirm the same password.
8. Click **Submit**.

Support of LDAP for UM

Support of LDAP for Unified Management Node

Cisco VIM supports enabling of LDAP for admin access to the Unified Management node. You can add it as a Day 0 or Day 1 activity. Multiple LDAP entries are allowed as only the domain_name and ldap_uri in each entry are mandatory. Ensure that the ldap_uris is secured over ldaps, and the TLS is enabled for the external api (external_lb_vip_tls: True).

To obtain sudo access to the management node, you must manually add the user with root privileges to the wheel group in the corresponding LDAP domain, for example, usermode -aG wheel user1.

To enable this feature, update the setup_data with the following during installation.

```
UM_LDAP_ADMINS:
  - domain_name: <domain_name>            # Required
    ldap_uri: "ldaps://<IP ADDRESS>"      # Required For multiple ldap server, pass comma separated value.
    ldap_search_base: "dc=cisco,dc=com"   # Required
    ldap_schema: rfc2307                  # Optional
    ldap_user_object_class: posixAccount  # optional
    ldap_user_uid_number: uidNumber       # Optional
    ldap_user_gid_number: uidNumber       # Optional
    ldap_group_member: memberUid          # Optional
    ldap_default_bind_dn: "<string>"      # Optional
    ldap_default_authtok: "<string>"      # Optional
    ldap_default_authtok_type: "<string>" # Optional (password|obfuscated_password)
    ldap_group_search_base: "<string>"    # Optional
    ldap_user_search_base: "<string>"     # Optional
    access_provider: "<string>"           # Optional
    simple_allow_groups: "<string>"       # Optional
    ldap_cert_path: "<cert_path>"         # Required
    ldap_id_use_start_tls: <boolean>      # Optional
    ldap_tls_reqcert: "<string>"          # Optional (never|allow|try|demand)
    chpass_provider: "<string>"           # Optional (ldap|krb5|ad|none)
```

Reinstallation of UM Node

Reinstallation of UM Node

Due to unforeseen circumstances, there might be a need to reinstall the UM application with the same image version. To alleviate the need for re-imaging the UM node, follow the steps listed below to uninstall and reinstall the UM application with the image tag used for install in the first place.

1. Copy the *setup_data.yaml* from */root/openstack-configs/* directory to *~/Save/*

   ```
   cd insight-<tag-id>/insight
   ./bootsrap_insight.py -a uninstall -k
   ```

   ⚠ Ensure that you pass *-k* option during uninstallation, to preserve the artifacts.

2. To verify that no docker containers are running, use the command:

   ```
   docker ps -a
   ```

3. To verify that no docker images are present, use the command:

   ```
   docker images
   ```

4. Once the uninstallation is complete, proceed with the installation steps mentioned in the Unified Management.

Verifying Installation

Verifying Installation

Displaying IP Addresses

Displaying IP Addresses

To display the IP addresses for all Cisco NFVI nodes, enter the following command:

```
# cd /root/openstack-configs
[root @nfvi_management_node openstack-configs]# cat
/root/installer/openstack-configs/mercury_servers_info
```

Sample output:

```
Total nodes: 8
Controller nodes: 3
+---------------+---------------+------------+------------+-----------+---------+
| Server        | CIMC          | Management | Provision  | Tenant    | Storage |
+---------------+---------------+------------+------------+-----------+---------+
| c44-control-1 | 172.26.233.54 | 10.21.1.25 | 10.21.1.25 | 10.2.2.22 | None    |
|                     |                      |            |            |           |          |
| c44-control-3 | 172.26.233.56 | 10.21.1.27 | 10.21.1.27 | 10.2.2.24 | None    |
|               |               |            |            |           |         |
| c44-control-2 | 172.26.233.55 | 10.21.1.28 | 10.21.1.28 | 10.2.2.25 | None    |
|               |               |            |            |           |         |
+---------------+---------------+------------+------------+-----------+---------+

Compute nodes: 2
+---------------+---------------+------------+------------+-----------+---------+
|     Server    |       CIMC    | Management | Provision  |   Tenant  | Storage
+---------------+---------------+------------+------------+-----------+---------+
| c44-compute-1 | 172.26.233.57 | 10.21.1.26 | 10.21.1.26 | 10.2.2.23 |   None  |
|               |               |            |            |           |         |
| c44-compute-2 | 172.26.233.58 | 10.21.1.23 | 10.21.1.23 | 10.2.2.21 |   None  |
|               |               |            |            |           |         |
+---------------+---------------+------------+------------+-----------+---------+

Storage nodes: 3

+---------------+---------------+------------+------------+--------+-----------+
|     Server    |      CIMC     | Management | Provision  | Tenant |  Storage  |
+---------------+---------------+------------+------------+--------+-----------+
| c44-storage-3 | 172.26.233.53 | 10.21.1.22 | 10.21.1.22 |  None  | 10.3.3.22 |
|               |               |            |            |        |           |
| c44-storage-2 |172.26.233.52  | 10.21.1.24 | 10.21.1.24 | None   | 10.3.3.23 |
|               |               |            |            |        |           |
| c44-storage-1 |172.26.233.51  | 10.21.1.21 | 10.21.1.21 | None   | 10.3.3.21 |
|               |               |            |            |        |           |
+---------------+---------------+------------+------------+--------+-----------+

[root@c44-top-mgmt openstack-configs]#
```

Cisco VIM Client CLI Availability

Cisco VIM Client CLI Availability

Cisco VIM client CLI is used for managing Cisco NFVI pods. After the completion of Cisco NFVI installation, verify that the Cisco VIM user is running and pointing to the right management node in the installer directory. Cisco NFVI provides a tool to check the REST API server status and directory where it is running.

1. To run the tool, enter the following command:

```
#cd installer-<tagid>/tools
#./restapi.py -a status

Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h ago
REST API launch directory: /root/installer-<tagid
```

2. Confirm if the server status is active and check whether the REST API directory matches with the directory where the installation is launched. The REST API command also provides options to start, tear down, and reset the REST API server password. Run the following REST API command to reset the password.

```
#./restapi.py -h
usage: restapi.py
[-h] --action ACTION [--yes] [--verbose]

REST API setup helper
optional arguments:
-h, --help   show this help message and exit
--action ACTION, -a ACTION
                                        setup - Install and start the REST API server.
                                        teardown - Stop and uninstall the REST API server.
                                    restart - Restart the REST API server.
                                regenerate-password -Regenerate the password for
                                    reset-password - Reset the REST API password with the given password.
                                        status - Check the status of the REST API server

--yes, -y           Skip the dialog. Yes to the action.
--verbose, -v        Perform the action in verbose mode.
```

3. If the REST API server is not running, executing **ciscovim** displays the following error message:

```
# cd installer-<tagid>/
# ciscovim -setupfile ~/Save/<setup_data.yaml> run
```

4. If the installer directory or the REST API state is not correct or pointing to an incorrect REST API directory, go to the installer-*<tagid>/tools* directory and execute the following command:

```
# ./restapi.py -action setup
```

5. Confirm that the REST API server state and directory are correct using the below command:

```
./restapi.py -action status
```

6. If the REST API recovery step was run on an existing pod, run the following command to ensure that the REST API server continues to manage it:

```
# cd installer-<tagid>/
# ciscovim --setupfile <setup_data_file_path> run --perform 7 -y
```


For more information on REST API, see REST API Overview

Displaying Cisco NFVI Logs

Displaying Cisco NFVI Logs

The Cisco NFVI installation logs are generated and available in */var/log/mercury//<install_uuid>/* directory of the management node. The last 20-log directories are tarred and kept in this directory. The logs are archived (tar.gz file) after each run.
The following table lists the Cisco NFVI installation steps and corresponding log files:

Step	Description	Log File
1	INPUT_VALIDATION	mercury_baremetal_install.log
2	MGMTNODE_ORCHESTRATION	mercury_buildorchestration.log
3	VALIDATION	mercury_baremetal_install.log
4	BAREMETAL	mercury_baremetal_install.log
5	COMMONSETUP	mercury_os_install.log
6	CEPH	mercury_ceph_install.log
7	ORCHESTRATION	mercury_os_install.log
8	VMTP	None

Accessing OpenStack API Endpoints

Accessing OpenStack API Endpoints

The Cisco NFVI installer stores the access credentials in */root/installer-<tag-number>/openstack-configs/openrc* of the management node.

The external_lb_vip_address provided in the setup_data.yaml is the IP address where OpenStack APIs are handled.

Example:

```
export OS_AUTH_URL=http://172.26.233.139:5000/v2.0 or
https://172.26.233.139:5000/v2.0 (if TLS is enabled)
export OS_USERNAME=admin
export OS_PASSWORD=xyzabcd
export OS_TENANT_NAME=admin
export OS_REGION_NAME=RegionOne
# For TLS, add
export OS_CACERT=/root/openstack-configs/haproxy-ca.crt
```

The corresponding setup_data.yaml entry:

```
###############################################
# HA Proxy
###############################################
external_lb_vip_address: 172.26.233.139
```

Assessing Cisco NFVI Health

Assessing Cisco NFVI Health with CloudPulse

You can use the OpenStack CloudPulse tool to verify Cisco NFVI health. CloudPulse servers are installed on all Cisco NFVI control nodes, while the CloudPulse users are connected to the management node. Run the following commands to display Cisco NFVI information. For information about CloudPulse, visit the OpenStack CloudPulse
To check the results of periodic CloudPulse runs:

```
# cd /root/openstack-configs
# source openrc
# cloudpulse result
+--------------------------------------+------+-------------------+----------+---------+
| uuid                                 | id   | name              | testtype | state   |
+--------------------------------------+------+-------------------+----------+---------+
| bf7fac70-7e46-4577-b339-b1535b6237e8 | 3788 | glance_endpoint   | periodic | success |
| 1f575ad6-0679-4e5d-bc15-952bade09f19 | 3791 | nova_endpoint     | periodic | success |
| 765083d0-e000-4146-8235-ca106fa89864 | 3794 | neutron_endpoint  | periodic | success |
| c1c8e3ea-29bf-4fa8-91dd-c13a31042114 | 3797 | cinder_endpoint   | periodic | success |
| 04b0cb48-16a3-40d3-aa18-582b8d25e105 | 3800 | keystone_endpoint | periodic | success |
| db42185f-12d9-47ff-b2f9-4337744bf7e5 | 3803 | glance_endpoint   | periodic | success |
| 90aa9e7c-99ea-4410-8516-1c08beb4144e | 3806 | nova_endpoint     | periodic | success |
| d393a959-c727-4b5e-9893-e229efb88893 | 3809 | neutron_endpoint  | periodic | success |
| 50c31b57-d4e6-4cf1-a461-8228fa7a9be1 | 3812 | cinder_endpoint   | periodic | success |
| d1245146-2683-40da-b0e6-dbf56e5f4379 | 3815 | keystone_endpoint | periodic | success |
| ce8b9165-5f26-4610-963c-3ff12062a10a | 3818 | glance_endpoint   | periodic | success |
| 6a727168-8d47-4a1d-8aa0-65b942898214 | 3821 | nova_endpoint     | periodic | success |
| 6fbf48ad-d97f-4a41-be39-e04668a328fd | 3824 | neutron_endpoint  | periodic | success |
```

To run a CloudPulse test on demand:

```
# cd /root/openstack-configs
# source openrc
# cloudpulse run --name <test_name>
# cloudpulse run --all-tests
# cloudpulse run --all-endpoint-tests
# cloudpulse run --all-operator-tests
```

To run a specific CloudPulse test on demand:

```
[root@vms-line2-build installer-3128.2]# cloudpulse run --name neutron_endpoint
+------------+--------------------------------------+
| Property   | Value                                |
+------------+--------------------------------------+
| name       | neutron_endpoint                     |
| created_at | 2016-03-29T02:20:16.840581+00:00     |
| updated_at | None                                 |
| state      | scheduled                            |
| result     | NotYetRun                            |
| testtype   | manual                               |
| id         | 3827                                 |
| uuid       | 5cc39fa8-826c-4a91-9514-6c6de050e503 |
+------------+--------------------------------------+
[root@vms-line2-build installer-3128.2]#
```

To show detailed results from a specific CloudPulse run:

```
[root@vms-line2-build installer-3128.2]# cloudpulse show 5cc39fa8-826c-4a91-9514-6c6de050e503
+------------+--------------------------------------+
| Property         | Value                                                |
+------------+--------------------------------------+
| name                  | neutron_endpoint                                          |
| created_at | 2016-03-29T02:20:16+00:00            |
| updated_at | 2016-03-29T02:20:41+00:00            |
| state                 | success                                                        |
| result         | success                                                 |
| testtype          | manual                                                      |
| id                   | 3827                                    |
| uuid                  | 5cc39fa8-826c-4a91-9514-6c6de050e503 |
```

CloudPulse has two test sets: endpoint_scenario (runs as a cron or manually) and operator test (run manually). Endpoint tests include:

- nova_endpoint
- neutron_endpoint
- keystone_endpoint
- glance_endpoint
- cinder_endpoint

Operator tests include

- ceph_check
- docker_check
- galera_check
- node_check
- rabbitmq_check

The following table lists the operator tests that you can perform with CloudPulse.

Test	Description
Ceph Check	Executes the ceph -f json status command on the Ceph-mon nodes and parses the output. If the result of the output is not HEALTH_OK, the ceph_check reports an error.
Docker Check	Finds out if all Docker containers are in running state on all nodes and reports an error if any containers are in the exited state. The Docker check runs the command, docker ps -aq --filter 'status=exited'.
Galera Check	Executes the command *mysql SHOW STATUS* on the controller nodes and displays the status.
Node Check	Checks if all the nodes in the system are up and online. It also compares the results of the Nova hypervisor list and determines whether all the compute nodes are available.
RabbitMQ Check	Runs the command, *rabbitmqctl cluster_status* on the controller nodes and finds out if the RabbitMQ cluster is in quorum. If nodes are offline, the rabbitmq_check reports a failure.

HA Proxy Dashboard/ELK Stack Logs

Displaying HA Proxy Dashboard and ELK Stack Logs

You can view the HA Proxy dashboard at: http://< *external_lb_vip_address* >:1936 using the following login credentials:

- Username—haproxy
- Password—Value for HAPROXY_PASSWORD in **/root/installer-<tag-number>/openstack-configs/secrets.yaml**

You can use the Kibana dashboard to view logs aggregated by Logstash at: *http://< management_node_IP>:5601* using the following login credentials:

- Username—admin
- Password—Value for ELK_PASSWORD in **/root/installer-<tag-number>/openstack-configs/secrets.yaml**

Testing Pod/Cloud Infrastructure

Testing Cisco NFVI Pod and Cloud Infrastructure

To test the Cisco NFVI pod and cloud infrastructure (host connectivity, basic mraiadb, rabbit, ceph cluster check, and RAID disks), you can use the cloud-sanity tool available on the management node.

For details on the execution of cloud-sanity with Cisco VIM, see Assessing Cisco NFVI Status.

Cisco VIM REST API

Cisco VIM REST API

The following topics explain how to use the Cisco VIM REST API to manage Cisco NFVI.

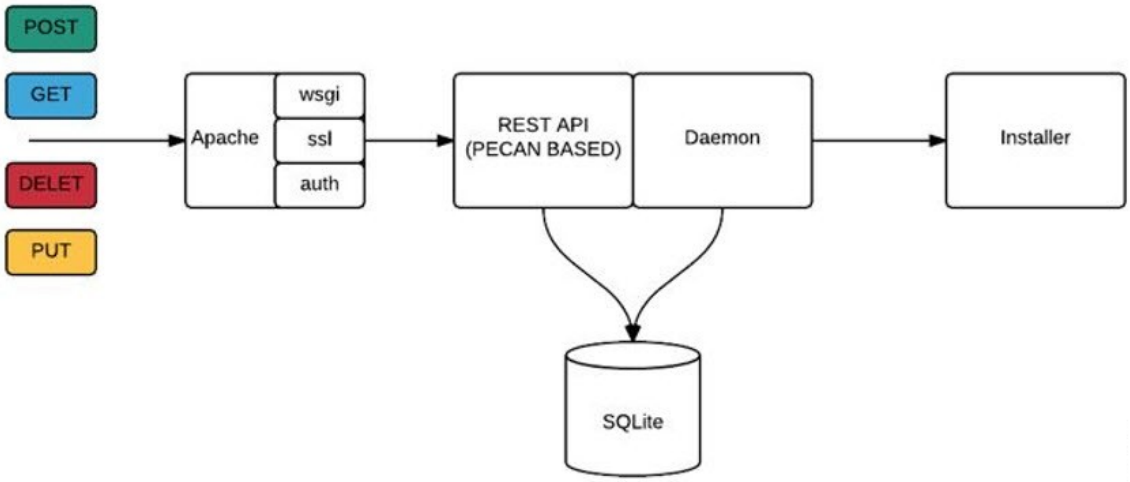
REST API Overview

REST API Overview

A Representational State Transfer (REST) API is used to install, expand, and update Cisco VIM. Actions performed using the REST APIs are:

- Install Cisco VIM on Cisco NFVI pods.
- Add and delete pods to and from Cisco NFVI during installation.
- Update Cisco VIM software.
- Replace controller nodes.
- Perform cloud maintenance operations.
- Run cloud validations using Virtual Machine ThroughPut (VMTP). VMTP is a data path performance measurement tool for OpenStack clouds.

The following figure shows the workflow of Cisco VIM REST API.



The Cisco VIM REST API security is provided by the Secure Sockets Layer (SSL) on the Apache web server. The *mod_wsgi* running on the Rest API server calls the Pecan-based web application. The Pecan REST API server requires a username and password to authorize the REST API server requests.

Apache handles the authorization of the request to access the Pecan web application.

Use the Cisco VIM API to:

- Upload a new setup_data.yaml file to start, stop, or query the state of the installation.
- Manage the cloud.
- Add/remove compute and Ceph nodes, and replace the controller nodes.
- Launch VMTP (L2/L3 data plane testing) and CloudPulse.

The Cisco VIM REST API is enabled by default in the management node, if you are using the supplied Cisco VIM buildnode.iso. You can access API server on the br_api interface on port 8445. The authentication is enabled by default in the web service.

You can access the API end points using the following URL format:

```
https://<Management_node_api_ip>:8445
```

By default, the basic authentication is enabled for the API endpoints in the management node. You can find the authentication credentials in the following file in the management node:

```
/opt/cisco/ui_config.json
```

The following code shows a sample ui_config.json file.

```
{
 "Kibana-Url": "http://10.10.10.10:5601",
 "RestAPI-Url": "https:// 10.10.10.10:8445",
 "RestAPI-Username": "admin",
 "RestAPI-Password": "a96e86ccb28d92ceb1df",
 "RestDB-Password": "e32de2263336446e0f57",
 "BuildNodeIP": "10.10.10.10"
}
```

API Resources

API Resources

Setupdata

REST wrapper for setupdata. Provides methods for listing, creating, modifying, and deleting setupdata.

Retrieving the setupdata

Resource URI

Verb	URI
GET	/v1/setupdata

Example

JSON Request

```
GET /v1/setupdata
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{"setupdatas": [{
"status": "Active",
"name":"GG34",
"uuid": "123"
"meta":{
"user":"root"
},
"jsondata":{
.......
}
}]}
```

Creating setupdata

Resource URI

Verb	URI
POST	/v1/setupdata

Example

JSON Request

```
POST /v1/setupdata
Accept: application/json
{
"name":"GG34",
"uuid": "123"
"meta":{
"user":"root"
},
"jsondata":{
.......
}
}
```

JSON Response

```
201 OK
Content-Type: application/json
{
        "status": "Active",
        "name":"GG34",
        "uuid": "123"
         "meta":{
         "user":"root"
},
"jsondata":{
.......
 }
}

400 Bad Request
Content-Type: application/json
{
       "debuginfo": null
       "faultcode":"Client"
       "faultstring": "Error"
}
409 CONFLICT
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Error"
}
```

Retrieving a single setupdata

Resource URI

Verb	URI
GET	/v1/setupdata/(id)

Property:
id—The ID of the setupdata that you want to retrieve.

Example

JSON Request

```
GET /v1/setupdata/123
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "status": "Active",
        "name":"GG34",
        "uuid": "123"
        "meta":{
        "user":"root"
},
"jsondata":{
.......
        }
}
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
"faultcode": "Client"
"faultstring": "Setupdata could not be found."
}
```

Updating a setupdata

Resource URI

Verb	URI
PUT	/v1/setupdata/(id)

Property:
id—The ID of the setupdata that you want to update. Example

JSON Request

```
PUT /v1/setupdata/123 Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
 "status": "Active",
 "name":"GG34",
 "uuid": "123"
 "meta":{
 "user":"root"
  },
 "jsondata":{
 .......
 }
}
404 NOT FOUND
Content-Type: application/json
{
 "debuginfo": null
 "faultcode": "Client"
 "faultstring": "Setupdata could not be found."
}
```

Deleting a setupdata

Resource URI

Verb	URI
DELETE	/v1/setupdata/(id)

Property:
id—The ID of the setupdata that you want to delete. Example

JSON Request

```
DELETE /v1/setupdata/123 Accept: application/json
```

JSON Response

```
204 NO CONTENT Returned on success
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Setupdata could not be found."
}
400 BAD REQUEST
Content-Type: application/json
{
"debuginfo": null "faultcode": "Client"
"faultstring": "Setupdata cannot be deleted when it is being used by an installation"
}
```

Install resource

REST wrapper for install. Provides methods for starting, stopping, and viewing the status of the installation process.

Return a list of installation

Resource URI

Verb	URI
GET	/v1/install

Example

JSON Request

```
GET /v1/install
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
  {"installs": [{
        "ceph": "Skipped",
        "uuid": "123",
        "setupdata": "345",
        "vmtpresult": "{
        "status": "PASS",
        "EXT_NET": []
  }",
        "baremetal": "Success",
        "orchestration": "Success",
        "validationstatus": "{
        "status": "PASS",
        "Software_Validation": [],
        "Hardware_Validation": []
  }",
    "currentstatus": "Completed",
        "validation": "Success",
        "hostsetup": "Success",
        "vmtp": "Skipped"
  }]
}
```

Create an installation

Resource URI

Verb	URI
POST	/v1/install

Example

JSON Request

```
GET /v1/install
Accept: application/js
{
        "setupdata": "123",
        "stages": [
        "validation",
        "bootstrap",
        "runtimevalidation",
        "baremetal",
        "orchestration",
        "hostsetup",
        "ceph",
        "vmtp"
        ]
}
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
        "ceph": "Skipped",
        "uuid": "123",
        "setupdata": "345",
        "vmtpresult": "{
        "status": "PASS",
        "EXT_NET": []
}",
        "baremetal": "Success",
        "orchestration": "Success",
        "validationstatus": "{
        "status": "PASS",
        "Software_Validation": [],
        "Hardware_Validation": []
}",
        "currentstatus": "Completed",
        "validation": "Success",
        "hostsetup": "Success",
        "vmtp": "Skipped"
}
409 CONFLICT
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Install already exists"
}
```

Retrieve the installation

Resource URI

Verb	URI
GET	/v1/install/{id}

Property:
id—The ID of the installation that you want to retrieve. Example

JSON Request

```
GET /v1/install/345
Accept: application/js
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "ceph": "Skipped",
        "uuid": "123",
        "setupdata": "345",
        "vmtpresult": "{
        "status": "PASS",
        "EXT_NET": []
}",
        "baremetal": "Success",
        "orchestration": "Success",
        "validationstatus": "{
        "status": "PASS",
        "Software_Validation": [],
        "Hardware_Validation": []
}",
        "currentstatus": "Completed",
        "validation": "Success",
        "hostsetup": "Success",
        "vmtp": "Skipped"
}
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Install doesn't exists"
}
```

Stop the installation

Resource URI

Verb	URI
DELETE	/v1/install/{id}

Property:
id—The ID of the installation that you want to stop. Example

JSON Request

```
DELETE /v1/install/345
Accept: application/js
```

JSON Response

```
204 NO CONTENT
 Content-Type: application/json

404 NOT FOUND
 Content-Type: application/json
 {
         "debuginfo": null "faultcode": "Client"
         "faultstring": "Install doesn't exists"
 }
```

Nodes

Getting a list of nodes
Resource URI

Verb	URI

GET	/v1/nodes

Example

JSON Request

```
Get /v1/nodes
Accept: application/js
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "nodes": [
        [
                "status": "Active",
                "uuid": "456",
                "setupdata": "123",
                "node_data": "{
                "rack_info": {
                "rack_id": "RackA"
                },
                "cimc_info": {
                  "cimc_ip": "10.10.10.10"
                },
        "management_ip": "7.7.7.10"
          }",
        "updated_at": null,
        "mtype": "compute",
        "install": "345",
        "install_logs": "logurl",
        "created_at":"2016-0710T06:17:03.761152",
        "name": " compute-1"
        }
   ]
}
```

Add New Nodes

The nodes are in compute or block_storage type. Before adding the nodes to the system, the name of the nodes and other necessary information like cimc_ip and rackid must be updated in the setupdata object. If the setupdata object is not updated, the post call does not allow you to add the node.
Resource URI

Verb	**URI**
POST	/v1/nodes

Example

JSON Request

```
POST /v1/nodes
Accept: application/js
 {
 "name" : "compute-5"
 }
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
        "status": "ToAdd",
        "uuid": "456",
        "setupdata": "123",
        "node_data": "{
        "rack_info": {
        "rack_id": "RackA"
        },
        "cimc_info": {
        "cimc_ip": "10.10.10.10"
        },
        "management_ip": "7.7.7.10"
        }",
        "updated_at": null,
        "mtype": "compute",
        "install": "345",
        "install_logs": "logurl",
        "created_at":"2016-0710T06:17:03.761152",
        "name": " compute-1"
}
```

Retrieve information about a particular node

Resource URI

Verb	URI
GET	/v1/nodes{id}

Property:
id—The ID of the node that you want to retrieve. Example

JSON Request

```
POST /v1/nodes
Accept: application/js
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "status": "Active",
        "uuid": "456",
        "setupdata": "123",
        "node_data": "{
        "rack_info": {
        "rack_id": "RackA"
        },
        "cimc_info": {
        "cimc_ip": "10.10.10.10"
        },
        "management_ip": "7.7.7.10"
        }",
        "updated_at": null,
        "mtype": "compute",
        "install": "345",
        "install_logs": "logurl",
        "created_at":"2016-0710T06:17:03.761152",
        "name": " compute-1"
}
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Node doesn't exists"
}
```

Remove a Node

The node to be deleted must be removed from the setupdata object. Once the setupdata object is updated, you can safely delete the node. The node object cannot be deleted until it calls the remove node backend and succeeds.
Resource URI

Verb	URI
DELETE	/v1/nodes{id}

Property:
id—The ID of the node that you want to remove. Example

JSON Request

```
DELETE /v1/nodes/456
Accept: application/js
```

JSON Response

```
204 ACCEPTED
Content-Type: application/json
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Node doesn't exists"
}
```

To clear the database and delete the entries in the nodes, the delete API is called with special parameters that are passed along with the delete request. The JSON parameters are in the following format.

JSON Request

```
DELETE /v1/nodes/456
Accept: application/js
 {
 "clear_db_entry":"True"\
 }
```

JSON Response

```
204 ACCEPTED
 Content-Type: application/json

 404 NOT FOUND
 Content-Type: application/json
 {
         "debuginfo": null
         "faultcode": "Client"
         "faultstring": "Node doesn't exists"
 }
```


This is done only if the node is deleted from the REST API database. The failure reason of the node must be rectified manually apart from the API. True is a string and not a boolean in the preceding line.

Replace a controller

Resource URI

Verb	URI
PUT	/v1/nodes{id}

Property:
id—The ID of the controller that you want to replace. Example

JSON Request

```
PUT /v1/nodes/456 Accept: application/js
```

JSON Response

```
200 OK
 Content-Type: application/json
 404 NOT FOUND
 Content-Type: application/json
 {
         "debuginfo": null
         "faultcode": "Client"
          "faultstring": "Node doesn't exists"
 }
```

Offline validation

REST wrapper does the offline validation of setupdata. Rest Wrapper does only the Software Validation of the input setupdata.

Create an offline validation operation

Resource URI

Verb	URI
POST	/v1/offlinevalidation

Example

JSON Request

```
POST /v1/offlinevalidation
Accept: application/json
 {
 "jsondata": "."
 }
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
"status": "NotValidated",
"uuid": "bb42e4ba-c8b7-4a5c-98b3-1f384aae2b69",
"created_at": "2016-02-03T02:05:28.384274",
"updated_at": "2016-02-03T02:05:51.880785",
"jsondata": "{}",
"validationstatus": {
"status": "PASS",
"Software_Validation": [],
"Hardware_Validation": []
}
}
```

Retrieve the results of offline validation

Resource URI

Verb	URI
GET	/v1/offlinevalidation

Property:
id—The ID of the node you want to retrieve. Example

JSON Request

```
GET /v1/offlinevalidation/789
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
"status": " ValidationSuccess",
"uuid": "bb42e4ba-c8b7-4a5c-98b3-1f384aae2b69",
"created_at": "2016-02-03T02:05:28.384274",
"updated_at": "2016-02-03T02:05:51.880785",
"jsondata": "{}",
"validationstatus": {
"status": "PASS",
"Software_Validation": [],
"Hardware_Validation": []
}
}
```

Update

Start an Update Process
Resource URI

Verb	URI

POST	/v1/update

Parameters:

- fileupload - "tar file to upload"
- filename - "Filename being uploaded"

Example

JSON Request

```
curl -sS -X POST --form
"fileupload=@Test/installer.good.tgz" --form
"filename=installer.good.tgz"
https://10.10.10.8445/v1/update
```

⚠ This curl request is done as a form request.

JSON Response

```
200 OK
 Content-Type: application/json
 {
        "update_logs": "logurl",
         "update_status": "UpdateSuccess",
        "update_filename": "installer-4579.tgz",
        "created_at": "2016-07-10T18:33:52.698656",
        "updated_at": "2016-07-10T18:54:56.885083"
 }
 409 CONFLICT
 Content-Type: application/json
 {
 "debuginfo": null "faultcode": "Client"
 "faultstring": "Uploaded file is not in tar format"
 }
```

Roll back an update

Resource URI

Verb	URI
PUT	/v1/update

Example

JSON Request

```
PUT /v1/update
 Accept: application/json
 {
 "action":"rollback"
 }
```

JSON Response

```
200 OK
 Content-Type: application/json
 {

 "update_logs": "logurl", "update_status": "ToRollback", "update_filename": "installer-4579.tgz",
 "created_at": "2016-07-10T18:33:52.698656", "updated_at": "2016-07-10T18:54:56.885083"
 }
```

Commit an update

Resource URI

Verb	URI
PUT	/v1/update

Example

JSON Request

```
PUT /v1/update
 Accept: application/json
 {
 "action":"commit"
 }
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 "update_logs": "logurl", "update_status": "ToCommit", "update_filename": "installer-4579.tgz",
 "created_at": "2016-07-10T18:33:52.698656", "updated_at": "2016-07-10T18:54:56.885083"
 }
```

Retrieve the details of an update

Resource URI

Verb	URI
GET	/v1/update

Example

JSON Request

```
GET /v1/update
 Accept: application/json
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
         "update_logs": "logurl",
        "update_status": "UpdateSuccess",
        "update_filename": "installer-4579.tgz",
    "created_at": "2016-07-10T18:33:52.698656",
        "updated_at": "2016-07-10T18:54:56.885083"
 }
```

Secrets

Retrieve the list of secrets that are associated with the OpenStack Setup
You can retrieve the set of secret password that are associated with the OpenStack setup using the preceding api. This gives the list of secrets for each service in OpenStack.
Resource URI

Verb	URI
GET	/v1/secrets

Example

JSON Request

```
GET /v1/secrets
 Accept: application/json
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 "HEAT_KEYSTONE_PASSWORD": "xxxx", "CINDER_KEYSTONE_PASSWORD": "xxxxx",
 ....
 ....
 "RABBITMQ_PASSWORD": "xxxxx"
 }
```

OpenStack Configs

Retrieve the list of OpenStack configs associated with the OpenStack Setup
You can retrieve the set of OpenStack configs associated with the OpenStack setup using the preceding api. This gives the current settings of different configurations such as verbose logging and debug logging for different OpenStack services.

Verb	URI
GET	/v1/secrets

JSON Request

```
GET /v1/openstack_config
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
"CINDER_DEBUG_LOGGING": false,
"KEYSTONE_DEBUG_LOGGING": false,
....
....
"NOVA_VERBOSE_LOGGING": true
}
```

Version

Retrieve the version of the Cisco Virtualized Infrastructure Manager. Resource URI

Verb	URI
GET	/v1/version

Example

JSON Request

GET /v1/version
Accept: application/json

JSON Response

200 OK
Content-Type: application/json
{"version": "1.9.1"}

Health of the Management Node

Retrieve the health of the Management node
This API is used to retrieve the health of the management node. It checks various parameters such as partitions, space and so on.
Resource URI

Verb	URI
GET	/v1/health

Example

JSON Request

GET /v1/health
Accept: application/json

JSON Response

200 OK
Content-Type: application/json
{
"status": "PASS", "pod_status": { "color": "BLUE",
"version": "<VERSION_NO.>"
},
"insight_version": "<VERSION_NO.>"
}
Color signifies the health of the pod for Insight:

- Grey signifies that no installation is kicked off on the pod.
- Green signifies that everything is in Good state and cloud installation is active.
- Blue signifies that some operation is running on the pod.
- Red signifies that the pod is in critical state and you might need TAC support to recover the pod.
- Amber indicates a warning if a pod management (Add/Remove/Replace) operation failed.

Hardware Information

REST wrapper to do hardware information of setupdata. This returns the hardware information of all hardware available in the setupdata.

Create a HWinfo operation

Resource URI

Verb	URI
GET	/v1/hwinfo

Example

JSON Request

POST /v1/hwinfo
Accept: application/json
{
"setupdata":"c94d7973-2fcc-4cd1-832d-453d66e6b3bf"
}

JSON Response

201 CREATED
Content-Type: application/json
{
"status": "hwinfoscheduled",
"uuid": "928216dd-9828-407b-9739-8a7162bd0676",
"setupdata": "c94d7973-2fcc-4cd1-832d-453d66e6b3bf", "created_at": "2017-03-19T13:41:25.488524",
"updated_at": null, "hwinforesult": ""
}

Retrieve the results of Hwinfo Operation

Resource URI

Verb	URI
GET	/v1/hwinfo/{id}

Property:
id—The ID of the node you want to query. Example

JSON Request

GET /v1/hwinfo/789 Accept: application/json

JSON Response

200 OK
Content-Type: application/json
{
"status": "hwinfosuccess",
"uuid": "928216dd-9828-407b-9739-8a7162bd0676",
"setupdata": "c94d7973-2fcc-4cd1-832d-453d66e6b3bf", "created_at": "2017-03-19T13:41:25.488524", "updated_at": "2017-03-19T13:42:05.087491",
"hwinforesult": "{\"172.29.172.73\": {\"firmware\": ……..
……
……..
}

Release mapping Information

This api is used to see the list of Features included and list of options which can be reconfigured in the Openstack Setup.

Retrieve the release mapping information

Resource URI

Verb	URI
GET	/v1/releasemapping

JSON Request

GET /v1/releasemapping Accept: application/json

JSON Response

200 OK
Content-Type: application/json [
{
"SWIFTSTACK": {
"feature_status": true,
],
"desc": "swift stack feature"
}
},.....
.....
}

POST Install operations

The following are the post install operations that can be performed, after the successful installation of OpenStack. It uses a common api. Following is an Example:

1. reconfigure
2. reconfigure -regenerate passwords
3. reconfigure -setpasswords,setopenstack_configs
4. reconfigure -alertmanager_config, -alerting_rules_config
5. check-fernet-keys
6. resync-fernet-keys
7. rotate-fernet-keys

Create a post install operation

Resource URI

Verb	URI
POST	/v1/misc

Examples:

JSON Request
POST /v1/misc
Accept: application/json
{"action": {"reconfigure": true}}

JSON Response

201 CREATED
Content-Type: application/json
{
"uuid": "7e30a671-bacf-4e3b-9a8f-5a1fd8a46733", "created_at": "2017-03-19T14:03:39.723914",
"updated_at": null,
"operation_status": "OperationScheduled", "operation_logs": "",
"operation_name": "{"reconfigure": true}"
}

JSON Request

POST /v1/misc
Accept: application/json
{"action": {"reconfigure": true, "alertmanager_config": <json_config>}}

JSON Response

201 CREATED
Content-Type: application/json
{
"uuid": "68b67265-8f09-480e-8608-b8aff77e0ec7", "created_at": "2019-01-09T16:42:11.484604+00:00",
"updated_at": null,

"operation_status": "OperationScheduled", "operation_logs": "",
"operation_name": "{"alertmanager_config": <json_config>, "reconfigure": true}"
}

Retrieve a status of the post install operation

Resource URI

Verb	URI
GET	/v1/misc

Example

JSON Request

GET /v1/misc
Accept: application/json

JSON Response

201 CREATED
Content-Type: application/json
{
"uuid": "7e30a671-bacf-4e3b-9a8f-5a1fd8a46733", "created_at": "2017-03-19T14:03:39.723914", "updated_at": "2017-03-19T14:03:42.181180",
"operation_status": "OperationRunning", "operation_logs": "xxxxxxxxxxxxxxxx", "operation_name": "{\"reconfigure\": true}"
}
In VIM Rest APIs exist to support NFVBench, query hardware information and to get a list of optional and mandatory features that the pod supports. Following are the API details:

NFVBench Network Performance Testing Create NFVBench Run

Starts the network performance test with provided configuration. REST API To Create Fixed Rate Test

Verb	URI
Post	v1/nfvbench/ create_ndr_pdr_test

Example

JSON Request

POST Request URL
/v1/nfvbench/create_fixed_rate_test JSON Request:
{"nfvbench_request":
{
"duration_sec": 20, "traffic_profile": [
{
"name": "custom", "l2frame_size": [

"64",
"IMIX", "1518"
]
}
],
"traffic": { "bidirectional": true, "profile": "custom"
},
"flow_count": 1000
}
}

JSON Response

201 CREATED
Content-Type: application/json
{
"status": "not_run", "nfvbench_request":
'{
"duration_sec": 20, "traffic_profile": [
{
"name": "custom", "l2frame_size": [
"64",
"IMIX", "1518"
]
}
],
"traffic": { "bidirectional": true, "profile": "custom"
},
"flow_count": 1000
}',
"created_at": "2017-08-16T06:14:54.219106",
"updated_at": null, "nfvbench_result": "", "test_name": "Fixed_Rate_Test"
}

Status Polling

Polling of NFVbench run status which is one of nfvbench_running, nfvbench_failed, nfvbench_completed.

Resource URI

Verb	URI
GET	v1/nfvbench/<test_name>

REST API To Get Fixed Rate Test Result
GET Request URL
/v1/upgrade/get_fixed_rate_test_result JSON Response:
Check If NFVbench Test is running
200 OK
Content-Type: application/json

{
"status": "nfvbench_running",
"nfvbench_request": '{"traffic": {"bidirectional": true, "profile": "custom"},
"rate": "1000000pps",
"traffic_profile": [{"l2frame_size": ["1518"], "name": "custom"}], "duration_sec": 60, "flow_count": 1000}',
"nfvbench_result": ""
"created_at": "2017-05-30T21:40:40.394274", "updated_at": "2017-05-30T21:40:41.367279",
}

Check If NFVbench Test is completed
200 OK
Content-Type: application/json

{
"status": "nfvbench_completed",
"nfvbench_request": '{"traffic": {"bidirectional": true, "profile": "custom"}, rate": "1000000pps",
"traffic_profile": [{"l2frame_size": ["1518"], "name": "custom"}], "duration_sec": 60, "flow_count": 1000}',
"nfvbench_result": '{"status": "PROCESSED", "message": {"date": "2017-08-15 23:15:04", "nfvbench_version": "0.9.3.dev2", ...}
"created_at": "2017-05-30T21:40:40.394274", "updated_at": "2017-05-30T22:29:56.970779",
}

REST API to create NDR/PDR Test
POST Request URL
/v1/nfvbench/create_ndr_pdr_test
Accept: application/json

{"nfvbench_request":
{
"duration_sec": 20, "traffic_profile": [
{
"name": "custom", "l2frame_size": [
"64",
"IMIX", "1518"
]
}
],
"traffic": { "bidirectional": true, "profile": "custom"
},
"flow_count": 1000
}
}

JSON Response
201 CREATED
Content-Type: application/json

{
"status": "not_run", "nfvbench_request":
'{
"duration_sec": 20, "traffic_profile": [
{
"name": "custom", "l2frame_size": [

"64",
"IMIX", "1518"
]
}
],
"traffic": { "bidirectional": true, "profile": "custom"
},
"flow_count": 1000
}'
"created_at": "2017-08-16T07:18:41.652891",
"updated_at": null, "nfvbench_result": "", "test_name": "NDR_PDR_Test"
}

REST API To Get NDR/PDR Test Results
GET Request URL
/v1/ nfvbench/get_ndr_pdr_test_result
JSON Response:
If NFVbench NDR/PDR test is running
200 OK

Content-Type: application/json
{
"status": "nfvbench_running",
"nfvbench_request": '{"duration_sec": 20,
"traffic": {"bidirectional": true, "profile": "custom"},
"traffic_profile": [{"l2frame_size": ["64", "IMIX", "1518"], "name": "custom"}], "flow_count": 1000}',
"nfvbench_result": ""
"created_at": "2017-08-16T07:18:41.652891", "updated_at": "2017-09-30T22:29:56.970779",
}
If NFVbench NDR/PDR test is completed
200 OK
Content-Type: application/json
{
"status": "nfvbench_completed", "nfvbench_request": '{"duration_sec": 20,
"traffic": {"bidirectional": true, "profile": "custom"},
"traffic_profile": [{"l2frame_size": ["64", "IMIX", "1518"], "name": "custom"}], "flow_count": 1000}',
"nfvbench_result": '{"status": "PROCESSED",...}' "created_at": "2017-08-16T07:18:41.652891", "updated_at": "2017-09-30T22:29:56.970779",
}

REST API to Get Node Hardware Information

Rest API helps you to get the hardware information of all the nodes in the POD through CIMC/UCSM.

- Total Memory
- Firmware Info (Model, Serial Number)
- CIMC IP

GET Request URL
/v1/hwinfo Output Response
{
"hwinforesult": "{"control-server-2": {"memory": {"total_memory": "131072"}, "firmware": {"serial_number": "FCH1905V16Q", "fw_model": "UCSC-C220-M4S"}, "cimc_ip": "172.31.230.100", "storage": {"num_storage": 4}, "cisco_vic_adapters": {"product_name": "UCS VIC 1225"},
"cpu": {"number_of_cores": "24"}, "power_supply": {"power_state": "on"}}
…
}

REST API to Get Mandatory Features Mapping

POST Request URL
/v1/releasemapping/mandatory_features_mapping
JSON Response:


```
{
"mandatory": { "networkType": {
"C": {
"feature_status": true,
"values": [{"name": "VXLAN/Linux Bridge", "value": "VXLAN/Linux Bridge"},],
"insight_label": "Tenant Network", "desc": "Tenant Network"
},
"B": {
"feature_status": true,
"values": [{"name": "VXLAN/Linux Bridge", "value": "VXLAN/Linux Bridge"},],
"insight_label": "Tenant Network", "desc": "Tenant Network"
}
},
"cephMode": {
"all": {
"feature_status": true,
"values": [{"name": "Central", "value": "Central"},], "insight_label": "Ceph Mode",
"desc": "Ceph Mode"
}
},
"podType": {
"C": {
"feature_status": true,
"values": [{"name": "Fullon", "value": "fullon"},], "insight_label": "POD Type",
"desc": "POD Type"
}, "B": {
"feature_status": true,
"values": [{"name": "Fullon", "value": "fullon"},], "insight_label": "POD Type",
"desc": "POD Type"
}
},
"installMode": { "all": {
"feature_status": true,
"values": [{"name": "Connected", "value": "connected"}, ], "insight_label": "Install Mode",
"desc": "Install Mode"
}

}
},
"platformType": [{"name": "B-series", "value": "B"}, {"name": "C-series", "value": "C"}],
"postinstalllinks": {
"view_cloudpulse": {"alwayson": true, "feature_status": true, "platformtype": "all", "insight_label": "Run VMTP", "desc": "Cloudpluse"},
"password_reconfigure": {"alwayson": true, "feature_status": true, "platformtype": "all", "insight_label": "Reconfigure Passwords", "desc": "Reconfigure
Passwords"}
}
}
```


REST API to Get Optional Features Mapping

POST Request URL
/v1/releasemapping/optional_features_mapping
JSON Response: [


```
{
"SWIFTSTACK": {
"feature_status": true, "insight_label": "Swiftstack", "repeated_redeployment": true,
"reconfigurable": ["cluster_api_endpoint", "reseller_prefix", "admin_password",
"protocol"],
"desc": "swift stack feature"
}
},
{
"heat": {
"feature_status": true, "insight_label": "Heat", "repeated_redeployment": false, "reconfigurable": ["all"], "desc": "Openstack HEAT service"
}
},
..... other features
]
```


Cloud sanity information

REST wrapper to run cloud-sanity test suites. The cloud-sanity extension to the VIM REST API enables support for managing cloud-sanity test actions

Create a cloud-sanity test

Verb	URI
Post	/v1/cloud-sanity/create

Example

JSON Request

POST /v1/cloudsanity/create Accept: application/json
'{"cloudsanity_request": {"command": "create",
"action": "test", "test_name": "cephmon", "uuid": ""}}'
test_name can be all,management,control,compute,cephmon,cephosd

JSON Response

201 Created
{
'cloudsanity_request': "{u'action': u'test', u'command': u'create', u'uuid': '5dff1662-3d33-4901-808d-479927c01dde',
u'test_name': u'cephmon'}", 'cloudsanity_result': '',
'created_at': '2018-01-26T20:32:20.436445',
'status': 'not_run', 'test_name': 'cephmon', 'updated_at': ''
}

List cloud-sanity test results

Verb	URI
GET	/v1/cloud-sanity

JSON Request
GET /v1/cloudsanity

JSON Response

200 OK
{ '0b91746f-90b4-4355-a748-727c2e5c59c5': { 'action': 'test',
'created_at': '2018-01-25 12:08:22',
'status': 'cloudsanity_completed', 'test_name': 'management',
'uuid': '0b91746f-90b4-4355-a748-727c2e5c59c5'},
'5695cb31-39e4-4be2-9dee-09e7daffc2e7': { 'action': 'test',
'created_at': '2018-01-25 12:03:06',
'status': 'cloudsanity_completed', 'test_name': 'compute',
'uuid': '5695cb31-39e4-4be2-9dee-09e7daffc2e7'},
'5dff1662-3d33-4901-808d-479927c01dde': { 'action': 'test',
'created_at': '2018-01-26 20:32:20',
'status': 'cloudsanity_completed', 'test_name': 'cephmon',
'uuid': '5dff1662-3d33-4901-808d-479927c01dde'},
'7946255d-df58-4432-b729-20cf16eb5ba5': { 'action': 'test',
'created_at': '2018-01-25 12:05:56',
'status': 'cloudsanity_completed', 'test_name': 'cephosd',
'uuid': '7946255d-df58-4432-b729-20cf16eb5ba5'},
'797d79ba-9ee0-4e11-9d9e-47791dd05e07': { 'action': 'test',
'created_at': '2018-01-25 12:05:11',
'status': 'cloudsanity_completed', 'test_name': 'cephmon',
'uuid': '797d79ba-9ee0-4e11-9d9e-47791dd05e07'},
'962e2c8e-c7b0-4e24-87c1-528cad84002c': { 'action': 'test',
'created_at': '2018-01-26 18:52:31',
'status': 'cloudsanity_completed', 'test_name': 'control',
'uuid': '962e2c8e-c7b0-4e24-87c1-528cad84002c'}, 'd0111530-ee3b-45df-994c-a0917fd18e11': { 'action': 'test',

'created_at': '2018-01-26 18:46:23',
'status': 'cloudsanity_completed', 'test_name': 'control',
'uuid': 'd0111530-ee3b-45df-994c-a0917fd18e11'}}

List specific cloud-sanity test results

Verb	URI
GET	/v1/cloud-sanity/list/?test_name={all, management, control,compute,cephmon,cephosd}

JSON Request
GET /v1/cloudsanity/list/?test_name=cephmon Accept: application/json

JSON Response

200 OK
{ '5dff1662-3d33-4901-808d-479927c01dde': { 'action': 'test',
'created_at': '2018-01-26 20:32:20',
'status': 'cloudsanity_completed', 'test_name': 'cephmon',
'uuid': '5dff1662-3d33-4901-808d-479927c01dde'},
'797d79ba-9ee0-4e11-9d9e-47791dd05e07': { 'action': 'test',
'created_at': '2018-01-25 12:05:11',
'status': 'cloudsanity_completed', 'test_name': 'cephmon',
'uuid': '797d79ba-9ee0-4e11-9d9e-47791dd05e07'}}

Show cloud-sanity test results

Verb	URI
GET	/v1/cloud-sanity/show/?uuid=<uuid>

JSON Request
GET /v1/cloudsanity/show/?uuid=d0111530-ee3b-45df-994c-a0917fd18e11

JSON Response

200 OK
{ 'action': 'test', 'cloudsanity_request':
"{u'action': u'test', u'command': u'create',
u'uuid': 'd0111530-ee3b-45df-994c-a0917fd18e11', u'test_name': u'control'}",
'cloudsanity_result': '{"status": "PROCESSED",
"message": {"status": "Pass",
"message": "[PASSED] Cloud Sanity Control Checks Passed", "results": {"control": {"ping_all_controller_nodes": "PASSED",
"check_rabbitmq_is_running": "PASSED", "check_rabbitmq_cluster_status": "PASSED", "check_nova_service_list": "PASSED", "ping_internal_vip":
"PASSED",

'created_at': '2018-01-26 18:46:23',
'status': 'cloudsanity_completed', 'test_name': 'control', 'updated_at': '2018-01-26 18:47:58',
"disk_maintenance_raid_health": "PASSED", "check_mariadb_cluster_size": "PASSED", "disk_maintenance_vd_health": "PASSED"}}}}',
'uuid': 'd0111530-ee3b-45df-994c-a0917fd18e11'}

Delete cloud-sanity test results

Verb	URI
DELETE	/v1/cloud-sanity/delete/?uuid=<uuid>

JSON Request
GET /v1/cloudsanity/delete/?uuid=444aa4c8-d2ba-4379-b035-0f47c686d1c4

JSON Response

200 OK
{
"status": "deleted",
"message": "UUID 444aa4c8-d2ba-4379-b035-0f47c686d1c4 deleted from database", "uuid": "444aa4c8-d2ba-4379-b035-0f47c686d1c4",
"error": "None"
}

Disk Maintenance information

REST wrapper to query information about RAID disks on Pod nodes. This returns the RAID disk information of all or a selection of RAID disks available in the Pod.
The disk management extension to the VIM REST API enables support for Disk Management actions

Create a Check disk operation

Resource URI

Verb	URI
POST	/v1/diskmgmt/check_disks

Example

JSON Request

POST /v1/diskmgmt/check_disks Accept: application/json '{"diskmgmt_request": {"command": "create",
"action": "check-disks",
"role": "control",
"locator": "False", "json_display": "False", "servers": "", "uuid": ""}}'

JSON Response

201 Created
Content-Type: application/json
{
'action': 'check-disks',
'created_at': '2018-03-08T02:03:18.170849+00:00',
'diskmgmt_request': "{u'uuid': '0729bdea-cc19-440f-8339-ab21e76be84b',

u'json_display': u'False',
u'servers': u'',
u'locator': u'False', u'role': u'control', u'action': u'check-disks', u'command': u'create'}",
'diskmgmt_result': '', 'status': 'not_run', 'updated_at': 'None'
}

Create a replace disk operation

Verb	URI
POST	/v1/diskmgmt/replace_disks

Example

JSON Request

POST /v1/diskmgmt/replace_disks Accept: application/json
'{"diskmgmt_request": {"command": "create",
"action": "replace-disks", "role": "control",
"locator": "False", "json_display": "False", "servers": "", "uuid": ""}}'

JSON Response

201 Created
Content-Type: application/json
{
"status": "not_run",
"diskmgmt_request": "{u'uuid': 'cb353f41-6d25-4190-9386-330e971603c9', u'json_display': u'False',
u'servers': u'', u'locator': u'False', u'role': u'control',
u'action': u'replace-disks', u'command': u'create'}",
"created_at": "2018-03-09T12:43:41.289531+00:00",
"updated_at": "", "diskmgmt_result": "", "action": "replace-disks"}

List check disk operation

Verb	URI
GET	/v1/diskmgmt/list/?action={check-disks,replace-disks \&role={all,management,control,compute}

Example

JSON Request

GET /v1/diskmgmt/list/?action=check-disks\&role=all

JSON Response

200 OK
Content-Type: application/json
{
'0be7a55a-37fe-43a1-a975-cbf93ac78893': {'action': 'check-disks',
'created_at': '2018-03-05 14:45:45+00:00',
'role': 'compute',
'status': 'diskmgmt_completed', 'uuid':
'0be7a55a-37fe-43a1-a975-cbf93ac78893'},
'861d4d73-ffee-40bf-9348-13afc697ee3d': {'action': 'check-disks',
'created_at': '2018-03-05 14:44:47+00:00',
'role': 'control',
'status': 'diskmgmt_completed', 'uuid':
'861d4d73-ffee-40bf-9348-13afc697ee3d'},
'cdfd18c1-6346-47a2-b0f5-661305b5d160': {'action': 'check-disks',
'created_at': '2018-03-05 14:43:50+00:00',
'role': 'all',
'status': 'diskmgmt_completed', 'uuid':
'cdfd18c1-6346-47a2-b0f5-661305b5d160'}
}
}

Show a completed diskmgmt operation

Verb	URI
GET	v1/diskmgmt/show/?uuid=<uuid>

Example

JSON Request

GET /v1/diskmgmt/show/?uuid=d24036c6-4557-4c12-8695-a92f6f9315ed

JSON Response

200 OK
Content-Type: application/json
{'action': 'check-disks',
'created_at': '2018-03-07 21:46:41+00:00',
'diskmgmt_request': "{u'uuid': 'd24036c6-4557-4c12-8695-a92f6f9315ed',
u'json_display': False, u'servers': u'f24-michigan-micro-2', u'locator': False,
u'role': u'compute', u'action': u'check-disks', u'command': u'create'}",
'diskmgmt_result': '{"status": "PROCESSED", "message": ["{\'Overall_Status\': \'PASS\',
\'Result\': {\'fcfg_disks_results_list\': [], \'spare_disks_results_list\': [],
\'raid_results_list\': [{\'RAID level\': \'RAID1\', \'Disk Med\': \'HDD\', \'server\':
\'7.7.7.6\', \'RAID type\': \'HW\', \'host\': \'f24-michigan-micro-2\', \'role\':
\'block_storage control compute\', \'VD health\': \'Optl\', \'Num VDs\': 1, \'Num PDs\': 8, \'RAID health\': \'Opt\'}], \'bad_disks_results_list\': [],
\'rbld_disks_results_list\':
[], \'add_as_spares_disks_results_list\': []}}"]}', 'role': 'compute',
'status': 'diskmgmt_completed', 'updated_at': '2018-03-07 21:47:35+00:00',
'uuid': 'd24036c6-4557-4c12-8695-a92f6f9315ed'
}

Delete a completed diskmgmt operation

Verb	URI
DELETE	v1/diskmgmt/delete/?uuid=<uuid>

Example

JSON Request

DELETE /v1/diskmgmt/delete/?uuid=d24036c6-4557-4c12-8695-a92f6f9315ed

JSON Response

200 OK
Content-Type: application/json
{
"status": "deleted",
"message": "UUID d24036c6-4557-4c12-8695-a92f6f9315ed deleted from database", "uuid": "d24036c6-4557-4c12-8695-a92f6f9315ed",
"error": "None"
}

OSD Maintenance information

REST wrapper to query information about OSD on Pod storage nodes. This returns to the OSD status information of all or a selection of OSDs available in the Pod.

Create a OSD disk operation

Verb	URI
POST	/v1/osdmgmt/check_osds

Example

JSON Request

POST /v1/osdmgmt/osdmgmt/check_osds '{"osdmgmt_request": {"command": "create",
"action": "check-osds",
"locator": "False", "json_display": "False", "servers": "",
"osd": "None",
"uuid": ""}}'

JSON Response

201 Created
Content-Type: application/json
{
'action': 'check-osds',
'created_at': '2018-03-08T21:26:15.329195+00:00',
'osdmgmt_request': "{u'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223', u'json_display': u'False', u'servers': u'', u'locator': u'False', u'command':
u'create', u'action':
u'check-osds', u'osd': u'None'}", 'osdmgmt_result': '', 'status': 'not_run', 'updated_at': 'None'
}

Create a replace OSD operation

Verb	URI
POST	v1/osdmgmt/replace_osd

Example

JSON Request

POST /v1/osdmgmt/replace_osd Accept: application/json
'{"osdmgmt_request": {"command": "create",
"action": "replace-osd",
"locator": "False", "json_display": "False", "servers": "f24-michigan-micro-1", "osd": "osd.9",
"uuid": ""}}'

JSON Response

201 Created
Content-Type: application/json
{
"status": "not_run",
"osdmgmt_request": "{u'uuid': '5140f6fb-dca3-4801-8c44-89b293405310', u'json_display': u'False', u'servers': u'f24-michigan-micro-1', u'locator': u'False',
u'command': u'create',
u'action': u'replace-osd', u'osd': u'osd.9'}", "created_at": "2018-03-09T15:07:10.731220+00:00",
"updated_at": null, "action": "replace-osd", "osdmgmt_result": ""
}
}

List check OSD operation

Verb	URI
GET	v1/osdmgmt/list/? action= {check-osds,replace-osd}

Example

JSON Request

GET /v1/osdmgmt/list/?action=check-osds

JSON Response

200 OK
Content-Type: application/json
{
'4efd0be8-a76c-4bc3-89ce-142de458d844': {'action': 'check-osds',
'created_at': '2018-03-08 21:31:01+00:00',
'status': 'osdmgmt_running', 'uuid':
'4efd0be8-a76c-4bc3-89ce-142de458d844'},
'5fd4f9b5-786a-4a21-a70f-bffac70a3f3f': {'action': 'check-osds',
'created_at': '2018-03-08 21:11:13+00:00',
'status': 'osdmgmt_completed', 'uuid':
'5fd4f9b5-786a-4a21-a70f-bffac70a3f3f'},

'9c64ee52-bed5-4b69-91a2-d589411dd223': {'action': 'check-osds',
'created_at': '2018-03-08 21:26:15+00:00',
'status': 'osdmgmt_completed', 'uuid':
'9c64ee52-bed5-4b69-91a2-d589411dd223'}
}
}
Show a completed osdmgmt operation

Verb	URI
GET	v1/osdmgmt/show/?uuid=<uuid>

Example

JSON Request

GET /v1/osdmgmt/show/?uuid=9c64ee52-bed5-4b69-91a2-d589411dd223

JSON Response

200 OK
Content-Type: application/json
{
'action': 'check-osds',
'created_at': '2018-03-08 21:26:15+00:00',
'osdmgmt_request': "{u'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223', u'json_display': u'False', u'servers': u'', u'locator': u'False', u'command': u'create', u'action':
u'check-osds', u'osd': u'None'}",
'osdmgmt_result': '{"status": "PROCESSED", "message": ["{\'Overall_Status\': \'PASS\',
\'Result\': { ommitted for doc }}]}', 'status': 'osdmgmt_completed', 'updated_at': '2018-03-08 21:27:16+00:00',
'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223'
}
}

Delete a completed osdmgmt operation

Verb	URI
DELETE	v1/osdmgmt/delete/?uuid=<uuid>

Example

JSON Request

DELETE /v1/osdmgmt/delete/?uuid=9c64ee52-bed5-4b69-91a2-d589411dd223

JSON Response

200 OK
Content-Type: application/json
{
'error': 'None',
'message': 'UUID 9c64ee52-bed5-4b69-91a2-d589411dd223 deleted from database', 'status': 'deleted',
'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223'
}

}

Hardware Management Utility

REST wrapper to control the execution of or query information from the hardware validation utility.

Create a Validate Operation

Verb	URI
POST	/v1/hardwaremgmt/validate

JSON Request
POST /v1/hardwaremgmt/validate '{"hwmgmt_request": {"command": "create",
"action": "validate", "hosts": "None",
"file": "None", "feature_list": "all", "uuid": ""}}'
feature_list is a comma separated list of valid features for the given POD

JSON Reponse

201 Created
Content-Type: application/json
{
'action': 'validate',
'created_at': '2018-03-08T22:01:22.195232+00:00',
'hwmgmt_request': "{u'feature_list': u'all', u'command': u'create', u'file': None, u'action': u'validate', u'hosts': None, u'uuid': '89e094d8-b246-4620-afca-ba3529385cac'}",
'hwmgmt_result': '',
'status': 'not_run', 'updated_at': 'None'
}

Create a Validate Operation for Failure

Verb	URI
GET	/v1/hardwaremgmt/resolve_failures

JSON Request
POST /v1/hardwaremgmt/resolve_failures
{
"hwmgmt_request": { "command": "create",
"action": "resolve-failures", "hosts": "None",
"file": "None", "feature_list": "all", "uuid": ""}
}
feature_list is a comma separated list of valid features for the given POD

JSON Response

201 Created
Content-Type: application/json
{

"status": "not_run",
"created_at": "2018-03-09T15:47:36.503712+00:00",
"hwmgmt_request": "{u'feature_list': u'all', u'command': u'create', u'file': None, u'action': u'resolve-failures', u'hosts': None, u'uuid': '49dc1dc9-3170-4f68-b152-0f99bd19f7b1'}",
"updated_at": "",
"action": "resolve-failures", "hwmgmt_result": ""
}

Create a Validate Operation

Verb	URI
GET	v1/hardwaremgmt/list

JSON Request
GET /v1/hardwaremgmt/list

JSON Response

200 OK
Content-Type: application/json
{'89e094d8-b246-4620-afca-ba3529385cac': {'action': 'validate',
'created_at': '2018-03-08 22:01:22+00:00',
'feature_list': 'all',
'status': 'hardwaremgmt_completed', 'uuid':
'89e094d8-b246-4620-afca-ba3529385cac'},
'9f70e872-a888-439a-8661-2d2f36a4f4b1': {'action': 'validate',
'created_at': '2018-03-08 20:34:32+00:00',
'feature_list': 'all',
'status': 'hardwaremgmt_completed', 'uuid':
'9f70e872-a888-439a-8661-2d2f36a4f4b1'}
}

Show a completed hardwaremgmt operation

Verb	URI
GET	/v1/hardwaremgmt /show /?uuid=<uuid>

JSON Request
GET /v1/hardwaremgmt/show/?uuid=9f70e872-a888-439a-8661-2d2f36a4f4b

JSON Response

200 OK
Content-Type: application/json
{
'action': 'validate',
'created_at': '2018-03-08 20:34:32+00:00',
'feature_list': 'all',
'hwmgmt_request': "{u'feature_list': u'all', u'hosts': None, u'file': None, u'action': u'validate', u'command': u'create', u'uuid': '9f70e872-a888-439a-8661-2d2f36a4f4b1'}",
'hwmgmt_result': '{"status": "PROCESSED", "message": "Validate of all completed", "results": {"status": "PASS", "results": [{"status": "PASS", "name": "CIMC Firmware Version
Check", "err": null}, {"status": "PASS", "name": "All Onboard LOM Ports Check", "err":
null}, {"status": "PASS", "name": "PCIe Slot: HBA Status Check", "err": null}, {"status":

"PASS", "name": "Server Power Status Check", "err": null}, {"status": "PASS", "name": "NFV Config Check", "err": null}, {"status": "PASS", "name": "Physical Drives Check", "err":
null}, {"status": "PASS", "name": "PCIe Slot(s) OptionROM Check", "err": null}, {"status": "PASS", "name": "Intel Network Adapter Check", "err": null}]}}',
'status': 'hardwaremgmt_completed', 'updated_at': '2018-03-08 20:38:02+00:00', 'uuid': '9f70e872-a888-439a-8661-2d2f36a4f4b1'

Delete a completed hardwaremgmt operation

Verb	URI
DELETE	/v1/hardwaremgmt/delete/?uuid=<uuid>

JSON Request
DELETE /v1/hardwaremgmt/delete/?uuid=9f70e872-a888-439a-8661-2d2f36a4f4b1

JSON Response

200 OK
Content-Type: application/json
{
'error': 'None',
'message': 'UUID 9f70e872-a888-439a-8661-2d2f36a4f4b1 deleted from database', 'status': 'deleted',
'uuid': '9f70e872-a888-439a-8661-2d2f36a4f4b1'
}

Setupdata and Offline Validation

Setupdata and Offline Validation

Setupdata

REST wrapper for setupdata. Provides methods for listing, creating, modifying, and deleting setupdata.

Retrieving the setupdata

Resource URI

Verb	URI
GET	/v1/setupdata

Example

JSON Request

```
GET /v1/setupdata
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{"setupdatas": [{
"status": "Active",
"name":"GG34",
"uuid": "123"
"meta":{
"user":"root"
},
"jsondata":{
.......
}
}]}
```

Creating setupdata

Resource URI

Verb	URI
POST	/v1/setupdata

Example

JSON Request

```
POST /v1/setupdata
Accept: application/json
{
"name":"GG34",
"uuid": "123"
"meta":{
"user":"root"
},
"jsondata":{
.......
}
}
```

JSON Response

```
201 OK
Content-Type: application/json
{
        "status": "Active",
        "name":"GG34",
        "uuid": "123"
         "meta":{
         "user":"root"
},
"jsondata":{
.......
 }
}

400 Bad Request
Content-Type: application/json
{
       "debuginfo": null
       "faultcode":"Client"
       "faultstring": "Error"
}
409 CONFLICT
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Error"
}
```

Retrieving a single setupdata

Resource URI

Verb	URI
GET	/v1/setupdata/(id)

Property:
id—The ID of the setupdata that you want to retrieve.

Example

JSON Request

```
GET /v1/setupdata/123
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "status": "Active",
        "name":"GG34",
        "uuid": "123"
        "meta":{
        "user":"root"
},
"jsondata":{
.......
        }
}
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
"faultcode": "Client"
"faultstring": "Setupdata could not be found."
}
```

Updating a setupdata

Resource URI

Verb	URI
PUT	/v1/setupdata/(id)

Property:
id—The ID of the setupdata that you want to update. Example

JSON Request

```
PUT /v1/setupdata/123 Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
 "status": "Active",
 "name":"GG34",
 "uuid": "123"
 "meta":{
 "user":"root"
  },
 "jsondata":{
 .......
 }
}
404 NOT FOUND
Content-Type: application/json
{
 "debuginfo": null
 "faultcode": "Client"
 "faultstring": "Setupdata could not be found."
}
```

Deleting a setupdata

Resource URI

Verb	URI

DELETE	/v1/setupdata/(id)

Property:
id—The ID of the setupdata that you want to delete. Example

JSON Request

```
DELETE /v1/setupdata/123 Accept: application/json
```

JSON Response

```
204 NO CONTENT Returned on success
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Setupdata could not be found."
}
400 BAD REQUEST
Content-Type: application/json
{
"debuginfo": null "faultcode": "Client"
"faultstring": "Setupdata cannot be deleted when it is being used by an installation"
}
```

Offline validation

REST wrapper does the offline validation of setupdata. Rest wrapper does only the software Validation of the input setupdata.

Create an offline validation operation

Resource URI

Verb	URI
POST	/v1/offlinevalidation

Example

JSON Request

```
POST /v1/offlinevalidation
Accept: application/json
 {
 "jsondata": "."
 }
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
"status": "NotValidated",
"uuid": "bb42e4ba-c8b7-4a5c-98b3-1f384aae2b69",
"created_at": "2016-02-03T02:05:28.384274",
"updated_at": "2016-02-03T02:05:51.880785",
"jsondata": "{}",
"validationstatus": {
"status": "PASS",
"Software_Validation": [],
"Hardware_Validation": []
}
}
```

Retrieve the results of offline validation

Resource URI

Verb	URI
GET	/v1/offlinevalidation

Property:
id—The ID of the node you want to retrieve. Example

JSON Request

```
GET /v1/offlinevalidation/789
Accept: application/json
```

JSON Response


```
200 OK
Content-Type: application/json
{
"status": " ValidationSuccess",
"uuid": "bb42e4ba-c8b7-4a5c-98b3-1f384aae2b69",
"created_at": "2016-02-03T02:05:28.384274",
"updated_at": "2016-02-03T02:05:51.880785",
"jsondata": "{}",
"validationstatus": {
"status": "PASS",
"Software_Validation": [],
"Hardware_Validation": []
}
}
```

Nodes and Replace Controller

Nodes and Replace Controller

Nodes

Getting a list of nodes

Resource URI

Verb	URI
GET	/v1/nodes

Example

JSON Request

```
Get /v1/nodes
Accept: application/js
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "nodes": [
        [
                "status": "Active",
                "uuid": "456",
                "setupdata": "123",
                "node_data": "{
                "rack_info": {
                "rack_id": "RackA"
                },
                "cimc_info": {
                  "cimc_ip": "10.10.10.10"
                },
        "management_ip": "7.7.7.10"
          }",
        "updated_at": null,
        "mtype": "compute",
        "install": "345",
        "install_logs": "logurl",
        "created_at":"2016-0710T06:17:03.761152",
        "name": " compute-1"
        }
   ]
}
```

Add New Nodes

The nodes are in compute or block_storage type. Before adding the nodes to the system, the name of the nodes and other necessary information like cimc_ip and rackid must be updated in the setupdata object. If the setupdata object is not updated, the post call does not allow you to add the node.
Resource URI

Verb	URI

POST	/v1/nodes

Example

JSON Request

```
POST /v1/nodes
Accept: application/js
 {
 "name" : "compute-5"
 }
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
        "status": "ToAdd",
        "uuid": "456",
        "setupdata": "123",
        "node_data": "{
        "rack_info": {
        "rack_id": "RackA"
        },
        "cimc_info": {
        "cimc_ip": "10.10.10.10"
        },
        "management_ip": "7.7.7.10"
        }",
        "updated_at": null,
        "mtype": "compute",
        "install": "345",
        "install_logs": "logurl",
        "created_at":"2016-0710T06:17:03.761152",
        "name": " compute-1"
}
```

Retrieve information about a particular node

Resource URI

Verb	URI
GET	/v1/nodes{id}

Property:
id—The ID of the node that you want to retrieve. Example

JSON Request

```
POST /v1/nodes
Accept: application/js
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "status": "Active",
        "uuid": "456",
        "setupdata": "123",
        "node_data": "{
        "rack_info": {
        "rack_id": "RackA"
        },
        "cimc_info": {
        "cimc_ip": "10.10.10.10"
        },
        "management_ip": "7.7.7.10"
        }",
        "updated_at": null,
        "mtype": "compute",
        "install": "345",
        "install_logs": "logurl",
        "created_at":"2016-0710T06:17:03.761152",
        "name": " compute-1"
}
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Node doesn't exists"
}
```

Remove a Node

The node to be deleted must be removed from the setupdata object. Once the setupdata object is updated, you can safely delete the node. The node object cannot be deleted until it calls the remove node backend and succeeds.
Resource URI

Verb	URI
DELETE	/v1/nodes{id}

Property:
id—The ID of the node that you want to remove. Example

JSON Request

```
DELETE /v1/nodes/456
Accept: application/js
```

JSON Response

```
204 ACCEPTED
Content-Type: application/json
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Node doesn't exists"
}
```

To clear the database and delete the entries in the nodes, the delete API is called with special parameters that are passed along with the delete request. The JSON parameters are in the following format.

JSON Request

```
DELETE /v1/nodes/456
Accept: application/js
 {
 "clear_db_entry":"True"\
 }
```

JSON Response

```
204 ACCEPTED
 Content-Type: application/json

 404 NOT FOUND
 Content-Type: application/json
 {
         "debuginfo": null
         "faultcode": "Client"
         "faultstring": "Node doesn't exists"
 }
```

⚠ This is done only if the node is deleted from the REST API database. The failure reason of the node must be rectified manually apart from the API. True is a string and not a boolean in the preceding line.

Health of the Management Node

This API is used to retrieve the health of the management node. It checks various parameters such as partitions, space and so on.
Resource URI

Verb	URI
GET	/v1/health

Example

JSON Request

```
GET /v1/health
 Accept: application/json
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 "status": "PASS", "pod_status": { "color": "BLUE",
 "version": "<VERSION_NO.>"
 },
 "insight_version": "<VERSION_NO.>"
 }
```

Color signifies the health of the pod for Insight:

- Grey signifies that no installation is kicked off on the pod.
- Green signifies that everything is in Good state and cloud installation is active.
- Blue signifies that some operation is running on the pod.
- Red signifies that the pod is in critical state and you might need TAC support to recover the pod.
- Amber indicates a warning if a pod management (Add/Remove/Replace) operation failed.

Replace a controller

Resource URI

Verb	URI
PUT	/v1/nodes{id}

Property:
id—The ID of the controller that you want to replace. Example

JSON Request

```
PUT /v1/nodes/456 Accept: application/js
```

JSON Response

```
200 OK
 Content-Type: application/json
 404 NOT FOUND
 Content-Type: application/json
 {
         "debuginfo": null
         "faultcode": "Client"
          "faultstring": "Node doesn't exists"
 }
```

Install Resource

Install Resource

REST wrapper for install. Provides methods for starting, stopping, and viewing the status of the installation process.

Return a list of installation

Resource URI

Verb	URI
GET	/v1/install

Example

JSON Request

```
GET /v1/install
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
  {"installs": [{
        "ceph": "Skipped",
        "uuid": "123",
        "setupdata": "345",
        "vmtpresult": "{
        "status": "PASS",
        "EXT_NET": []
  }",
        "baremetal": "Success",
        "orchestration": "Success",
        "validationstatus": "{
        "status": "PASS",
        "Software_Validation": [],
        "Hardware_Validation": []
  }",
    "currentstatus": "Completed",
        "validation": "Success",
        "hostsetup": "Success",
        "vmtp": "Skipped"
  }]
}
```

Create an installation

Resource URI

Verb	URI
POST	/v1/install

Example

JSON Request

```
GET /v1/install
Accept: application/js
{
        "setupdata": "123",
        "stages": [
        "validation",
        "bootstrap",
        "runtimevalidation",
        "baremetal",
        "orchestration",
        "hostsetup",
        "ceph",
        "vmtp"
        ]
}
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
        "ceph": "Skipped",
        "uuid": "123",
        "setupdata": "345",
        "vmtpresult": "{
        "status": "PASS",
        "EXT_NET": []
}",
        "baremetal": "Success",
        "orchestration": "Success",
        "validationstatus": "{
        "status": "PASS",
        "Software_Validation": [],
        "Hardware_Validation": []
}",
        "currentstatus": "Completed",
        "validation": "Success",
        "hostsetup": "Success",
        "vmtp": "Skipped"
}
409 CONFLICT
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Install already exists"
}
```

Retrieve the installation

Resource URI

Verb	URI
GET	/v1/install/{id}

Property:
id—The ID of the installation that you want to retrieve.

Example

JSON Request

```
GET /v1/install/345
Accept: application/js
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "ceph": "Skipped",
        "uuid": "123",
        "setupdata": "345",
        "vmtpresult": "{
        "status": "PASS",
        "EXT_NET": []
}",
        "baremetal": "Success",
        "orchestration": "Success",
        "validationstatus": "{
        "status": "PASS",
        "Software_Validation": [],
        "Hardware_Validation": []
}",
        "currentstatus": "Completed",
        "validation": "Success",
        "hostsetup": "Success",
        "vmtp": "Skipped"
}
404 NOT FOUND
Content-Type: application/json
{
        "debuginfo": null
        "faultcode": "Client"
        "faultstring": "Install doesn't exists"
}
```

Stop the installation

Resource URI

Verb	URI
DELETE	/v1/install/{id}

Property:
id—The ID of the installation that you want to stop. Example

JSON Request

```
DELETE /v1/install/345
Accept: application/js
```

JSON Response

```
204 NO CONTENT
 Content-Type: application/json

404 NOT FOUND
 Content-Type: application/json
 {
        "debuginfo": null "faultcode": "Client"
        "faultstring": "Install doesn't exists"
 }
```

OpenStack Setup

OpenStack Setup

Secrets

Retrieve the list of secrets that are associated with the OpenStack Setup

You can retrieve the set of secret password that are associated with the OpenStack setup using the preceding api. This gives the list of secrets for each service in OpenStack.
Resource URI

Verb	URI
GET	/v1/secrets

Example

JSON Request

```
GET /v1/secrets
 Accept: application/json
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 "HEAT_KEYSTONE_PASSWORD": "xxxx", "CINDER_KEYSTONE_PASSWORD": "xxxxx",
 ....
 ....
 "RABBITMQ_PASSWORD": "xxxxx"
 }
```

OpenStack Configuration

Retrieve the list of configurations associated with the OpenStack Setup

You can retrieve the set of OpenStack configurations associated with the OpenStack setup using the preceding api. This gives the current settings of different configurations such as verbose logging and debug logging for different OpenStack services.

Verb	URI
GET	/v1/secrets

JSON Request

```
GET /v1/openstack_config
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
{
        "CINDER_DEBUG_LOGGING": false,
        "KEYSTONE_DEBUG_LOGGING": false,
        ....
        ....
        "NOVA_VERBOSE_LOGGING": true
}
```

Release mapping Information

This api is used to see the list of features included and list of options which can be reconfigured in the Openstack Setup.

Retrieve the release mapping information

Resource URI

Verb	URI
GET	/v1/releasemapping

JSON Request

```
GET /v1/releasemapping
Accept: application/json
```

JSON Response

```
200 OK
Content-Type: application/json
[
   {
        "SWIFTSTACK": {
                "feature_status": true,
                 ],
        "desc": "swift stack feature"
    }
   },........
..............
}
```

Update

Update

Start an Update Process

Resource URI

Verb	URI
POST	/v1/update

Parameters:

- fileupload - tar file to be uploaded.
- filename - Name of the uploaded file.

Example

JSON Request

```
curl -sS -X POST --form
"fileupload=@Test/installer.good.tgz" --form
"filename=installer.good.tgz"
https://10.10.10.8445/v1/update
```

⚠ This curl request is done as a form request.

JSON Response

```
200 OK
 Content-Type: application/json
 {
        "update_logs": "logurl",
         "update_status": "UpdateSuccess",
        "update_filename": "installer-4579.tgz",
        "created_at": "2016-07-10T18:33:52.698656",
        "updated_at": "2016-07-10T18:54:56.885083"
 }
 409 CONFLICT
 Content-Type: application/json
 {
 "debuginfo": null "faultcode": "Client"
 "faultstring": "Uploaded file is not in tar format"
 }
```

Roll back an update

Resource URI

Verb	URI
PUT	/v1/update

Example

JSON Request

```
PUT /v1/update
 Accept: application/json
 {
 "action":"rollback"
 }
```

JSON Response

```
200 OK
 Content-Type: application/json
 {

 "update_logs": "logurl", "update_status": "ToRollback", "update_filename": "installer-4579.tgz",
 "created_at": "2016-07-10T18:33:52.698656", "updated_at": "2016-07-10T18:54:56.885083"
 }
```

Commit an update

Resource URI

Verb	URI
PUT	/v1/update

Example

JSON Request

```
PUT /v1/update
Accept: application/json
{
 "action":"commit"
}
```

JSON Response

```
200 OK
Content-Type: application/json
{
 "update_logs": "logurl", "update_status": "ToCommit", "update_filename": "installer-4579.tgz",
 "created_at": "2016-07-10T18:33:52.698656", "updated_at": "2016-07-10T18:54:56.885083"
}
```

Retrieve the details of an update

Resource URI

Verb	URI
GET	/v1/update

Example

JSON Request

```
GET /v1/update
 Accept: application/json
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
         "update_logs": "logurl",
        "update_status": "UpdateSuccess",
        "update_filename": "installer-4579.tgz",
    "created_at": "2016-07-10T18:33:52.698656",
        "updated_at": "2016-07-10T18:54:56.885083"
 }
```

Version and Hardware Information

Version and Hardware Information

Version

Retrieve the version of the Cisco VIM.

Resource URI

Verb	URI
GET	/v1/version

Example

JSON Request

```
GET /v1/version
 Accept: application/json
```

JSON Response

```
200 OK
 Content-Type: application/json
 {"version": "1.9.1"}
```

Hardware Information

REST wrapper returns the hardware information available in the setupdata.

Create a HWinfo Operation

Resource URI

Verb	URI
GET	/v1/hwinfo

Example

JSON Request

```
POST /v1/hwinfo
 Accept: application/json
 {
 "setupdata":"c94d7973-2fcc-4cd1-832d-453d66e6b3bf"
 }
```

JSON Response

```
201 CREATED
 Content-Type: application/json
 {
 "status": "hwinfoscheduled",
 "uuid": "928216dd-9828-407b-9739-8a7162bd0676",
 "setupdata": "c94d7973-2fcc-4cd1-832d-453d66e6b3bf", "created_at": "2017-03-19T13:41:25.488524",
 "updated_at": null, "hwinforesult": ""
 }
```

Retrieve Hwinfo Operation Results

Resource URI

Verb	URI
GET	/v1/hwinfo/{id}

Property:
id—The ID of the node you want to query. Example

JSON Request

```
GET /v1/hwinfo/789 Accept: application/json
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 "status": "hwinfosuccess",
 "uuid": "928216dd-9828-407b-9739-8a7162bd0676",

 "setupdata": "c94d7973-2fcc-4cd1-832d-453d66e6b3bf", "created_at":
"2017-03-19T13:41:25.488524", "updated_at":
"2017-03-19T13:42:05.087491",
 "hwinforesult": "{\"172.29.172.73\": {\"firmware\": ..............
 ............
 ..................
 }
```

Get Node Hardware Information

Rest API helps you to get the hardware information of all the nodes in the pod through CIMC/UCSM.

- Total Memory
- Firmware Info (Model, Serial Number)
- CIMC IP

```
GET Request URL
/v1/hwinfo
Output Response
{
        "hwinforesult": "{"control-server-2": {"memory": {"total_memory": "131072"},
        "firmware": {"serial_number": "FCH1905V16Q", "fw_model": "UCSC-C220-M4S"},
        "cimc_ip": "172.31.230.100", "storage": {"num_storage": 4},
        "cisco_vic_adapters": {"product_name": "UCS VIC 1225"},
        "cpu": {"number_of_cores": "24"}, "power_supply": {"power_state": "on"}}
...
}
```

Post-Installation Operations

Post-Installation Operations

The following are the post install operations that can be performed, after the successful installation of OpenStack. It uses a common api. Following is an Example:

1. reconfigure
2. reconfigure -regenerate passwords
3. reconfigure -setpasswords,setopenstack_configs
4. reconfigure -alertmanager_config, -alerting_rules_config
5. check-fernet-keys
6. resync-fernet-keys
7. rotate-fernet-keys

Create a post install operation

Resource URI

Verb	URI
POST	/v1/misc

Examples:

JSON Request

```
POST /v1/misc
 Accept: application/json
 {"action": {"reconfigure": true}}
```

JSON Response

```
201 CREATED
 Content-Type: application/json
 {
        "uuid": "7e30a671-bacf-4e3b-9a8f-5a1fd8a46733",
        "created_at": "2017-03-19T14:03:39.723914",
         "updated_at": null,
         "operation_status": "OperationScheduled",
        "operation_logs": "",
    "operation_name": "{"reconfigure": true}"
 }
```

JSON Request

```
POST /v1/misc
 Accept: application/json
 {"action": {"reconfigure": true, "alertmanager_config": <json_config>}}
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
 "uuid": "68b67265-8f09-480e-8608-b8aff77e0ec7",
 "created_at": "2019-01-09T16:42:11.484604+00:00",
 "updated_at": null,
 "operation_status": "OperationScheduled",
 "operation_logs": "",
 "operation_name": "{"alertmanager_config": <json_config>, "reconfigure": true}"
 }
```

Retrieve post install operation status

Resource URI

Verb	URI
GET	/v1/misc

Example

JSON Request

```
GET /v1/misc
 Accept: application/json
```

JSON Response

```
201 CREATED
 Content-Type: application/json
 {
        "uuid":
        "7e30a671-bacf-4e3b-9a8f-5a1fd8a46733",
        "created_at": "2017-03-19T14:03:39.723914",
        "updated_at": "2017-03-19T14:03:42.181180",
        "operation_status": "OperationRunning",
        "operation_logs": "xxxxxxxxxxxxxxxx",
        "operation_name": "{\"reconfigure\": true}"
 }
```

Testing and Polling

Testing and Polling

NFVBench Network Performance Testing

Create NFVBench Run

Starts the network performance test with provided configuration.

REST API to create fixed rate test

Verb	URI
Post	v1/nfvbench/ create_ndr_pdr_test

Example

JSON Request

```
POST Request URL
 /v1/nfvbench/create_fixed_rate_test JSON Request:
 {"nfvbench_request":
         {
         "duration_sec": 20,
         "traffic_profile": [
                 {
                   "name": "custom",
                   "l2frame_size": ["64","IMIX", "1518"]
                   }
         ],
         "traffic": { "bidirectional": true,
                         "profile": "custom"
                               },
         "flow_count": 1000
 }
}
```

JSON Response

```
201 CREATED
Content-Type: application/json
{
        "status": "not_run",
        "nfvbench_request":
  '{
        "duration_sec": 20,
        "traffic_profile": [
                {
                "name": "custom",
                "l2frame_size": ["64","IMIX","1518"]
                }
        ],
        "traffic": {"bidirectional": true,
                                "profile": "custom"
                                },
        "flow_count": 1000
        }',
"created_at": "2017-08-16T06:14:54.219106",
"updated_at": null,
"nfvbench_result": "",
"test_name": "Fixed_Rate_Test"
}
```

Status Polling

The polling status of NFVbench status can be nfvbench_running, nfvbench_failed, or nfvbench_completed.

Resource URI

Verb	URI
GET	v1/nfvbench/<test_name>

Get fixed rate test result

```
GET Request URL
/v1/upgrade/get_fixed_rate_test_result
JSON Response:
Check If NFVbench Test is running
200 OK
Content-Type: application/json
{
 "status": "nfvbench_running",
 "nfvbench_request": '{"traffic": {"bidirectional": true, "profile": "custom"},
 "rate": "1000000pps",
 "traffic_profile": [{"l2frame_size": ["1518"], "name": "custom"}], "duration_sec": 60, "flow_count": 1000}',
 "nfvbench_result": ""
 "created_at": "2017-05-30T21:40:40.394274", "updated_at": "2017-05-30T21:40:41.367279",
 }
Check If NFVbench Test is completed
200 OK
Content-Type: application/json
{
 "status": "nfvbench_completed",
 "nfvbench_request": '{"traffic": {"bidirectional": true, "profile": "custom"}, "rate": "1000000pps",
 "traffic_profile": [{"l2frame_size": ["1518"], "name": "custom"}], "duration_sec": 60, "flow_count": 1000}',
 "nfvbench_result": '{"status": "PROCESSED", "message": {"date": "2017-08-15 23:15:04", "nfvbench_version":
"0.9.3.dev2", ....}
 "created_at": "2017-05-30T21:40:40.394274", "updated_at": "2017-05-30T22:29:56.970779",
 }
```

Execute NDR/PDR test

```
POST Request URL
/v1/nfvbench/create_ndr_pdr_test

Accept: application/json
{"nfvbench_request":
{
        "duration_sec": 20,
        "traffic_profile": [
         {
                "name": "custom",
                "l2frame_size": ["64","IMIX","1518"]
                }
        ],
        "traffic": {"bidirectional": true, "profile": "custom"}, "flow_count": 1000}}

JSON Response
201 CREATED
Content-Type: application/json
{
        "status": "not_run",
        "nfvbench_request":
        '{
                "duration_sec": 20,
                "traffic_profile": [{"name": "custom",
        "l2frame_size": ["64","IMIX","1518"]}],
        "traffic": {"bidirectional": true, "profile": "custom"}, "flow_count": 1000}'
        "created_at": "2017-08-16T07:18:41.652891",
        "updated_at": null,
        "nfvbench_result": "",
        "test_name": "NDR_PDR_Test"
}
```

Get NDR/PDR test results

```
GET Request URL
/v1/ nfvbench/get_ndr_pdr_test_result
JSON Response:
If NFVbench NDR/PDR test is running
200 OK
Content-Type: application/json
{
        "status": "nfvbench_running",
        "nfvbench_request": '{"duration_sec": 20,
        "traffic": {"bidirectional": true, "profile": "custom"},
        "traffic_profile": [{"l2frame_size": ["64", "IMIX", "1518"], "name": "custom"}],
        "flow_count": 1000}',
        "nfvbench_result": ""
        "created_at": "2017-08-16T07:18:41.652891",
        "updated_at": "2017-09-30T22:29:56.970779",
}
If NFVbench NDR/PDR test is completed
200 OK
Content-Type: application/json
{
        "status": "nfvbench_completed",
        "nfvbench_request": '{"duration_sec": 20,
        "traffic": {"bidirectional": true, "profile": "custom"},
        "traffic_profile": [{"l2frame_size": ["64", "IMIX", "1518"], "name": "custom"}], "flow_count":1000}',
        "nfvbench_result": '{"status": "PROCESSED",...}'
        "created_at": "2017-08-16T07:18:41.652891",
        "updated_at": "2017-09-30T22:29:56.970779",
}
```

Mandatory/Optional Feature Mapping

Mandatory/Optional Feature Mapping

Mandatory Feature Mapping

```
POST Request URL
/v1/releasemapping/mandatory_features_mapping

JSON Response:
{
        "mandatory": {
        "networkType": {
        "C": {
                "feature_status": true,
                "values": [{"name": "VXLAN/Linux Bridge", "value": "VXLAN/Linux Bridge"},],
                "insight_label": "Tenant Network",
                "desc": "Tenant Network"
                },
        "B": {
                "feature_status": true,
                "values": [{"name": "VXLAN/Linux Bridge", "value": "VXLAN/Linux Bridge"},],
                "insight_label": "Tenant Network",
                "desc": "Tenant Network"
                }
},
        "cephMode": {
                "all": {
                        "feature_status": true,
                        "values": [{"name": "Central", "value": "Central"},],
                        "insight_label": "Ceph Mode",
                        "desc": "Ceph Mode"
                                }
                        },
        "podType": {
                "C": {
                        "feature_status": true,
                        "values": [{"name": "Fullon", "value": "fullon"},],
                        "insight_label": "POD Type",
                        "desc": "POD Type"
                        },
                "B": {
                        "feature_status": true,
                        "values": [{"name": "Fullon", "value": "fullon"},],
                        "insight_label": "POD Type",
                        "desc": "POD Type"
                        }
},
        "installMode": {
                        "all": {
                                "feature_status": true,
                                "values": [{"name": "Connected", "value": "connected"}, ],
                                "insight_label": "Install Mode",
                                "desc": "Install Mode"
                                }
        }
},
        "platformType": [{"name": "B-series", "value": "B"}, {"name": "C-series", "value":
                        "C"}],
        "postinstalllinks": {
                                "view_cloudpulse": {"alwayson": true, "feature_status": true, "platformtype":
"all",
                                "insight_label": "Run VMTP", "desc": "Cloudpluse"},
                                "password_reconfigure": {"alwayson": true, "feature_status": true,
"platformtype":
                                "all", "insight_label": "Reconfigure Passwords", "desc": "Reconfigure
Passwords"}
                        }
}
```

Optional Feature Mapping

```
POST Request URL
/v1/releasemapping/optional_features_mapping

JSON Response:
[
{
        "SWIFTSTACK": {
                "feature_status": true,
                "insight_label": "Swiftstack",
                "repeated_redeployment": true,
                "reconfigurable": ["cluster_api_endpoint", "reseller_prefix", "admin_password",
                "protocol"],
                "desc": "swift stack feature"
                }
        },
{
        "heat": {
                "feature_status": true,
                "insight_label": "Heat",
                "repeated_redeployment": false,
                "reconfigurable": ["all"],
                "desc": "Openstack HEAT service"
                        }
                },
..... other features
]
```

Cloud Sanity

Cloud Sanity

REST wrapper to run cloud-sanity test suites. The cloud-sanity extension to the VIM REST API enables support for managing cloud-sanity test actions.

Create a cloud-sanity test

Verb	URI
Post	/v1/cloud-sanity/create

Example

JSON Request

```
POST /v1/cloudsanity/create
Accept: application/json
 '{"cloudsanity_request": {"command": "create",
                                                  "action": "test",
                                                  "test_name": "cephmon",
                                                  "uuid": ""}}'
 test_name can be all, management, control, compute, cephmon, cephosd
```

JSON Response

```
201 Created
{
'cloudsanity_request': "{u'action': u'test', u'command': u'create', u'uuid':
'5dff1662-3d33-4901-808d-479927c01dde',
 u'test_name': u'cephmon'}",
'cloudsanity_result': '',
'created_at': '2018-01-26T20:32:20.436445',
'status': 'not_run',
'test_name': 'cephmon',
'updated_at': ''
}
```

List cloud-sanity test results

Verb	URI
GET	/v1/cloud-sanity

JSON Request

```
GET /v1/cloudsanity
```

JSON Response

```
200 OK
{ '0b91746f-90b4-4355-a748-727c2e5c59c5': { 'action': 'test',
                                                                                'created_at': '2018-01-
25 12:08:22',
                                                                                'status':
'cloudsanity_completed',
                                                                                'test_name':
'management',
                                                                                'uuid': '0b91746f-90b4-
4355-a748-727c2e5c59c5'},

  '5695cb31-39e4-4be2-9dee-09e7daffc2e7': { 'action': 'test',
                                                                                  'created_at': '2018-
01-25 12:03:06',
                                                                                'status':
'cloudsanity_completed',
                                                                                'test_name': 'compute',
                                                                                'uuid': '5695cb31-39e4-
4be2-9dee-09e7daffc2e7'},

  '5dff1662-3d33-4901-808d-479927c01dde': { 'action': 'test',
                                                                                'created_at': '2018-01-
26 20:32:20',
                                                                                'status':
'cloudsanity_completed',
                                                                                'test_name': 'cephmon',
                                                                                'uuid': '5dff1662-3d33-
4901-808d-479927c01dde'},

  '7946255d-df58-4432-b729-20cf16eb5ba5': { 'action': 'test',
                                                                                'created_at': '2018-01-
25 12:05:56',
                                                                                'status':
'cloudsanity_completed',
                                                                                'test_name': 'cephosd',

                                                                                'uuid': '7946255d-df58-
4432-b729-20cf16eb5ba5'},
  '797d79ba-9ee0-4e11-9d9e-47791dd05e07': { 'action': 'test',
                                            'created_at': '2018-01-25 12:05:11',
                                                                                'status':
'cloudsanity_completed',
                                                                                'test_name': 'cephmon',

                                                                                'uuid': '797d79ba-9ee0-
4e11-9d9e-47791dd05e07'},
  '962e2c8e-c7b0-4e24-87c1-528cad84002c': { 'action': 'test',
                                                                                'created_at': '2018-01-
26 18:52:31',
                                                                                'status':
'cloudsanity_completed',
                                                                                'test_name': 'control',
                                                                                'uuid': '962e2c8e-c7b0-
4e24-87c1-528cad84002c'},

  'd0111530-ee3b-45df-994c-a0917fd18e11': { 'action': 'test',
                                                                                'created_at': '2018-01-
26 18:46:23',
                                                                                'status':
'cloudsanity_completed',
                                                                                'test_name': 'control',
                                                                                'uuid': 'd0111530-ee3b-
45df-994c-a0917fd18e11'}}
```

List specific cloud-sanity test results

Verb	URI

GET	/v1/cloud-sanity/list/?test_name={all, management, control,compute,cephmon,cephosd}

JSON Request

```
GET /v1/cloudsanity/list/?test_name=cephmon
Accept: application/json
```

JSON Response

```
200 OK
 { '5dff1662-3d33-4901-808d-479927c01dde': { 'action': 'test',
                                                                                'created_at': '2018-
01-26 20:32:20',
                                                                               'status':
'cloudsanity_completed',
                                                                               'test_name': 'cephmon',
                                                                             'uuid': '5dff1662-3d33-
4901-808d-479927c01dde'},
   '797d79ba-9ee0-4e11-9d9e-47791dd05e07': { 'action': 'test',
                                                                               'created_at': '2018-01-
25 12:05:11',
                                                                               'status':
'cloudsanity_completed',
                                                                               'test_name': 'cephmon',
                                                                                'uuid': '797d79ba-
9ee0-4e11-9d9e-47791dd05e07'}}
```

Show cloud-sanity test results

Verb	URI
GET	/v1/cloud-sanity/show/?uuid=<uuid>

JSON Request

```
GET /v1/cloudsanity/show/?uuid=d0111530-ee3b-45df-994c-a0917fd18e11
```

JSON Response

```
200 OK
 { 'action': 'test',
   'cloudsanity_request':
         "{u'action': u'test',
           u'command': u'create',
           u'uuid': 'd0111530-ee3b-45df-994c-a0917fd18e11',
           u'test_name': u'control'}",
   'cloudsanity_result':
          '{"status": "PROCESSED",
                "message": {"status": "Pass",
               "message": "[PASSED] Cloud Sanity Control Checks Passed",
               "results": {"control": {"ping_all_controller_nodes": "PASSED",
                                                                    "check_rabbitmq_is_running": "PASSED",
                                                                   "check_rabbitmq_cluster_status": "PASSED",
                                                                   "check_nova_service_list": "PASSED",
                                                                   "ping_internal_vip": "PASSED",
                                                                   "disk_maintenance_raid_health": "PASSED",
                                                                   "check_mariadb_cluster_size": "PASSED",
                                                                   "disk_maintenance_vd_health": "PASSED"}}}}',
        'created_at': '2018-01-26 18:46:23',
         'status': 'cloudsanity_completed',
        'test_name': 'control',
    'updated_at': '2018-01-26 18:47:58',
        'uuid': 'd0111530-ee3b-45df-994c-a0917fd18e11'}
```

Delete cloud-sanity test results

Verb	URI
DELETE	/v1/cloud-sanity/delete/?uuid=<uuid>

JSON Request

```
GET /v1/cloudsanity/delete/?uuid=444aa4c8-d2ba-4379-b035-0f47c686d1c4
```

JSON Response

```
200 OK
{
 "status": "deleted",
 "message": "UUID 444aa4c8-d2ba-4379-b035-0f47c686d1c4 deleted from database",
 "uuid": "444aa4c8-d2ba-4379-b035-0f47c686d1c4",
 "error": "None"
 }
```

Disk and OSD Maintenance

Disk and OSD Maintenance

Disk Maintenance information

REST wrapper to query information about RAID disks on Pod nodes. This returns the RAID disk information of all or a selection of RAID disks available in the Pod.
The disk management extension to the VIM REST API enables support for Disk Management actions

Create a Check disk operation

Resource URI

Verb	URI
POST	/v1/diskmgmt/check_disks

Example

JSON Request

```
POST /v1/diskmgmt/check_disks
Accept: application/json
'{"diskmgmt_request": {"command": "create",
                                          "action": "check-disks",
                                          "role": "control",
                                          "locator": "False",
                                          "json_display": "False",
                                          "servers": "",
                                          "uuid": ""}}'
```

JSON Response

```
201 Created
Content-Type: application/json
{
        'action': 'check-disks',
        'created_at': '2018-03-08T02:03:18.170849+00:00',
        'diskmgmt_request': "{u'uuid': '0729bdea-cc19-440f-8339-ab21e76be84b',
                                                u'json_display': u'False',
    u'servers': u'',
        u'locator': u'False',
        u'role': u'control',
        u'action': u'check-disks',
        u'command': u'create'}",
        'diskmgmt_result': '',
        'status': 'not_run',
        'updated_at': 'None'
}
```

Create a replace disk operation

Verb	URI
POST	/v1/diskmgmt/replace_disks

Example

JSON Request

```
POST /v1/diskmgmt/replace_disks
Accept: application/json
 '{"diskmgmt_request": {"command": "create",
                                                    "action": "replace-disks",
                                                   "role": "control",
                                                   "locator": "False",
                                                   "json_display": "False",
                                                   "servers": "", "uuid": ""}}'
```

JSON Response

```
201 Created
Content-Type: application/json
{
 "status": "not_run",
 "diskmgmt_request": "{u'uuid': 'cb353f41-6d25-4190-9386-330e971603c9',
                                          u'json_display': u'False',
                                          u'servers': u'',
                                          u'locator': u'False',
                                          u'role': u'control',
                                          u'action': u'replace-disks',
                                          u'command': u'create'}",
 "created_at": "2018-03-09T12:43:41.289531+00:00",
 "updated_at": "",
 "diskmgmt_result": "",
 "action": "replace-disks"}
```

List check disk operation

Verb	URI
GET	/v1/diskmgmt/list/?action={check-disks,replace-disks \&role={all,management,control,compute}

Example

JSON Request

```
GET /v1/diskmgmt/list/?action=check-disks\&role=all
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 '0be7a55a-37fe-43a1-a975-cbf93ac78893': {'action': 'check-disks',
                                                                                'created_at': '2018-03-05 14:
45:45+00:00',
                                                                                'role': 'compute',
                                                                                'status':
'diskmgmt_completed',
                                                                                'uuid': '0be7a55a-37fe-43a1-
a975-cbf93ac78893'},
 '861d4d73-ffee-40bf-9348-13afc697ee3d': {'action': 'check-disks',
                                                                                 'created_at': '2018-03-05 14:
44:47+00:00',
                                                                                'role': 'control',
                                                                                 'status':
'diskmgmt_completed',
                                                                                'uuid': '861d4d73-ffee-40bf-
9348-13afc697ee3d'},
 'cdfd18c1-6346-47a2-b0f5-661305b5d160': {'action': 'check-disks',
                                                                                'created_at': '2018-03-05 14:
43:50+00:00',
                                          'role': 'all',
                                          'status': 'diskmgmt_completed',
                                          'uuid': 'cdfd18c1-6346-47a2-b0f5-661305b5d160'}}
 }
```

Show a completed diskmgmt operation

Verb	URI
GET	v1/diskmgmt/show/?uuid=<uuid>

Example

JSON Request

```
GET /v1/diskmgmt/show/?uuid=d24036c6-4557-4c12-8695-a92f6f9315ed
```

JSON Response

```
200 OK
Content-Type: application/json
{'action': 'check-disks',
 'created_at': '2018-03-07 21:46:41+00:00',
 'diskmgmt_request': "{u'uuid': 'd24036c6-4557-4c12-8695-a92f6f9315ed',
 u'json_display': False,
 u'servers': u'f24-michigan-micro-2',
 u'locator': False,
 u'role': u'compute',
 u'action': u'check-disks',
 u'command': u'create'}",
 'diskmgmt_result': '{"status": "PROCESSED", "message": ["{\'Overall_Status\': \'PASS\',
 \'Result\': {\'fcfg_disks_results_list\': [], \'spare_disks_results_list\': [],
 \'raid_results_list\': [{\'RAID level\': \'RAID1\', \'Disk Med\': \'HDD\', \'server\':
 \'7.7.7.6\', \'RAID type\': \'HW\', \'host\': \'f24-michigan-micro-2\', \'role\':

 \'block_storage control compute\', \'VD health\': \'Optl\', \'Num
VDs\': 1, \'Num PDs\': 8, \'RAID health\': \'Opt\'}],
\'bad_disks_results_list\': [], \'rbld_disks_results_list\':
 [], \'add_as_spares_disks_results_list\': []}}"]}',
 'role': 'compute',
 'status': 'diskmgmt_completed',
 'updated_at': '2018-03-07 21:47:35+00:00',
 'uuid': 'd24036c6-4557-4c12-8695-a92f6f9315ed'
 }
```

Delete a completed diskmgmt operation

Verb	URI
DELETE	v1/diskmgmt/delete/?uuid=<uuid>

Example

JSON Request

```
DELETE /v1/diskmgmt/delete/?uuid=d24036c6-4557-4c12-8695-a92f6f9315ed
```

JSON Response

```
200 OK
Content-Type: application/json
{
 "status": "deleted",
 "message": "UUID d24036c6-4557-4c12-8695-a92f6f9315ed deleted from database",
 "uuid": "d24036c6-4557-4c12-8695-a92f6f9315ed",
 "error": "None"
}
```

OSD Maintenance information

REST wrapper to query information about OSD on Pod storage nodes. This returns to the OSD status information of all or a selection of OSDs available in the Pod.

Create a OSD disk operation

Verb	URI
POST	/v1/osdmgmt/check_osds

Example

JSON Request

```
POST /v1/osdmgmt/osdmgmt/check_osds
'{"osdmgmt_request": {"command": "create",
                                          "action": "check-osds",
                                          "locator": "False",
                                      "json_display": "False",
                                          "servers": "",
                                      "osd": "None",
                                          "uuid": ""}}'
```

JSON Response

```
201 Created
Content-Type: application/json
{
 'action': 'check-osds',
 'created_at': '2018-03-08T21:26:15.329195+00:00',
 'osdmgmt_request': "{u'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223',
 u'json_display': u'False', u'servers': u'', u'locator': u'False',
 u'command': u'create', u'action':
 u'check-osds', u'osd': u'None'}",
 'osdmgmt_result': '',
 'status': 'not_run',
 'updated_at': 'None'
}
```

Create a replace OSD operation

Verb	URI
POST	v1/osdmgmt/replace_osd

Example

JSON Request

```
POST /v1/osdmgmt/replace_osd
Accept: application/json
 '{"osdmgmt_request": {"command": "create",
                                           "action": "replace-osd",
                                           "locator": "False",
                                           "json_display": "False",
                                           "servers": "f24-michigan-micro-1",
                                           "osd": "osd.9",
                       "uuid": ""}}'
```

JSON Response

```
201 Created
Content-Type: application/json
{
 "status": "not_run",
 "osdmgmt_request": "{u'uuid': '5140f6fb-dca3-4801-8c44-89b293405310',
 u'json_display': u'False',
 u'servers': u'f24-michigan-micro-1',
 u'locator': u'False',
 u'command': u'create',
 u'action': u'replace-osd',
 u'osd': u'osd.9'}",
 "created_at": "2018-03-09T15:07:10.731220+00:00",
 "updated_at": null,
 "action": "replace-osd",
 "osdmgmt_result": ""
 }
 }
```

List check OSD operation

Verb	URI
GET	v1/osdmgmt/list/? action= {check-osds,replace-osd}

Example

JSON Request

```
GET /v1/osdmgmt/list/?action=check-osds
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 '4efd0be8-a76c-4bc3-89ce-142de458d844': {'action': 'check-osds',
                                                                                'created_at': '2018-03-08 21:
31:01+00:00',
                                                                                'status': 'osdmgmt_running',
                                                                                'uuid': '4efd0be8-a76c-4bc3-
89ce-142de458d844'},
 '5fd4f9b5-786a-4a21-a70f-bffac70a3f3f': {'action': 'check-osds',
                                                                                 'created_at': '2018-03-08 21:
11:13+00:00',
                                                                                 'status':
'osdmgmt_completed',
                                                                                'uuid':'5fd4f9b5-786a-4a21-
a70f-bffac70a3f3f'},

 '9c64ee52-bed5-4b69-91a2-d589411dd223': {'action': 'check-osds',
                                                                                 'created_at': '2018-03-08 21:
26:15+00:00',
                                                                                 'status':
'osdmgmt_completed',
                                          'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223'}
 }
 }
```

Show a completed osdmgmt operation

Verb	URI

GET	v1/osdmgmt/show/?uuid=<uuid>

Example

JSON Request

```
GET /v1/osdmgmt/show/?uuid=9c64ee52-bed5-4b69-91a2-d589411dd223
```

JSON Response

```
200 OK
Content-Type: application/json
{
 'action': 'check-osds',
 'created_at': '2018-03-08 21:26:15+00:00',

 'osdmgmt_request': "
 {u'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223',
 u'json_display': u'False',
 u'servers': u'',
 u'locator': u'False',
 u'command': u'create', u'action':
 u'check-osds', u'osd': u'None'}",
 'osdmgmt_result': '{"status": "PROCESSED", "message": ["{\'Overall_Status\': \'PASS\',
 \'Result\': { ommitted for doc }}]}',
 'status': 'osdmgmt_completed',
 'updated_at': '2018-03-08 21:27:16+00:00',
 'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223'
 }
 }
```

Delete a completed osdmgmt operation

Verb	URI
DELETE	v1/osdmgmt/delete/?uuid=<uuid>

Example

JSON Request

```
DELETE /v1/osdmgmt/delete/?uuid=9c64ee52-bed5-4b69-91a2-d589411dd223
```

JSON Response

```
200 OK
Content-Type: application/json
{
 'error': 'None',
 'message': 'UUID 9c64ee52-bed5-4b69-91a2-d589411dd223 deleted from database',
 'status': 'deleted',
 'uuid': '9c64ee52-bed5-4b69-91a2-d589411dd223'
 }

}
```

Hardware Management Utility

Hardware Management Utility

REST wrapper to control the execution of or query information from the hardware validation utility.

Create a Validate Operation

Verb	URI
POST	/v1/hardwaremgmt/validate

JSON Request

```
POST /v1/hardwaremgmt/validate
'{"hwmgmt_request": {"command": "create",
                                    "action": "validate", "hosts": "None",
                                        "file": "None",
                                        "feature_list": "all",
                                        "uuid": ""}}'
                                        Feature_list is a comma separated list of valid features for the given
pod.
```

JSON Reponse

```
201 Created
Content-Type: application/json
{
 'action': 'validate',
 'created_at': '2018-03-08T22:01:22.195232+00:00',
 'hwmgmt_request': "{u'feature_list': u'all', u'command': u'create', u'file': None, u'action': u'validate',
u'hosts': None,
  u'uuid': '89e094d8-b246-4620-afca-ba3529385c'}",
 'hwmgmt_result': '',
 'status': 'not_run',
 'updated_at': 'None'
 }
```

Create a Validate Operation for Failure

Verb	URI
GET	/v1/hardwaremgmt/resolve_failures

JSON Request

```
POST /v1/hardwaremgmt/resolve_failures
 {
 "hwmgmt_request": { "command": "create",
                                          "action": "resolve-failures",
                                         "hosts": "None",
                     "file": "None",
                                         "feature_list": "all",
                                         "uuid": ""}
 }
 feature_list is a comma separated list of valid features for the given POD
```

JSON Response

```
201 Created
 Content-Type: application/json
 {

 "status": "not_run",
 "created_at": "2018-03-09T15:47:36.503712+00:00",

 "hwmgmt_request": "{u'feature_list': u'all', u'command': u'create',
 u'file': None, u'action': u'resolve-failures', u'hosts': None, u'uuid':
 '49dc1dc9-3170-4f68-b152-0f99bd19f7b1'}",
 "updated_at": "",
 "action": "resolve-failures",
 "hwmgmt_result": ""
 }
```

Create a Validate Operation

Verb	URI
GET	v1/hardwaremgmt/list

JSON Request

```
GET /v1/hardwaremgmt/list
```

JSON Response

```
200 OK
Content-Type: application/json
{'89e094d8-b246-4620-afca-ba3529385cac': {'action': 'validate',
                                                                                'created_at': '2018-03-08 22:
01:22+00:00',
                                                                                'feature_list': 'all',
                                                                                 'status':
'hardwaremgmt_completed',
                                                                                'uuid': '89e094d8-b246-4620-
afca-ba3529385cac'},
 '9f70e872-a888-439a-8661-2d2f36a4f4b1': {'action': 'validate',
                                                                                'created_at': '2018-03-08 20:
34:32+00:00',
                                                                                'feature_list': 'all',
                                                                                 'status':
'hardwaremgmt_completed',
                                         'uuid':'9f70e872-a888-439a-8661-2d2f36a4f4b1'}
 }
```

Show a completed hardwaremgmt operation

Verb	URI
GET	/v1/hardwaremgmt /show /?uuid=<uuid>

JSON Request

```
GET /v1/hardwaremgmt/show/?uuid=9f70e872-a888-439a-8661-2d2f36a4f4b
```

JSON Response

```
200 OK
 Content-Type: application/json
 {
 'action': 'validate',
 'created_at': '2018-03-08 20:34:32+00:00',
 'feature_list': 'all',

 'hwmgmt_request': "{u'feature_list': u'all', u'hosts': None, u'file':
None, u'action': u'validate', u'command': u'create', u'uuid':
'9f70e872-a888-439a-8661-2d2f36a4f4b1'}",
 'hwmgmt_result':
'{"status": "PROCESSED", "message": "Validate of all completed",
"results": {"status": "PASS", "results": [{"status": "PASS", "name":
"CIMC Firmware Version
 Check", "err": null}, {"status": "PASS", "name": "All Onboard LOM Ports Check", "err":
 null}, {"status": "PASS", "name": "PCIe Slot: HBA Status Check", "err": null}, {"status":
"PASS", "name": "Server Power Status Check", "err": null}, {"status":
"PASS", "name": "NFV Config Check", "err": null}, {"status": "PASS",
"name": "Physical Drives Check", "err":
 null}, {"status": "PASS",
"name": "PCIe Slot(s) OptionROM Check", "err": null}, {"status": "PASS",
 "name": "Intel Network Adapter Check", "err": null}]}}',
 'status': 'hardwaremgmt_completed',
 'updated_at': '2018-03-08 20:38:02+00:00',
 'uuid': '9f70e872-a888-439a-8661-2d2f36a4f4b1'
```

Delete a completed hardwaremgmt operation

Verb	URI
DELETE	/v1/hardwaremgmt/delete/?uuid=<uuid>

JSON Request

```
DELETE /v1/hardwaremgmt/delete/?uuid=9f70e872-a888-439a-8661-2d2f36a4f4b1
```

JSON Response

```
200 OK
Content-Type: application/json
{
 'error': 'None',
 'message': 'UUID 9f70e872-a888-439a-8661-2d2f36a4f4b1 deleted from database',
 'status': 'deleted',
 'uuid': '9f70e872-a888-439a-8661-2d2f36a4f4b1'
 }
```

Cisco VIM REST API Using curl for IPv4

Cisco VIM REST API Using curl for IPv4

Getting REST API Username & Password

Use the following configuration to get REST API Username and Password:

```
cat /opt/cisco/ui_config.json
 {
        "Kibana-Url": "http://172.31.231.17:5601",
        "RestAPI-Username": "admin",
        "RestAPI-Password": "***",
        "RestDB-Password": "***",
        "RestAPI-Url": "https://172.31.231.17:8445",
        "BuildNodeIP": "172.31.231.17"
 }
```

CCP APIs and Commands

Get CCP
Use the following command to get the list of CCP operations executed:

```
curl -i -X GET -H 'Content-Type: application/json' -H 'Authorization: ****' -H '
Accept: application/json' --cacert
/var/www/mercury/mercury-ca.crt https://172.29.84.207:8445/ccp
```

Response

```
HTTP/1.1 200 OK
 content-length: 360
 x-xss-protection: 1
 x-content-type-options: nosniff
 strict-transport-security: max-age=31536000 server: WSGIServer/0.1 Python/2.7.5
 cache-control: no-cache, no-store, must-revalidate, max-age=0 date: Mon, 01 Jul 2019 11:22:03 GMT
 x-frame-options: SAMEORIGIN content-type: application/json

 {u'ccps': {u'status': u'Success', u'ccp_result': {u'delete_tenant':
False}, u'created_at': u'2019-07-01T10:50:31+00:00', u'updated_at':
u'2019-07-01T11:06:25+00:00', u'op_name':
 u'CCP_Verify'}}
```

POST CCP Install:

Use the following command to initiate installation of CCP:

```
curl -i -X POST -H 'Content-Type: application/json' -H 'Authorization: ****' -H 'Accept:
 application/ --cacert /var/www/mercury/mercury-ca.crt -d 'None' https://172.29.84.207:8445/ccp
```

Response

```
HTTP/1.1 201 Created
 content-length: 133
 x-xss-protection: 1
 x-content-type-options: nosniff
 strict-transport-security: max-age=31536000 server: WSGIServer/0.1 Python/2.7.5
 cache-control: no-cache, no-store, must-revalidate, max-age=0 date: Mon, 01 Jul 2019 10:46:18 GMT
 x-frame-options: SAMEORIGIN
 content-type: application/json
 {u'status': u'ToRun', u'ccp_result': u'', u'created_at': u'2019-07-01T10:46:18.106517+00:00', u'updated_at':
None, u'op_name': u'CCP_Install'}
```

CCP Verify

Execute the following command to execute CCP Verify (Check tenant cluster status):

```
curl -i -X POST -H 'Content-Type: application/json' -H 'Authorization: ****' -H 'Accept:
 application/json' --cacert /var/www/mercury/mercury-ca.crt -d '{u'skip_delete': False}' https://172.29.84.207:
8445/ccp/ccp_verify
```

Response

```
HTTP/1.1 201 Created
 content-length: 158
 x-xss-protection: 1
 x-content-type-options: nosniff
 strict-transport-security: max-age=31536000 server: WSGIServer/0.1 Python/2.7.5
 cache-control: no-cache, no-store, must-revalidate, max-age=0 date: Mon, 01 Jul 2019 08:04:52 GMT
 x-frame-options: SAMEORIGIN content-type: application/json

 {u'status': u'ToRun', u'ccp_result': {u'delete_tenant': False}, u'created_at': u'2019-07-01T08:04:52.310432+00:
00', u'updated_at': None, u'op_name': u'CCP_Verify'}
```

Delete Control Cluster

Use the following command to delete the deployed control cluster:

```
curl -i -X DELETE -H 'Content-Type: application/json' -H 'Authorization: ****' -H 'Accept:
application/json' -H 'User-Agent: python-ciscovimclient' --cacert
/var/www/mercury/mercury-ca.crt -d '{u'delete_tenant': False, u'delete_control': True}' https://172.29.84.207:
8445/ccp
```

Response

```
HTTP/1.1 204 No Content
x-xss-protection: 1
x-content-type-options: nosniff
strict-transport-security: max-age=31536000
server: WSGIServer/0.1 Python/2.7.5
cache-control: no-cache, no-store, must-revalidate, max-age=0
date: Mon, 01 Jul 2019 11:29:59 GM
x-frame-options: SAMEORIGIN
```

Nodes APIs and Commands

List Nodes
Use the following curl command to get the node's status, power status, reboot status, and mtype information:

```
curl -i -X GET -u admin:**** -H 'Content-Type: application/json' -H 'Accept: application/json'
 --cacert /var/www/mercury/mercury-ca.crt https://172.31.231.17:8445/v1/nodes
```

Response

```
{"nodes": [{"status": ". . . . "name": "Store-2"}]}
```

Power OFF Nodes

To get the power off status of the nodes, use the below command:

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H 'Accept:
application/json' --cacert /var/www/mercury/mercury-ca.crt -d '{'status': 'PowerOff',
'force_op': False, 'name': '<Node UUID>'}'
 https://172.31.231.17:8445/v1/nodes/node_power_status
```

⚠ You can find the UUID of the node from the list nodes command.

Power ON Nodes

To get the power ON status of the nodes, use the following command:

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H 'Accept:
 application/json' --cacert /var/www/mercury/mercury-ca.crt -d '{'status': 'PowerOn', 'force_op': False,
'name': '<Node UUID>'}'
 https://172.31.231.17:8445/v1/nodes/node_power_status
```

⚠ You can find the UUID of the node from the list nodes command.

Power Status of Nodes

To get the Live status of the nodes, first send POST request to /v1/hwinfoAPI, and then place the GET request on v1/hwinfo/get_nodes_power_status after a minute approximately.
Run the below commands to send the POST request and get the power status:

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H 'Accept:
application/json' --cacert /var/www/mercury/mercury-ca.crt -d '{}'
https://172.31.231.17:8445/v1/hwinfo
curl -i -X GET -H 'Content-Type: application/json' -u admin:**** -H 'Accept: application/json'
 --cacert /var/www/mercury/mercury-ca.crt
https://172.31.231.17:8445/v1/hwinfo/get_nodes_power_status
```

Response

```
{'Store-3': {'intended_power_state': 'PowerOnSuccess', 'actual_power_state': 'on'},}}
```

Reboot Node

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H
'Accept: application/json' --cacert /var/www/mercury/mercury-ca.crt -d
'{'status': 'Reboot', 'force_op': False, 'name': '<Node UUID>'}' https://172.31.231.17:8445/v1/nodes
/node_power_status
```

⚠ You can find the UUID of the node from the list nodes command.

Reboot Status

Use the following two commands, to get the reboot status of the node:

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H
'Accept: application/json' --cacert /var/www/mercury/mercury-ca.crt
 -d 'None' https://172.31.231.17:8445/v1/nodes/reboot_status
 curl -i -X GET -H 'Content-Type: application/json' -u admin:**** -H 'Accept: application/json'
 --cacert /var/www/mercury/mercury-ca.crt https://172.31.231.17:8445/v1/nodes
```

List Openstack Configuration Command

```
curl -i -X GET -H 'Content-Type: application/json' -u admin:**** -H 'Accept: application/json'
 --cacert /var/www/mercury/mercury-ca.crt https://172.31.231.17:8445/v1/openstack_config
```

Response

```
{"KEYSTONE_VERBOSE_LOGGING": true, "GNOCCHI_VERBOSE_LOGGING": true, . . }
```

List Password Secrets

Command

```
curl -i -X GET -H 'Content-Type: application/json' -u admin:**** -H 'Accept: application/json'
 --cacert /var/www/mercury/mercury-ca.crt https://172.31.231.17:8445/v1/secrets
```

Response

```
{'HEAT_KEYSTONE_PASSWORD': '***', 'CINDER_KEYSTONE_PASSWORD': '***' . . }
```

Cluster Recovery

Command

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H 'Accept:
application/json' --cacert /var/www/mercury/mercury-ca.crt -d '{'action': {'cluster-recovery': {'run-disk-
checks': False}}}'
https://172.31.231.17:8445/v1/misc
```

Response

```
{'uuid': 'ae3be813-4fae-4510-8467-fab09ac60d2b', 'created_at':
'2019-01-07T08:17:01.229976+00:00', 'updated_at': None, 'operation_status':
'OperationScheduled', 'operation_logs': '', 'operation_name': {'cluster-recovery':
{'run-disk-checks': False}}}
```

NFVIMON

Command

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H
'Accept: application/json' --cacert /var/www/mercury/mercury-ca.crt -d
'{'action': {'nfvimon': True,
 'generate_ssh_keys': '****'}}' https://172.31.231.17:8445/v1/misc
```

Response

```
{'uuid': 'd33e534b-b8c7-41c9-b8e4-7b1befe528c8', 'created_at': '2019-01-07T08:27:56.925029+00:00',
'updated_at': None,
'operation_status': 'OperationScheduled', 'operation_logs': '',
'operation_name': {'generate_ssh_keys': '****', 'nfvimon': True}}
```

Last-Run-Status

Command

```
curl -i -X GET -H 'Content-Type: application/json' -H 'Authorization: ****' -H 'Accept: application/json' -H
'User-Agent: python-ciscovimclient' --cacert
 /var/www/mercury/mercury-ca.crt https://172.31.231.17:8445/v1/op_info
```

Response

```
{'created_at': '2019-01-07 08:27:56+00:00', 'updated_at': '2019-01-07 08:28:03+00:00',
 'reboot_required': False, 'update_status': False, 'current_op_logs':
 'https://172.31.231.17:8008/mercury/79c402d2-f156-4ba2-8f17-ec109401a538',
 'current_op_status': 'OperationRunning', 'insight_monitor_status':
 'Running', 'current_op_name': 'Generate_ssh_keys', 'current_op_monitor':
 'Runner_Op_Generate_ssh_keys'}
```

Reconfigure Regenerate Secrets

Command

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H 'Accept: application/json' --cacert /var
/www/mercury/mercury-ca.crt -d
'{'action': {'regenerate_secrets': '****', 'reconfigure': True}}' https://172.31.231.17:8445/v1/misc
```

Response

```
{'uuid': '83cf2700-275f-4c18-a900-96c36c4987aa', 'created_at': '2019-01-07T08:36:19.279425+00:00',
'updated_at': None, 'operation_status': 'OperationScheduled',
 'operation_logs': '',
 'operation_name': {'regenerate_secrets': '****',
 'reconfigure': True}}
```

Reconfigure Set Password

Command

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H 'Accept: application/json' --cacert /var
/www/mercury/mercury-ca.crt -d '{"action": {"setpassword": {"HAPROXY_PASSWORD": "*****"}, "reconfigure":
true}}' https://172.31.231.17:8445/v1/misc
```

Response

```
{"uuid": "16d89b9e-cadc-4467-b1d8-5a8a60171d90", "created_at": "2020-06-30T16:51:17.316126+00:00",
"updated_at": null, "operation_status": "OperationScheduled", "operation_logs": "", "operation_name": "{\"
setpassword\": {\"HAPROXY_PASSWORD\": \"****\"}, \"reconfigure\": true}"}
```

Reconfigure Set Openstack Configuration

Command

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H 'Accept:
 application/json' --cacert /var/www/mercury/mercury-ca.crt -d '{'action': {'reconfigure': True,
'setopenstackconfigs':{'GNOCCHI_VERBOSE_LOGGING': True}}}'
https://172.31.231.17:8445/v1/misc
```

Response

```
{'uuid': '5bbbeff7-76df-4444-a38a-8819a8b579e4', 'created_at':
 '2019-01-07T08:54:13.733254+00:00', 'updated_at': None,
 'operation_status': 'OperationScheduled', 'operation_logs': '',
 'operation_name': {'setopenstackconfigs':
 {'GNOCCHI_VERBOSE_LOGGING': True}, 'reconfigure': True}}
```

Reconfigure CIMC Password

1. List down the setupdata and find UUID of active setupdata using the following command:

   ```
   curl -i -X GET -H 'Content-Type: application/json' -u admin:**** -H
   'Accept: application/json' --cacert /var/www/mercury/mercury-ca.crt https://172.31.231.17:8445/v1
   /setupdata
   ```

   Response

2. Put the content of setupdata with new CIMC Password using the following command:

```
curl -i -X PUT -H 'Content-Type: application/json' -u admin:**** -H
'Accept: application/json' --cacert /var/www/mercury/mercury-ca.crt -d
'{'meta': {}, 'name': 'NEWSETUPDATA', 'jsondata':
{'external_lb_vip_address': '172.29.86.9' . . .}, 'uuid':
'3e97381e-4b1c-41a2-9af4-f970a1f1493a'}' https://172.31.231.17:8445/v1/setupdata/3e97381e-4b1c-41a2-9af4-
f970a1f1493a
```

3. Post on Misc API using the below command:

```
curl -i -X POST -H 'Content-Type: application/json' -u admin:**** -H
'Accept: application/json' --cacert /var/www/mercury/mercury-ca.crt -d
'{'action':
 {'reconfigure_cimc_password': True, 'reconfigure': True}}' https://172.31.231.17:8445/misc
```

Response

```
{'uuid': 'f00e1ae0-5674-4218-b1de-8995c9f9c546', 'created_at':
'2019-01-07T09:19:40.210121+00:00', 'updated_at': None, 'operation_status':
'OperationScheduled', 'operation_logs': '', 'operation_name':
{'reconfigure_cimc_password': '****', 'reconfigure': True}}
```

Cisco VIM REST API Using curl for IPv6

Cisco VIM REST API Using curl for IPv6

Prerequisites

1. You need to copy the certificates from the management node to local machine from where you would launch the APIs.
2. Create a folder in local machine and copy the certificates:

```
# mkdir ~/certificates
```

3. Copy REST API CA Certificates (for mercury commands)

```
# scp root@<Management Node>:/var/www/mercury/mercury-ca.crt ~/certificates
```

> ⚠ The key information that you need are br_api and cloud_api (external_lb_vip_ipv6_address).

4. For each POD, get the REST API credentials:

```
# cat /opt/cisco/ui_config.json
{
        "Kibana-Url": "http://[2001:420:293:2440:b696:91ff:fe22:2dd8]:5601",
        "RestAPI-Username": "admin",
        "RestAPI-Password": "cfb605586d50115333c8",
        "RestDB-Password": "744ebc5feee30b733ac8",
        "RestAPI-Url": "https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445",
        "BuildNodeIP": "2001:420:293:2440:b696:91ff:fe22:2dd8" -> br_api
}
```

Offline Validation using curl

1. Create offline validation test

Request

```
curl -g -i -X POST -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{"jsondata" : {<SetupData in JSON Format>}}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/v1/offlinevalidation
UUID is returned from request
```

Response

```
{"status": "NotValidated", "uuid": "2b8253f4-ad9f-4fbf-b224-a65bd210392a", "created_at":
"2019-02-28T18:02:36.808740+00:00", "updated_at": null, "jsondata": "{}"}
```

2. Get the offline validation test result:

   Request

```
Curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/v1/offlinevalidation/2b8253f4-ad9f-4fbf-b224-
a65bd210392a
```

   Response

```
{"status": "ValidationFailed", "uuid": "2b8253f4-ad9f-4fbf-b224-a65bd210392a",
"created_at": "2019-02-28T18:02:36+00:00", "updated_at": "2019-02-28T18:02:57+00:00",
"jsondata": ""}
```

Start New Installation

1. Create new setup date before starting new installation, for example:

```
curl -g -i -X POST -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{u'meta': {}, u'name': u'NEWSETUPDATA', u'jsondata': {<SetupData in
JSON Format>}}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/setupdata
```

2. To start the installation:
   Request

```
Curl -g -i -X POST -H 'Content-Type: application/json' admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{u'stages': u'vmtp', u'setupdata': u'8b0d4a46-c67f-4121-99af-
32fde52a82eb'}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/install
```

   Response

```
{u'uuid': u'6b02c2ab-441e-471a-9dcc-e771136186e1', u'setupdata':
u'8b0d4a46-c67f-4121-99af-32fde52a82eb', u'vmtpresult': u'', u'updated_at': None,
u'validationstatus': u'', u'currentstatus': u'Not Available', u'install_logs': u'',
u'stages': {u'baremetal': u'Scheduled', u'bootstrap': u'Scheduled', u'runtimevalidation':
u'Scheduled', u'ceph': u'Scheduled', u'orchestration': u'Scheduled', u'validation':
u'Scheduled', u'hostsetup': u'Scheduled', u'vmtp': u'Scheduled'}, u'created_at':
u'2019-03-05T05:22:30.986823+00:00'}
```

3. Get active setupdata with UUID after installation is started:

   Request

```
curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/setupdata
```

   Response

   It will return in the list format. You must check the status. The status can be Active, Installation Failed,or Installing.

```
{"setupdatas": [{"status": "Active", "uuid": "c5bc5fd9-6f4b-43e7-a61a-a9d409569943",
"jsondata": " {<Setupdata JSON>}", "meta": "{}", "name": "NEWSETUPDATA"}]}
```

4. Monitoring the installation using OP-information (current operation information):

   Request

   ```
   curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
   'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
   ~/certificates/mercury-ca.crt
   https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/op_info
   ```

   Response

   Check for the value of key insight_monitor_status. If it is **Running**, it indicates that the last operation is still in running state. Once the operation is completed, the value is either **Success/Failed** based on the result.

   ```
   {u'created_at': u'2019-02-25 18:15:00+00:00', u'updated_at': u'2019-02-25 18:15:00+00:00',
   u'reboot_required': False, u'update_status': False, u'current_op_logs':
   u'https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8008/mercury/ae3ed699-2ffe-4ae0-a8ab-83ef7fdce008',
   u'current_op_status': u'Running', u'insight_monitor_status': u'Running',
   u'current_op_name': u'install_op Orchestration', u'current_op_monitor':
   u'Install_Op_orchestration'}
   ```

   Sample output information after successful completion is given below:

   ```
   {"created_at": "2019-03-04 21:35:00+00:00", "updated_at": "2019-03-04 21:36:24+00:00",
   "reboot_required": false, "update_status": false, "current_op_logs": "",
   "current_op_status": "diskmgmt_completed", "insight_monitor_status": "Success",
   "current_op_name": "DiskMgmt", "current_op_monitor": ""}
   ```

Pod Management Operations

Prerequisites

Before performing any pod management operation, you need to update the setup data using PUT method.

Update setup data

1. Get the active setup data UUID using the install API

   Request

   ```
   curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
   'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
   ~/certificates/mercury-ca.crt
   https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/install
   ```

   Response

   ```
   {u'installs': {u'uuid': u'6b02c2ab-441e-471a-9dcc-e771136186e1', u'setupdata':
   u'8b0d4a46-c67f-4121-99af-32fde52a82eb', . . .}}
   ```

2. Send PUT request on setup data UUID

   ```
   curl -g -i -X PUT -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
   'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
   ~/certificates/mercury-ca.crt -d '{u'meta': {}, u'name': u'NEWSETUPDATA', u'jsondata':
   {<Setupdata JSON>}}'
   https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/setupdata/8b0d4a46-c67f-4121-99af-32fde52a82eb
   ```

   You can perform the following pod management operations:

- Add compute
- Add storage
- Remove compute
- Remove storage
- Replace controller

Add Compute

1. Add the node entry in setup data and update the setup data by following the steps given under prerequisites.
2. POST to nodes to add entry:

```
curl -g -i -X POST -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52
-H 'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{u'name': u'Compute-4'}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes/add_compute
```

Add Storage

1. Add the node entry in setup data and update the setup data by following the steps given under prerequisites.
2. POST to nodes to add entry:

```
curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{u'name': u'Store-4'}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes/add_storage
```

Remove Compute

1. List the nodes:

   Request

   ```
   curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
   'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
   ~/certificates/mercury-ca.crt https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes
   ```

   Response

   ```
   {"nodes": [{"status": "Active", "uuid": "1929776f-8b77-4b35-b55c-0abd6433b989",
   "setupdata": "8b0d4a46-c67f-4121-99af-32fde52a82eb", "node_data": "{\"rack_info\":
   {\"rack_id\": \"RackC\"}, \"cimc_info\": {\"cimc_ip\": \"172.29.172.81\"},
   \"management_ip\": \"21.0.0.13\"}", "updated_at": "2019-03-04T21:42:38+00:00",
   "reboot_required": "No", "mtype": " block_storage", "install":
   "6b02c2ab-441e-471a-9dcc-e771136186e1", "power_status": "PowerOnSuccess", "install_logs":
   "https://172.31.231.17:8008/mercury/071e79a5-b279-4628-bcf0-df168152cc42", "created_at":
   "2019-03-05T05:42:38+00:00", "name": "compute-3"}, . . . ]}
   ```

2. Remove the node entry in setup data and update the setup data by following the steps given under prerequisites.
3. Send delete request on nodes, to remove the storage node for that UUID:

```
curl -g -i -X DELETE -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52
-H 'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{u'force_op': False, u'name':
u'1929776f-8b77-4b35-b55c-0abd6433b989'}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes/remove_compute
```

Remove Storage

1. Get the UUID of the node to be removed by getting the list of nodes
   Request

```
curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes
```

Response


```
{"nodes": [{"status": "Active", "uuid": "0b7b2b6e-305c-48e0-b9f3-0ddb72bd3b3f",
"setupdata": "8b0d4a46-c67f-4121-99af-32fde52a82eb", "node_data": "{\"rack_info\":
{\"rack_id\": \"RackC\"}, \"cimc_info\": {\"cimc_ip\": \"172.29.172.81\"},
\"management_ip\": \"21.0.0.13\"}", "updated_at": "2019-03-04T21:42:38+00:00",
"reboot_required": "No", "mtype": " block_storage", "install":
"6b02c2ab-441e-471a-9dcc-e771136186e1", "power_status": "PowerOnSuccess", "install_logs":
"https://172.31.231.17:8008/mercury/071e79a5-b279-4628-bcf0-df168152cc42", "created_at":
"2019-03-05T05:42:38+00:00", "name": "Store-3"}, . . . ]}
```


2. Remove the node entry in setup data and update the setup data using steps mentioned in the prerequisites.
3. Send delete request on nodes, to remove the storage node for that UUID.

```
curl -g -i -X DELETE -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52
-H 'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{u'force_op': False, u'name':
u'0b7b2b6e-305c-48e0-b9f3-0ddb72bd3b3f'}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes/remove_storage
```

Replace controller

1. Get the UUID of the node to be removed by getting the list of nodes:

Request

```
curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes
```

Response


```
{"nodes": [{"status": "Active", "uuid": "79e43c4c-8cbd-4c81-8c22-3aec717298e9",
"setupdata": "8b0d4a46-c67f-4121-99af-32fde52a82eb", "node_data": "{\"rack_info\":
{\"rack_id\": \"RackC\"}, \"cimc_info\": {\"cimc_ip\": \"172.29.172.81\"},
\"management_ip\": \"21.0.0.13\"}", "updated_at": "2019-03-04T21:42:38+00:00",
"reboot_required": "No", "mtype": " control", "install":
"6b02c2ab-441e-471a-9dcc-e771136186e1", "power_status": "PowerOnSuccess", "install_logs":
"https://172.31.231.17:8008/mercury/071e79a5-b279-4628-bcf0-df168152cc42", "created_at":
"2019-03-05T05:42:38+00:00", "name": "gg34-10"}, . . . ]}
```


2. Remove the node entry in setup data and update the setup data using steps mentioned in the prerequisites.
3. Put nodes to replace entry:

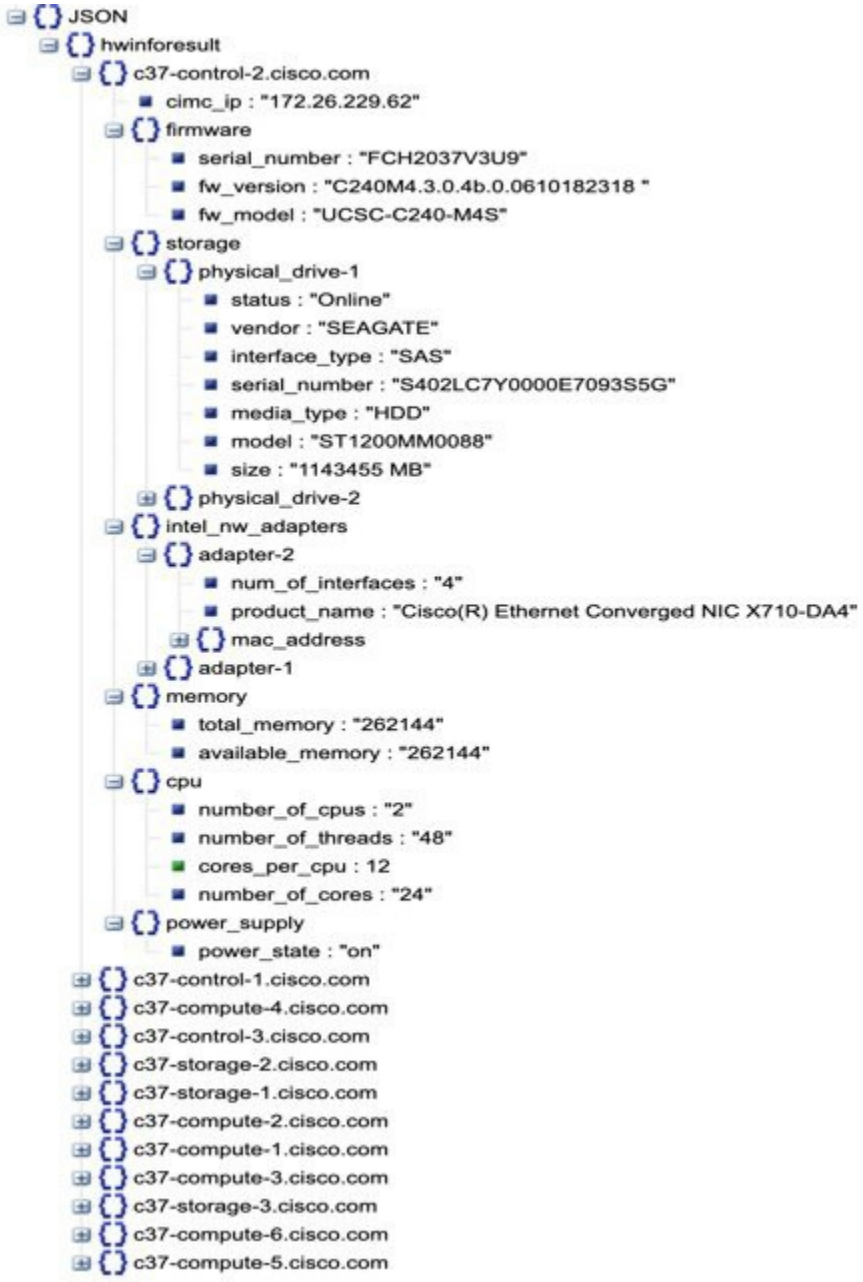
```
curl -g -i -X PUT -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt -d '{u'status': u'ToReplace', u'force_op': False, u'name':
u'gg34-10'}'
https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/nodes/79e43c4c-8cbd-4c81-8c22-3aec717298e9
```

Fetch Hardware Inventory

Request

```
curl -g -i -X GET -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H
'Accept: application/json' -H 'User-Agent: python-ciscovimclient' --cacert
~/certificates/mercury-ca.crt https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/v1/hwinfo
```

Response



Glance Image Upload

Use RestAPIs to upload and delete multiple images to/from the cloud.

Following are the REST API that are available for usage.

POST /upload

This API is responsible for uploading the image to respective Openstack Cloud.

JSON Payload

```
{
"podsip":[
"172.31.231.17",
"10.30.116.244",
],
"images":[
"Vodafone.iso",
"Rakuten.qcow2",
]
}
Response
{"Upload":true}
```

CURL Request

Following is an example Curl request

```
curl -s -k -X POST -d '{"upload": {"podsip":["172.23.105.218",
"172.29.85.78"],"images":["buildnode-internal-20606.iso","CentOS-7-x86_64-GenericCloud-1503.qcow2"]}}'
-H "Auth: <Token>" https://172.29.85.78:9001/upload
```

Delete /upload

This API is responsible for deleting the image from respective Openstack Cloud.

JSON Payload

```
{
"podsip":[
"172.31.231.17",
"10.30.116.244",
],
"images":[
"Vodafone.iso",
"Rakuten.qcow2",
]
}
```

CURL Request
Following is the example Curl request:

```
curl -s -k -X DELETE -d '{"upload": {"podsip":["172.23.105.218",
"172.29.85.78"],"images":["buildnode-internal-20606.iso","CentOS-7-x86_64-GenericCloud-1503.qcow2"]}}'
-H "Auth: <Token>" https://172.29.85.78:9001/upload
```

Response

```
{"Delete":true}
```

GET /upload

This API is responsible to get the image list from respective Openstack Cloud.

Following are the query string parameters to be passed with GET URL

1. odsip: It is a comma separated string which represents pod IPs, whose Openstack image list needs to be fetched.
2. images: It is a comma separated string which represents Openstack images whose status needs to be fetched.
3. refresh: Takes the value true or false. Used to get updated Openstack images list.

Following are the CURL request examples:

Example 1:

```
curl -s -k -H "Auth: <Token>" https://172.29.85.78:9001/upload
This gives the result of pods on which upload/get/delete operation are performed.
{
        "uploaded": {
                "172.29.85.78": {
                "opsinprogress": 0,
                "images": null,
                "error": ""
                                },
                "172.23.105.218": {
                "opsinprogress": 0,
                "images": null,
                "error": ""
                }
        }
}
```

Example 2:

```
curl -s -k -H "Auth: <Token>" https://172.29.85.78:9001/upload?"podsip=172.29.85.78"
{
        "uploaded": {
                "172.29.85.78": {
                "opsinprogress": 0,
                "images": [
                {
                        "OSStatus": "active",
                        "UploadStatus": "UploadSuccess",
                        "ErrStatus": "",
                        "ID": "c50284d7-191a-42ed-a289-9b52d19b9fd5",
                        "Name": "buildnode-internal-20606.iso"
                },
        {
                        "OSStatus": "active",
                        "UploadStatus": "UploadSuccess",
                        "ErrStatus": "",
                        "ID": "fee44efc-684e-46ac-aa89-b6e785faf1b4",
                        "Name": "CentOS-7-x86_64-GenericCloud-1503.qcow2"
                }
        ],
                "error": ""
                }
                }
}
```

Example 3:

```
curl -s -k -H "Auth: <Token>"
https://172.29.85.78:9001/upload?"podsip=172.29.85.78&refresh=true"
{
        "uploaded": {
                "172.29.85.78": {
                "opsinprogress": 1,
                "images": null,
                "error": ""
},
}
```

Example 4:

```
curl -s -k -H "Auth: <Token>" https://172.29.85.78:9001/upload?"podsip=172.29.85.78&
images=buildnode-internal-20606.iso"
{
        "uploaded": {
        "172.29.85.78": {
        "opsinprogress": 0,
        "images": [
        {
                "OSStatus": "active",
                "UploadStatus": "UploadSuccess",
                "ErrStatus": "",
                "ID": "c50284d7-191a-42ed-a289-9b52d19b9fd5",
                "Name": "buildnode-internal-20606.iso"
        }
        ],
        "error": ""
        }
}
}
```

Management Node VMs Lifecycle

Life-cycle Management of Management Node VM via Rest API

To help meet the vision of complete automation, a set of Rest-APIs are developed to manage the deployment of the management node VMs.

Prerequisites

1. Copy the certificates from the management node to local machine from where you launch the APIs.
2. Create a folder in local machine and copy the certificates:

```
# mkdir ~/certificates
```

3. Copy the REST API CA certificates (for mercury commands)

```
# scp root@<Management Node>:/var/www/mercury/mercury-ca.crt ~/certificates
```

   The key information needed are br_api and cloud_api (external_lb_vip_ipv6_address).
4. For the pod hosting the management node VMs, get the REST API credentials:

```
# cat /opt/cisco/ui_config.json
{
    "Kibana-Url": "http://[2001:420:293:2440:b696:91ff:fe22:2dd8]:5601",
    "RestAPI-Username": "admin",
    "RestAPI-Password": "cfb605586d50115333c8",
    "RestDB-Password": "744ebc5feee30b733ac8",
    "RestAPI-Url": "https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445",
    "BuildNodeIP": "2001:420:293:2440:b696:91ff:fe22:2dd8" -> br_api
}
```

Request to launch All Management Node VMs (defined in setup_data)

URL

```
POST /v1/central_vm
```

Request

```
curl -g -i -X POST -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H 'Accept: application
/json' -H 'User-Agent: python-ciscovimclient' --cacert ~/certificates/mercury-ca.crt -d '{"name": "deploy_vms",
"jsondata": {"FLAVORS": {"vcpus": 8, "ram": 24576, "name": "cvim-mgmt.8x24-nonlocal"}, "KEYPAIRS": "****",
"CENTRAL_MGMT_USER_INFO": {"username": "cental_mgmt", "password": "****"}, "PODTYPE": "MGMT_CENTRAL", "IMAGES":
{"file_location": "/root/cm_images/buildnode-internal-24832.qcow2", "name": "cvim-mgmt-24832"}, "TIMEZONE": "US
/Pacific", "SERVERS_IN_VMS": {"name": "shardev1", "cvimadmin_password_hash": "****", "nics": {"fixed_ips":
{"subnet": "v6_api_subnet", "ipaddress": "2001:420:293:243c:10:8:98:4"}, "network_name": "prov-net-api-1230",
"name": "sc-br_api"}, "image": "cvim-mgmt-24832", "node_type": "management", "keypair": "****", "flavor": "cvim-
mgmt.8x24-nonlocal", "disk_vol_size": 512}, "NETWORKS": {"subnets": {"name": "v6_api_subnet",
"dns_nameservers": "2001:420:68d:4001::a", "range": "2001:420:293:243c::500", "ip_version": 6, "network_cidr":
"2001:420:293:243c::/64", "gateway": "2001:420:293:243c::2"}, "segment": "api", "name": "prov-net-api-1230",
"vlan_id": 1230}}, "launch_all": True}' https://[2001:420:293:2440:b696:91ff:fe22:2dd8]:8445/central_vm
```

⚠ You can change the name of the deployment. By default, it is *deploy_vms*.

Response


```
 {"status": "ToRun", "delete_vms": "", "add_vms": "", "name": "deploy_vms", "created_at": "2020-03-04T05:59:
00.492525+00:00", u"pdated_at": "2020-03-04T05:59:00.492528+00:00", "jsondata": {"FLAVORS": {"vcpus": 8, "ram":
24576, "name": "cvim-mgmt.8x24-nonlocal"}, "KEYPAIRS": "****", "CENTRAL_MGMT_USER_INFO": {u"sername":
"cental_mgmt", "password": "****"}, "PODTYPE": "MGMT_CENTRAL", "IMAGES": {"file_location": "/root/cm_images
/buildnode-internal-24832.qcow2", "name": "cvim-mgmt-24832"}, "TIMEZONE": u"S/Pacific", "SERVERS_IN_VMS":
{"name": "shardev1", "cvimadmin_password_hash": "****", "nics": {"fixed_ips": {"subnet": "v6_api_subnet",
"ipaddress": "2001:420:293:243c:10:8:98:4"}, "network_name": "prov-net-api-1230", "name": "sc-br_api"},
"image": "cvim-mgmt-24832", "node_type": "management", "keypair": "****", "flavor": "cvim-mgmt.8x24-nonlocal",
"disk_vol_size": 512}, "NETWORKS": {"subnets": {"name": "v6_api_subnet", "dns_nameservers": "2001:420:68d:4001::
a", "range": "2001:420:293:243c::500", "ip_version": 6, "network_cidr": "2001:420:293:243c::/64", "gateway":
"2001:420:293:243c::2"}, "segment": "api", "name": "prov-net-api-1230", "vlan_id": 1230}}, "vms_info": "",
"current_op_logs": "", "list_vms": False, "clean_all": False, "current_op_name": "Launching All VMs",
"launch_all": True}
```


⚠ To monitor the status of the current request, see *Monitoring Ongoing Deployment* section below.

Delete All Management Node VMs

URL

```
PUT /v1/central_vm/<Deployment Name>
```

Request

```
curl -g -i -X PUT -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H 'Accept: application
/json' -H 'User-Agent: python-ciscovimclient' --cacert ~/certificates/mercury-ca.crt -d '{"clean_all": True,
"name": "deploy_vms", "jsondata": {"FLAVORS": {"vcpus": 8, "ram": 24576, "name": "cvim-mgmt.8x24-nonlocal"},
"KEYPAIRS": "****", "CENTRAL_MGMT_USER_INFO": {"username": "cental_mgmt", "password": "****"}, "PODTYPE":
"MGMT_CENTRAL", "IMAGES": {"file_location": "/root/cm_images/buildnode-internal-24832.qcow2", "name": "cvim-
mgmt-24832"}, "TIMEZONE": "US/Pacific", "NETWORKS": {"subnets": {"name": "v6_api_subnet", "dns_nameservers":
"2001:420:68d:4001::a", "range": "2001:420:293:243c::500", "ip_version": 6, "network_cidr": "2001:420:293:243c::
/64", "gateway": "2001:420:293:243c::2"}, "segment": "api", "name": "prov-net-api-1230", "vlan_id": 1230}}}'
https://[2001:420:293:2433:172:29:85:106]:8445/central_vm/deploy_vms
```

Response


```
{"status": "ToRun", "delete_vms": "", "add_vms": "", "name": "deploy_vms", "created_at": "2020-03-04T05:59:
00+00:00", "updated_at": "2020-03-04T05:59:27+00:00", "jsondata": {"FLAVORS": {"vcpus": 8, "ram": 24576,
"name": "cvim-mgmt.8x24-nonlocal"}, "KEYPAIRS": "****", "CENTRAL_MGMT_USER_INFO": {"username": "cental_mgmt",
"password": "****"}, "PODTYPE": "MGMT_CENTRAL", "IMAGES": {"file_location": "/root/cm_images/buildnode-internal-
24832.qcow2", "name": "cvim-mgmt-24832"}, "TIMEZONE": "US/Pacific", "NETWORKS": {"subnets": {"name":
"v6_api_subnet", "dns_nameservers": "2001:420:68d:4001::a", "range": "2001:420:293:243c::500", "ip_version": 6,
"network_cidr": "2001:420:293:243c::/64", "gateway": "2001:420:293:243c::2"}, "segment": "api", "name": "prov-
net-api-1230", "vlan_id": 1230}}, "vms_info": "", "current_op_logs": "", "list_vms": False, "clean_all": True,
"current_op_name": "Clean Up All Resources", "launch_all": False}
```


⚠ To monitor the status of the current request, see *Monitoring Ongoing Deployment* section below.

Delete Selected Management Node VMs

URL

```
PUT /v1/central_vm/<Deployment Name>
```

Request

```
curl -g -i -X PUT -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H 'Accept: application
/json' -H 'User-Agent: python-ciscovimclient' --cacert ~/certificates/mercury-ca.crt -d '{"delete_vms":
vm_dev1, vm_dev2", "name": "deploy_vms", "jsondata": {"FLAVORS": {"vcpus": 8, "ram": 24576, "name": "cvim-mgmt.
8x24-nonlocal"}, "KEYPAIRS": "****", "CENTRAL_MGMT_USER_INFO": {"username": "cental_mgmt", "password": "****"},
"PODTYPE": "MGMT_CENTRAL", "IMAGES": {"file_location": "/root/cm_images/buildnode-internal-24832.qcow2",
"name": "cvim-mgmt-24832"}, "TIMEZONE": "US/Pacific", "SERVERS_IN_VMS": {"name": "shardev1",
"cvimadmin_password_hash": "****", "nics": {"fixed_ips": {"subnet": "v6_api_subnet", "ipaddress": "2001:420:293:
243c:10:8:98:4"}, "network_name": "prov-net-api-1230", "name": "sc-br_api"}, "image": "cvim-mgmt-24832",
"node_type": "management", "keypair": "****", "flavor": "cvim-mgmt.8x24-nonlocal", "disk_vol_size": 512},
"NETWORKS": {"subnets": {"name": "v6_api_subnet", "dns_nameservers": "2001:420:68d:4001::a", "range": "2001:420:
293:243c::500", "ip_version": 6, "network_cidr": "2001:420:293:243c::/64", "gateway": "2001:420:293:243c::2"},
"segment": "api", "name": "prov-net-api-1230", "vlan_id": 1230}}}' https://[2001:420:293:2433:172:29:85:106]:
8445/central_vm/deploy_vms
```

Response

```
{"status": "ToRun", "delete_vms": "chandradev1", "add_vms": "", "name": "deploy_vms", "created_at": "2020-03-
04T05:59:00+00:00", "updated_at": "2020-03-04T09:37:45+00:00", "jsondata": {"FLAVORS": {"vcpus": 8, "ram":
24576, "name": "cvim-mgmt.8x24-nonlocal"}, "KEYPAIRS": "****", "CENTRAL_MGMT_USER_INFO": {"username":
"cental_mgmt", "password": "****"}, "PODTYPE": "MGMT_CENTRAL", "IMAGES": {"file_location": "/root/cm_images
/buildnode-internal-24832.qcow2", "name": "cvim-mgmt-24832"}, "TIMEZONE": "US/Pacific", "SERVERS_IN_VMS":
{"name": "shardev1", "cvimadmin_password_hash": "****", "nics": {"fixed_ips": {"subnet": "v6_api_subnet",
"ipaddress": "2001:420:293:243c:10:8:98:4"}, "network_name": "prov-net-api-1230", "name": "sc-br_api"},
"image": "cvim-mgmt-24832", "node_type": "management", "keypair": "****", "flavor": "cvim-mgmt.8x24-nonlocal",
"disk_vol_size": 512}, "NETWORKS": {"subnets": {"name": "v6_api_subnet", "dns_nameservers": "2001:420:68d:4001::
a", "range": "2001:420:293:243c::500", "ip_version": 6, "network_cidr": "2001:420:293:243c::/64", "gateway":
"2001:420:293:243c::2"}, "segment": "api", "name": "prov-net-api-1230", "vlan_id": 1230}}, "vms_info": "",
"current_op_logs": "", "list_vms": False, "clean_all": False, "current_op_name": "Deleting VMs: vm_dev1,
vm_dev2", "launch_all": False}
```

⚠ To monitor the status of the current request, see *Monitoring Ongoing Deployment* section below.

Add New Management Node VMs to Existing Deployment

URL

```
PUT /v1/central_vm/<Deployment Name
```

Request

```
curl -g -i -X PUT -H 'Content-Type: application/json' -u admin:46d13357ef15e5482b52 -H 'Accept: application
/json' -H 'User-Agent: python-ciscovimclient' --cacert ~/certificates/mercury-ca.crt -d '{"add_vms": "vm_dev1",
"name": "deploy_vms", "jsondata": {"FLAVORS": [{"vcpus": 8, "ram": 24576, "name": "cvim-mgmt.8x24-nonlocal"}],
"KEYPAIRS": [{"public_key_file": "/root/.ssh/id_rsa.pub", "name": "mgmt_vm_keypair"}],
"CENTRAL_MGMT_USER_INFO": {"username": "cental_mgmt", "password": "Lab1234!"}, "PODTYPE": "MGMT_CENTRAL",
"IMAGES": [{"file_location": "/root/cm_images/buildnode-internal-24832.qcow2", "name": "cvim-mgmt-24832"}],
"TIMEZONE": "US/Pacific", "SERVERS_IN_VMS": [{"name": "cmdev1", "cvimadmin_password_hash": "$6$WCVKuxRf.
LQdBNHT$HfgmirX/DMx6KNlS7VblGKms6UUrq4r8DAdQ/xHqbwMtg9ReHNSKGiap1hR0EPIbhWlYGAbxfhV8OxYRt1sZu1", "nics":
[{"network_name": "prov-net-mgmt-1229", "fixed_ips": [{"subnet": "v4_mgmt_subnet", "ipaddress": "10.8.97.10"},
{"subnet": "v6_mgmt_subnet", "ipaddress": "2001:420:293:243b:10:8:97:10"}], "name": "cmdev1-br_mgmt"},
{"network_name": "prov-net-api-1230", "fixed_ips": [{"subnet": "v4_api_subnet", "ipaddress": "10.8.98.10"},
{"subnet": "v6_api_subnet", "ipaddress": "2001:420:293:243c:10:8:98:2"}], "name": "cmdev1-br_api"}], "image":
"cvim-mgmt-24832", "keypair": "mgmt_vm_keypair", "node_type": "management", "flavor": "cvim-mgmt.8x24-
nonlocal", "disk_vol_size": 512}, {"name": "vm_dev1", "cvimadmin_password_hash": "$6$WCVKuxRf.LQdBNHT$HfgmirX
/DMx6KNlS7VblGKms6UUrq4r8DAdQ/xHqbwMtg9ReHNSKGiap1hR0EPIbhWlYGAbxfhV8OxYRt1sZu1", "nics": [{"network_name":
"prov-net-mgmt-1229", "fixed_ips": [{"subnet": "v4_mgmt_subnet", "ipaddress": "10.8.97.11"}, {"subnet":
"v6_mgmt_subnet", "ipaddress": "2001:420:293:243b:10:8:97:11"}], "name": "cg-br_mgmt"}, {"network_name": "prov-
net-api-1230", "fixed_ips": [{"subnet": "v4_api_subnet", "ipaddress": "10.8.98.11"}, {"subnet":
"v6_api_subnet", "ipaddress": "2001:420:293:243c:10:8:98:3"}], "name": "cg-br_api"}], "image": "cvim-mgmt-
24832", "keypair": "mgmt_vm_keypair", "node_type": "management", "flavor": "cvim-mgmt.8x24-nonlocal",
"disk_vol_size": 512}, {"name": "shardev1", "cvimadmin_password_hash": "$6$WCVKuxRf.LQdBNHT$HfgmirX
/DMx6KNlS7VblGKms6UUrq4r8DAdQ/xHqbwMtg9ReHNSKGiap1hR0EPIbhWlYGAbxfhV8OxYRt1sZu1", "nics": [{"network_name":
"prov-net-mgmt-1229", "fixed_ips": [{"subnet": "v4_mgmt_subnet", "ipaddress": "10.8.97.12"}, {"subnet":
"v6_mgmt_subnet", "ipaddress": "2001:420:293:243b:10:8:97:12"}], "name": "sc-br_mgmt"}, {"network_name": "prov-
net-api-1230", "fixed_ips": [{"subnet": "v4_api_subnet", "ipaddress": "10.8.98.12"}, {"subnet":
"v6_api_subnet", "ipaddress": "2001:420:293:243c:10:8:98:4"}], "name": "sc-br_api"}], "image": "cvim-mgmt-
24832", "keypair": "mgmt_vm_keypair", "node_type": "management", "flavor": "cvim-mgmt.8x24-nonlocal",
"disk_vol_size": 512}], "NETWORKS": [{"subnets": [{"range": ["10.8.97.5", "10.8.97.199"], "name":
"v4_mgmt_subnet", "ip_version": 4, "network_cidr": "10.8.97.0/24", "dns_nameservers": ["171.70.168.183"],
"gateway": "10.8.97.2"}, {"range": ["2001:420:293:243b::100", "2001:420:293:243b::500"], "name":
"v6_mgmt_subnet", "ip_version": 6, "network_cidr": "2001:420:293:243b::/64", "dns_nameservers": ["2001:420:68d:
4001::a"], "gateway": "2001:420:293:243b::2"}], "segment": "management", "name": "prov-net-mgmt-1229",
"vlan_id": 1229}, {"subnets": [{"range": ["10.8.98.5", "10.8.98.199"], "name": "v4_api_subnet", "ip_version":
4, "network_cidr": "10.8.98.0/24", "dns_nameservers": ["171.70.168.183"], "gateway": "10.8.98.2"}, {"range":
["2001:420:293:243c::100", "2001:420:293:243c::500"], "name": "v6_api_subnet", "ip_version": 6, "network_cidr":
"2001:420:293:243c::/64", "dns_nameservers": ["2001:420:68d:4001::a"], "gateway": "2001:420:293:243c::2"}],
"segment": "api", "name": "prov-net-api-1230", "vlan_id": 1230}]}
```

Response

```
{"status": "ToRun", "delete_vms": "", "add_vms": "vm_dev1", "name": "deploy_vms", "created_at": "2020-03-04T05:
59:00+00:00", "updated_at": "2020-03-04T09:51:40+00:00", "jsondata": {"FLAVORS": {"vcpus": 8, "ram": 24576,
"name": "cvim-mgmt.8x24-nonlocal"}, "KEYPAIRS": "****", "CENTRAL_MGMT_USER_INFO": {"username": "cental_mgmt",
"password": "****"}, "PODTYPE": "MGMT_CENTRAL", "IMAGES": {"file_location": "/root/cm_images/buildnode-internal-
24832.qcow2", "name": "cvim-mgmt-24832"}, "TIMEZONE": "US/Pacific", "SERVERS_IN_VMS": {"name": "shardev1",
"cvimadmin_password_hash": "****", "nics": {"fixed_ips": {"subnet": "v6_api_subnet", "ipaddress": "2001:420:293:
243c:10:8:98:4"}, "network_name": "prov-net-api-1230", "name": "sc-br_api"}, "image": "cvim-mgmt-24832",
"node_type": "management", "keypair": "****", "flavor": "cvim-mgmt.8x24-nonlocal", "disk_vol_size": 512},
"NETWORKS": {"subnets": {"name": "v6_api_subnet", "dns_nameservers": "2001:420:68d:4001::a", "range": "2001:420:
293:243c::500", "ip_version": 6, "network_cidr": "2001:420:293:243c::/64", "gateway": "2001:420:293:243c::2"},
"segment": "api", "name": "prov-net-api-1230", "vlan_id": 1230}}, "vms_info": "", "current_op_logs": "",
"list_vms": False, "clean_all": False, "current_op_name": "Adding VMs: chandradev1", "launch_all": False}
```

⚠ To monitor the status of the current request, see *Monitoring Ongoing Deployment* section below.

Monitoring On-going Deployment

Use the following method to monitor any ongoing operation related to a given deployment.

URL

```
GET /v1/central_vm/status?name=<Deployment Name>
```

Request

```
curl -g -i -X GET -H 'Content-Type: application/json' -u  admin:46d13357ef15e5482b52 -H 'Accept: application
/json' -H 'User-Agent: python-ciscovimclient' --cacert ~/certificates/mercury-ca.crt  https://[2001:420:293:
2440:b696:91ff:fe22:2dd8]:8445/ central_vm/status?name=deploy_vms
```

Response

```
{"status": "ToRun", "current_op_name": "Launching All VMs", "current_op_logs": "", "name": "deploy_vms"}
```

Response with Log Files

```
{"status": "Running", "current_op_name": "Launching All VMs", "current_op_logs": "https://[2001:420:293:2433:
172:29:85:106]:8008/mercury/central_vm_deploy2020-03-03_21-59-04.log", "name": "deploy_vms"}
```

Possible values for *Status*

- ToRun
- Running
- Success
- Failed

Request to List All Management Node VMs

URL

```
GET /v1/central_vm/vms_info?name=deploy_vms
```

Request

```
curl -g -i -X GET -H 'Content-Type: application/json' -u  admin:46d13357ef15e5482b52 -H 'Accept: application
/json' -H 'User-Agent: python-ciscovimclient' --cacert ~/certificates/mercury-ca.crt https://[2001:420:293:2433:
172:29:85:106]:8445/central_vm/vms_info?name=deploy_vms
```

Response

```
{"vms_info": [{"Status": "ACTIVE", "Name": "shardev1", "Networks": "prov-net-mgmt-1229=10.8.97.12, 2001:420:293:
243b:10:8:97:12; prov-net-api-1230=10.8.98.12, 2001:420:293:243c:10:8:98:4"}, {"Status": "ACTIVE", "Name":
"vmdev1", "Networks": "prov-net-mgmt-1229=10.8.97.11, 2001:420:293:243b:10:8:97:11; prov-net-api-1230=10.
8.98.11, 2001:420:293:243c:10:8:98:3"}, {"Status": "ACTIVE", "Name": "cmdev1", "Networks": "prov-net-mgmt-
1229=10.8.97.10, 2001:420:293:243b:10:8:97:10; prov-net-api-1230=10.8.98.10, 2001:420:293:243c:10:8:98:2"}]}
```

Fetch Status of Last Deployment Request

URL

```
GET /v1/central_vm
```

Request

```
curl -g -i -X GET -H 'Content-Type: application/json' -u  admin:46d13357ef15e5482b52 -H 'Accept: application
/json' -H 'User-Agent: python-ciscovimclient' --cacert ~/certificates/mercury-ca.crt https://[2001:420:293:2433:
172:29:85:106]:8445/central_vm
```

Response


```
{
  "centralVMs": [
    {
      "add_vms": "chandradev1",
      "current_op_name": "Adding VMs: chandradev1",
      "launch_all": false,
      "clean_all": false,
      "list_vms": false,
      "status": "Failed",
      "delete_vms": "",
      "name": "deploy_vms",
      "created_at": "2020-03-04T05:59:00+00:00",
      "updated_at": "2020-03-05T06:32:40+00:00",
      "jsondata": "{\"FLAVORS\": [{\"vcpus\": 8, \"ram\": 24576, \"name\": \"cvim-mgmt.8x24-nonlocal\"}], \"
KEYPAIRS\": [{\"public_key_file\": \"/root/.ssh/id_rsa.pub\", \"name\": \"mgmt_vm_keypair\"}], \"
CENTRAL_MGMT_USER_INFO\": {\"username\": \"cental_mgmt\", \"password\": \"Lab1234!\"}, \"PODTYPE\": \"
MGMT_CENTRAL\", \"IMAGES\": [{\"file_location\": \"/root/cm_images/buildnode-internal-24832.qcow2\", \"name\":
\"cvim-mgmt-24832\"}], \"TIMEZONE\": \"US/Pacific\", \"SERVERS_IN_VMS\": [{\"name\": \"cmdev1\", \"
cvimadmin_password_hash\": \"$6$WCVKuxRf.LQdBNHT$HfgmirX/DMx6KNlS7VblGKms6UUrq4r8DAdQ
/xHqbwMtg9ReHNSKGiap1hR0EPIbhWlYGAbxfhV8OxYRt1sZu1\", \"nics\": [{\"network_name\": \"prov-net-mgmt-1229\", \"
fixed_ips\": [{\"subnet\": \"v4_mgmt_subnet\", \"ipaddress\": \"10.8.97.10\"}, {\"subnet\": \"v6_mgmt_subnet\",
\"ipaddress\": \"2001:420:293:243b:10:8:97:10\"}], \"name\": \"cmdev1-br_mgmt\"}, {\"network_name\": \"prov-net-
api-1230\", \"fixed_ips\": [{\"subnet\": \"v4_api_subnet\", \"ipaddress\": \"10.8.98.10\"}, {\"subnet\": \"
v6_api_subnet\", \"ipaddress\": \"2001:420:293:243c:10:8:98:2\"}], \"name\": \"cmdev1-br_api\"}], \"image\": \"
cvim-mgmt-24832\", \"keypair\": \"mgmt_vm_keypair\", \"node_type\": \"management\", \"flavor\": \"cvim-mgmt.
8x24-nonlocal\", \"disk_vol_size\": 512}, {\"name\": \"chandradev1\", \"cvimadmin_password_hash\":
\"$6$WCVKuxRf.LQdBNHT$HfgmirX/DMx6KNlS7VblGKms6UUrq4r8DAdQ/xHqbwMtg9ReHNSKGiap1hR0EPIbhWlYGAbxfhV8OxYRt1sZu1\",
\"nics\": [{\"network_name\": \"prov-net-mgmt-1229\", \"fixed_ips\": [{\"subnet\": \"v4_mgmt_subnet\", \"
ipaddress\": \"10.8.97.11\"}, {\"subnet\": \"v6_mgmt_subnet\", \"ipaddress\": \"2001:420:293:243b:10:8:97:
11\"}], \"name\": \"cg-br_mgmt\"}, {\"network_name\": \"prov-net-api-1230\", \"fixed_ips\": [{\"subnet\": \"
v4_api_subnet\", \"ipaddress\": \"10.8.98.11\"}, {\"subnet\": \"v6_api_subnet\", \"ipaddress\": \"2001:420:293:
243c:10:8:98:3\"}], \"name\": \"cg-br_api\"}], \"image\": \"cvim-mgmt-24832\", \"keypair\": \"
mgmt_vm_keypair\", \"node_type\": \"management\", \"flavor\": \"cvim-mgmt.8x24-nonlocal\", \"disk_vol_size\":
512}, {\"name\": \"shardev1\", \"cvimadmin_password_hash\": \"$6$WCVKuxRf.LQdBNHT$HfgmirX
/DMx6KNlS7VblGKms6UUrq4r8DAdQ/xHqbwMtg9ReHNSKGiap1hR0EPIbhWlYGAbxfhV8OxYRt1sZu1\", \"nics\": [{\"
network_name\": \"prov-net-mgmt-1229\", \"fixed_ips\": [{\"subnet\": \"v4_mgmt_subnet\", \"ipaddress\": \"
10.8.97.12\"}, {\"subnet\": \"v6_mgmt_subnet\", \"ipaddress\": \"2001:420:293:243b:10:8:97:12\"}], \"name\": \"
sc-br_mgmt\"}, {\"network_name\": \"prov-net-api-1230\", \"fixed_ips\": [{\"subnet\": \"v4_api_subnet\", \"
ipaddress\": \"10.8.98.12\"}, {\"subnet\": \"v6_api_subnet\", \"ipaddress\": \"2001:420:293:243c:10:8:98:4\"}],
\"name\": \"sc-br_api\"}], \"image\": \"cvim-mgmt-24832\", \"keypair\": \"mgmt_vm_keypair\", \"node_type\": \"
management\", \"flavor\": \"cvim-mgmt.8x24-nonlocal\", \"disk_vol_size\": 512}], \"NETWORKS\": [{\"subnets\":
[{\"range\": [\"10.8.97.5\", \"10.8.97.199\"], \"name\": \"v4_mgmt_subnet\", \"ip_version\": 4, \"
network_cidr\": \"10.8.97.0/24\", \"dns_nameservers\": [\"171.70.168.183\"], \"gateway\": \"10.8.97.2\"}, {\"
range\": [\"2001:420:293:243b::100\", \"2001:420:293:243b::500\"], \"name\": \"v6_mgmt_subnet\", \"
ip_version\": 6, \"network_cidr\": \"2001:420:293:243b::/64\", \"dns_nameservers\": [\"2001:420:68d:4001::a\"],
\"gateway\": \"2001:420:293:243b::2\"}], \"segment\": \"management\", \"name\": \"prov-net-mgmt-1229\", \"
vlan_id\": 1229}, {\"subnets\": [{\"range\": [\"10.8.98.5\", \"10.8.98.199\"], \"name\": \"v4_api_subnet\", \"
ip_version\": 4, \"network_cidr\": \"10.8.98.0/24\", \"dns_nameservers\": [\"171.70.168.183\"], \"gateway\": \"
10.8.98.2\"}, {\"range\": [\"2001:420:293:243c::100\", \"2001:420:293:243c::500\"], \"name\": \"
v6_api_subnet\", \"ip_version\": 6, \"network_cidr\": \"2001:420:293:243c::/64\", \"dns_nameservers\": [\"2001:
420:68d:4001::a\"], \"gateway\": \"2001:420:293:243c::2\"}], \"segment\": \"api\", \"name\": \"prov-net-api-
1230\", \"vlan_id\": 1230}]}",
      "vms_info": "",
      "current_op_logs": "https://[2001:420:293:2433:172:29:85:106]:8008/mercury/central_vm_deploy2020-03-04_22-
32-25.log"
    }
  ]
}
```


Delete Central Management Deployment

URL

```
DELETE /v1/central_vm/<Deployment Name>
```

Request

```
# curl -i -X DELETE -s -u admin:10e897312b8c606d3899 --cacert /var/www/mercury/mercury-ca.crt https://172.
29.85.78:8445/v1/central_vm/gg34_vms
```

Response

```
HTTP/1.1 204 No Content
Date: Fri, 16 Oct 2020 10:08:15 GMT
Server: WSGIServer/0.2 CPython/3.6.8
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
CVIM-API-Minimum-Version: 2.4.0
CVIM-API-Maximum-Version: 4.0.0
CVIM-API-Version: 2.4.0
vary: CVIM-API-Version
```

Monitoring Performance

Monitoring Cisco VIM Performance

The following topics tell you how to display logs to monitor Cisco VIM performance.

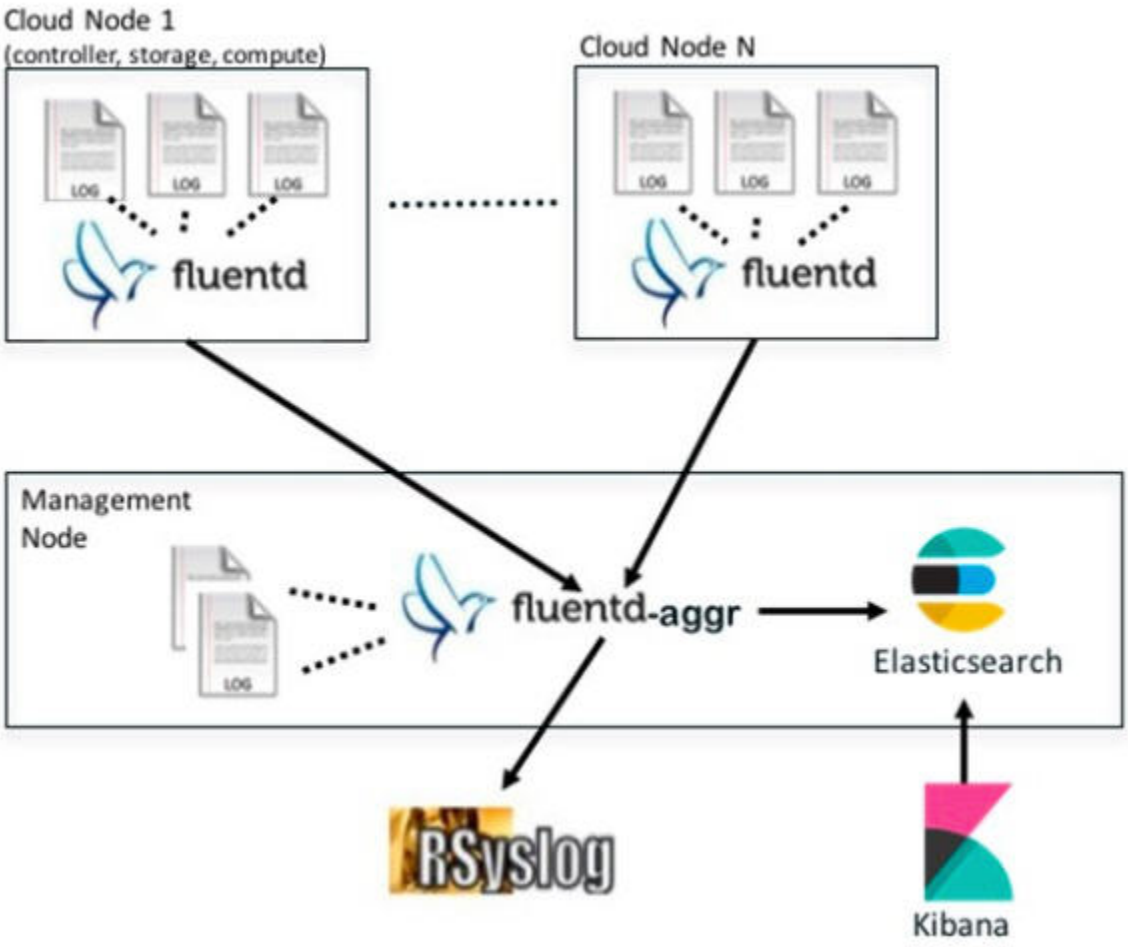
Infrastructure Log Management

Infrastructure Log Management

Cisco VIM uses a combination of open source tools to collect and monitor the Cisco OpenStack services including Elasticsearch, Fluentd, and the Kibana dashboard (EFK). Cisco VIM uses Fluentd instead of logstash. However, to maintain backward compatibility, the code and documentation refers to ELK, instead of EFK at various places. Hence, both ELK and EFK are interchangeably used. OpenStack services followed by EFK include:

- MariaDB: A relational database management system which is based on MySQL. All the OpenStack components store their data in MariaDB.
- HAProxy: HAProxy is a free open source software that provides a high-availability load balancer, and proxy server for TCP and HTTP-based applications that spreads requests across multiple servers.
- Keystone: Keystone is an OpenStack project that provides identity, token, catalog, and policy services for specific use by projects in the OpenStack.
- Glance: An OpenStack project that allows you to upload and discover data assets that are meant for use with other services.
- Neutron: An OpenStack project that provides the network connectivity between interface devices such as vNICs managed by other OpenStack services, for example, Nova.
- Nova: An OpenStack project that is designed to provide on demand massively scalable self-service access to compute resources.
- HTTP: An Apache HTTP server project that is used to develop and maintain an open-source HTTP server.
- Cinder: An OpenStack block storage service that is designed to present storage resources to the users that are consumed by the OpenStack compute project (Nova).
- Memcached: A general-purpose distributed memory caching system.
- CloudPulse: An OpenStack tool that checks the health of the cloud. CloudPulse includes operator and end-point tests.
- Heat: It is the main OpenStack Orchestration program. Heat implements an orchestration engine, to launch multiple composite cloud applications that is based on text file templates.
- Other OpenStack services: RabbitMQ, Ceph, Open vSwitch, Linux bridge, and Neutron VTS (optional).

A Fluentd container resides on each control, compute, and storage nodes and forwards the logs to the Fluentd-aggr server residing on the management node. The following figure shows a high-level schematic view of the EFK service assurance architecture.



The EFK flow includes:

- Fluentd extracts the relevant data from the logs and tags them, so that Kibana can use it later to display useful information about those logs.
- Fluentd sends the logs from all the compute, controller, and storage nodes to the Fluentd-aggr server on the management node.
- Fluentd-aggr in the management node sends the structured logs into the Elasticsearch database.
- Elasticsearch stores the data, indexes it, and supports fast queries against a large amount of log data.
- Kibana visualizes the data that is stored in Elasticsearch using a custom dashboard. You can also add filters to the data to visualize interesting fragments of the log data.

Displaying Log Files

Displaying Cisco VIM Log Files Using CLI

Cisco VIM log file location depends on the node and log type. Installer logs for the last 20 directories are tarred and kept in the management node under the */var/log/mercury/<install_uuid>/* directory. These files contain logs related to bootstrap, build orchestration, baremetal, common setup, and OpenStack orchestration.

If the installer fails, look at the last tar.gz file for logs, for example:

```
[root@mgmtnode mercury]# ls -lrt
total 20
drwxr-xr-x. 2 root root 80 Jul 19 23:42 573f2b7f-4463-4bfa-b57f-98a4a769aced
drwxr-xr-x. 2 root root 4096 Jul 20 03:29 installer
drwxr-xr-x. 2 root root 79 Jul 20 03:29 e9117bc5-544c-4bda-98d5-65bffa56a18f
drwxr-xr-x. 2 root root 79 Jul 20 04:54 36cdf8b5-7a35-4e7e-bb79-0cfb1987f550
drwxr-xr-x. 2 root root 79 Jul 20 04:55 bd739014-fdf1-494e-adc0-98b1fba510bc
drwxr-xr-x. 2 root root 79 Jul 20 04:55 e91c4a6c-ae92-4fef-8f7c-cafa9f5dc1a3
drwxr-xr-x. 2 root root 79 Jul 20 04:58 1962b2ba-ff15-47a6-b292-25b7fb84cd28
drwxr-xr-x. 2 root root 79 Jul 20 04:59 d881d453-f6a0-448e-8873-a7c51d8cc442
drwxr-xr-x. 2 root root 78 Jul 20 05:04 187a15b6-d425-46a8-a4a2-e78b65e008b6
drwxr-xr-x. 2 root root 4096 Jul 20 06:47 d0346cdd-5af6-4058-be86-1330f7ae09d1
drwxr-xr-x. 2 root root 79 Jul 20 17:09 f85c8c6c-32c9-44a8-b649-b63fdb11a79a
drwxr-xr-x. 2 root root 67 Jul 20 18:09 179ed182-17e4-4f1f-a44d-a3b6c16cf323
drwxr-xr-x. 2 root root 68 Jul 20 18:13 426cb05f-b1ee-43ce-862d-5bb4049cc957
drwxr-xr-x. 2 root root 68 Jul 20 18:13 1d2eec9d-f4d8-4325-9eb1-7d96d23e30fc
drwxr-xr-x. 2 root root 68 Jul 20 18:13 02f62a2f-3f59-46a7-9f5f-1656b8721512
drwxr-xr-x. 2 root root 68 Jul 20 18:14 c7417be9-473e-49da-b6d0-d1ab8fb4b1fc
drwxr-xr-x. 2 root root 68 Jul 20 18:17 b4d2077b-c7a9-46e7-9d39-d1281fba9baf
drwxr-xr-x. 2 root root 68 Jul 20 18:35 21972890-3d45-4642-b41d-c5fadfeba21a
drwxr-xr-x. 2 root root 80 Jul 20 19:17 d8b1b54c-7fc1-4ea6-83a5-0e56ff3b67a8
drwxr-xr-x. 2 root root 80 Jul 20 19:17 23a3cc35-4392-40bf-91e6-65c62d973753
drwxr-xr-x. 2 root root 80 Jul 20 19:17 7e831ef9-c932-4b89-8c81-33a45ad82b89
drwxr-xr-x. 2 root root 80 Jul 20 19:18 49ea0917-f9f4-4f5d-82d9-b86570a02dad
drwxr-xr-x. 2 root root 80 Jul 20 19:18 21589a61-5893-4e30-a70e-55ad0dc2e93f
drwxr-xr-x. 2 root root 80 Jul 20 19:22 6ae6d136-7f87-4fc8-92b8-64cd542495bf
drwxr-xr-x. 2 root root 4096 Jul 20 19:46 1c6f4547-c57d-4dcc-a405-ec509306ee25
drwxr-xr-x. 2 root root 68 Jul 20 21:20 c6dcc98d-b45b-4904-a217-d25001275c85
drwxr-xr-x. 2 root root 68 Jul 20 21:40 ee58d5d6-8b61-4431-9f7f-8cab2c331637
drwxr-xr-x. 2 root root 4096 Jul 20 22:06 243cb0f8-5169-430d-a5d8-48008a00d5c7
drwxr-xr-x. 2 root root 4096 Jul 20 22:16 188d53da-f129-46d9-87b7-c876b1aea70c
```

Cisco VIM autobackup logs are found in the following location:

```
# CVIM autobackup logs (auto-backup enabled by default)
/var/log/mercury/autobackup_3.2.x_2019-03-19_15-11-10.log

# cobbler apache log (may be needed for PXE troubleshooting)
/var/log/cobblerhttpd/access_log
/var/log/cobblerhttpd/error_log

# VMTP logs
/var/log/vmtp/vmtp.log
```

Cisco VIM RestAPI log location

```
# CVIM RestAPI logs
/var/log/mercury_restapi/restapi.log

# CIM RestAPI apache logs (TCP port 8445)
/var/log/httpd/mercury_access.log
/var/log/httpd/mercury_error.log

# CIM RestAPI log-directory logs (TCP port 8008)
/var/log/httpd/access_log
/var/log/httpd/error_log
```

EFK log location

```
# Elasticsearch-fluentd-Kibana
/var/log/elasticsearch/
/var/log/fluentd-aggr/
/var/log/kibana/
/var/log/curator/
# HAProxy TLS certificate expiration check
/var/log/curator/certchecker.lo
```

Viewing Cisco VIM Logs

```
# list logs sorted reverse on time
ls -lrt /var/log/mercury/
# untar logs
tar xvzf /var/log/mercury/<UUID>/mercury_install_2018-3-20_10-2.tar.gz -C /tmp/
```

Cisco VIM Configuration Files

```
# example configuration files
/root/openstack-configs/setup_data.yaml.B_Series_EXAMPLE
/root/openstack-configs/setup_data.yaml.C_Series_EXAMPLE

# system maintained setup files - do not modify directly
# always supply user copy of setup_data.yaml
# when using ciscovim client
/root/openstack-configs/setup_data.yaml

# system inventory in pretty format
/root/openstack-configs/mercury_servers_info

# passwords store
/root/openstack-configs/secrets.yaml

# openstack configuration file
/root/openstack-configs/openstack_config.yaml

# RestAPI password
/opt/cisco/ui_config.json

# Insight password
/opt/cisco/insight/secrets.yaml
```

Enabling debug logs for certain OpenStack Services

```
# openstack config file
/root/openstack-configs/openstack_config.yaml

# help
ciscovim help

# list openstack keys
ciscovim list-openstack-configs

# help on reconfigure sub-command
ciscovim help reconfigure

# how to execute subcommand, example below
# important note: reconfigure requires a maintenance window
ciscovim reconfigure --setopenstackconfig KEYSTONE_DEBUG_LOGGING,CINDER_DEBUG_LOGGING
```

On controller and compute nodes, all services are run within their respective Docker™ containers.

To list the Docker containers in the node, execute the following:

```
[root@control-server-2 ~]# docker ps -a
CONTAINER ID IMAGE COMMAND
CREATED STATUS PORTS NAMES
258b2ca1d46a 172.31.228.164:5000/mercury-rhel7-osp8/nova-scheduler:4780
"/usr/bin/my_init /no" 25 minutes ago Up 25 minutes novascheduler_4780
ffe70809bbe0 172.31.228.164:5000/mercury-rhel7-osp8/nova-novncproxy:4780
"/usr/bin/my_init /st" 25 minutes ago Up 25 minutes novanovncproxy_4780
12b92bcb9dc0 172.31.228.164:5000/mercury-rhel7-osp8/nova-consoleauth:4780
"/usr/bin/my_init /st" 26 minutes ago Up 26 minutes
......
novaconsoleauth_4780
7295596f5167 172.31.228.164:5000/mercury-rhel7-osp8/nova-api:4780
"/usr/bin/my_init /no" 27 minutes ago Up 27 minutes novaapi_478
```

To view the Docker logs of any container, execute the following on the corresponding host:

```
ls -l /var/log/<service_name>/<log_filename>
e.g. ls -l /var/log/keystone/keystone.log
```

To get into a specific container, execute the following commands:

```
[root@control-server-2 ~]# alias | grep container
root@control-server-2 ~]# source /root/.bashrc
#execute the alias:
[root@control-server-2 ~]# novaapi
novaapi_4761 [nova@control-server-2 /]$
novaapi_4761 [nova@control-server-2 /]$ exit
exit
```

If the Docker status indicates a container is down (based on output of “docker ps –a”), collect the Docker service logs as well:

```
cd /etc/systemd/system/multi-user.target.wants/
ls docker* # get the corresponding service name from the output
systemctl status <service_name> -n 1000 > /root/filename # redirects the output to the file
```

For storage nodes running Ceph, execute the following to check the cluster status:

```
ceph -v # on monitor nodes (controller), show's ceph version
ceph -s # on monitor nodes (controller), show cluster status
ceph osd lspools #on monitor nodes (controller),list pools
ceph mon stat # summarize monitor status
ceph-disk list # on OSD / storage nodes; List disks, partitions, and Ceph OSDs
rbd list images # on monitor nodes (controller); dump list of image snapshots
rbd list volumes # on monitor nodes (controller); dump list of volumes
```

Kibana Dashboard Login

Kibana Dashboard Login

Kibana is an open source data visualization platform that is used to explore Cisco VIM logs.

Logging into Kibana Dashboard

To log into the Kibana dashboard, follow the below steps:

1. With a terminal client, use SSH to log into your management node and enter the password to login. The following command shows that the IP address of the management node is 17.0.0.2:

```
# ssh root@17.0.0.2
root@17.0.0.2's password
```

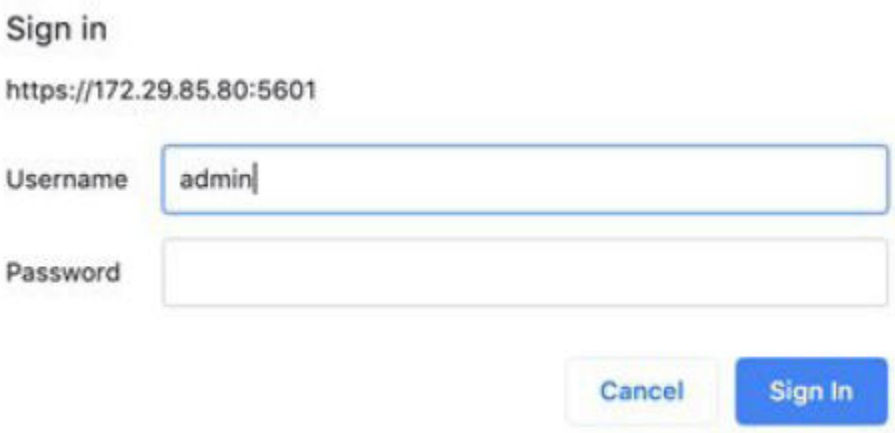
2. To obtain the password, check whether VAULT feature is enabled. If it is enabled, refer to the Vault section, otherwise locate the line containing KIBANA_PASSWORD in */root/installer-{tag id}/openstack-configs/secrets.yaml* during SSH terminal session. Note the value of the KIBANA_PASSWORD as it is used in Step 4.

```
cat /root/installer-{tag-id}/openstack-configs/secrets.yaml
...
KIBANA_PASSWORD: <note this value>
...
```

3. Navigate to the http://<management_node_ip_address>:5601.

- Kibana uses the HTTPS + TLS to provide a secure connection between the browser and the Kibana service.
- By default, Kibana uses the certificate located at */var/www/mercury/mercury.<crt|key>* or you can provide your own certificates in */root/openstack-configs/* directory (using the same mercury.<crt|key> file names).
- If you are accessing Kibana for the first time, by default it shows self-signed certificate. Some browsers display the warning message *Yourconnectionisnotprivate*. Click **Proceed** to access the Kibana link. A window dialog box appears

4. Enter the **Username** and **Password**:



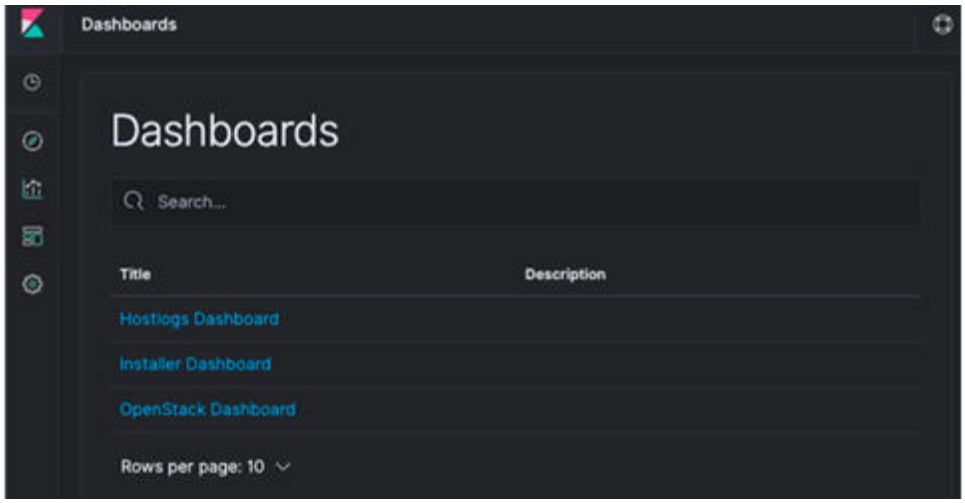
User Name: admin

Password: <value of KIBANA_PASSWORD from Step 2>. The Kibana dashboard displays the Cisco VIM service and installer logs.

5. Choose the desired dashboard from the list.

Ensure that you do not use management options available on the left pane.

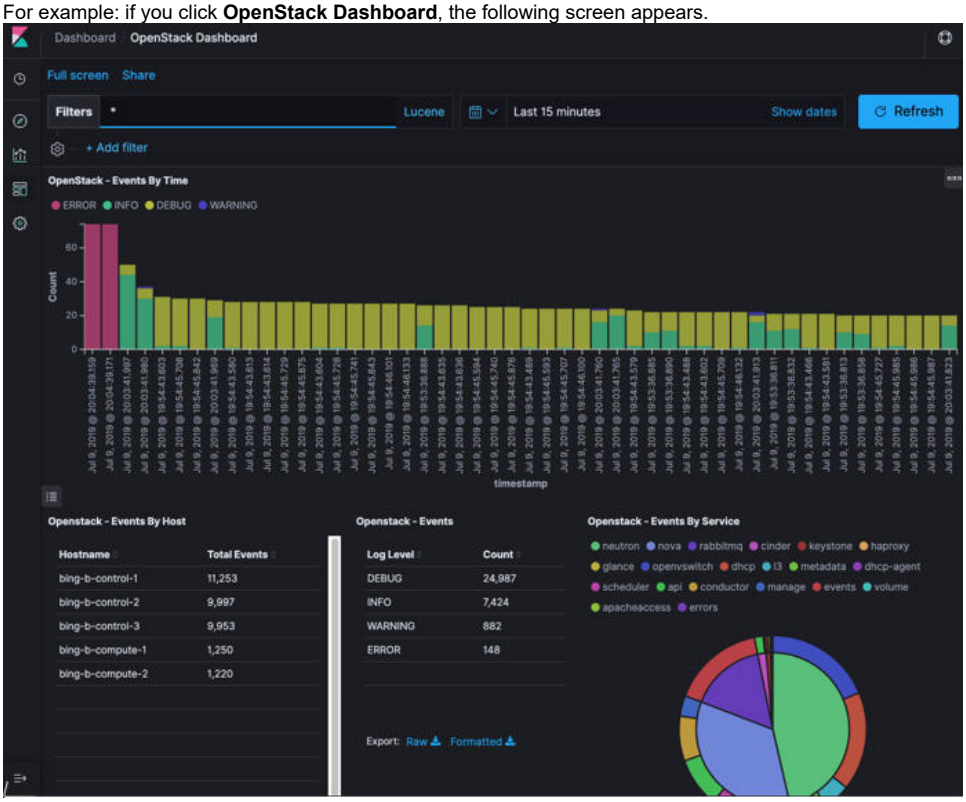
The following figure shows the lists of Dashboards.

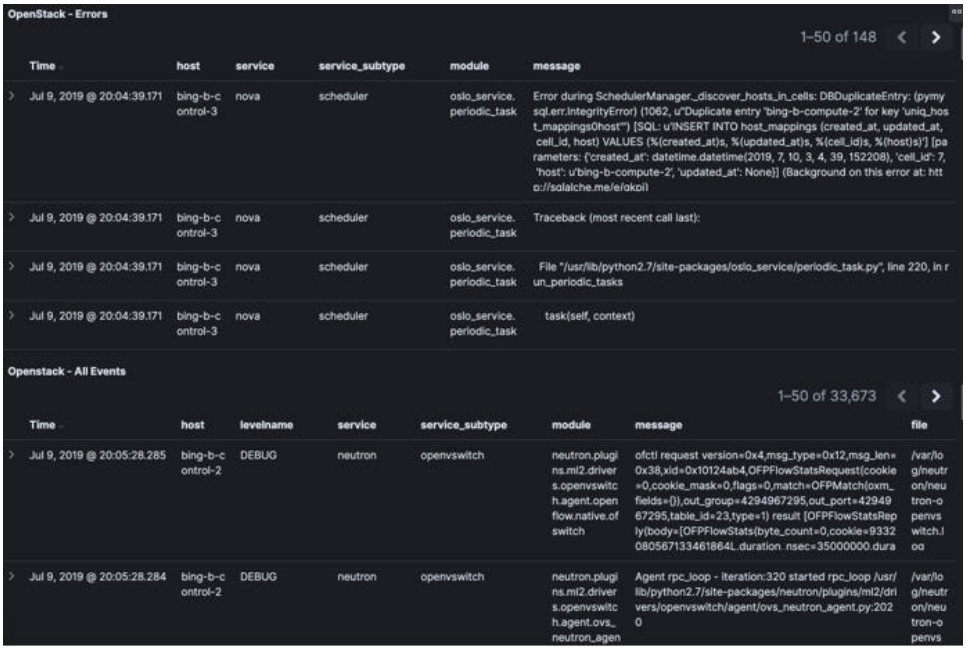


The following are the list of dashboards:

- Hostlogs Dashboard: Provides log information of the system for the cloud nodes. This displays the entries from the host logs-* index in Elasticsearch. It contains the log from */var/log/messages* file on each server.
- Installer Dashboard: Provides information about the management node and the installation process. It can only read uncompressed files. Hence, it reads the files prior to the cloud installation. This displays the entries from the installer-* index in Elasticsearch.
- OpenStack Dashboard: (openstack-* index) Provides log information about all the OpenStack processes. This displays the entries from the openstack-* index in Elasticsearch.
- VMTP Dashboard: Provides log information about the VMTP runs performed against the cloud. It displays the entries from the vmtp-* index in Elasticsearch.

For example: if you click **OpenStack Dashboard**, the following screen appears.





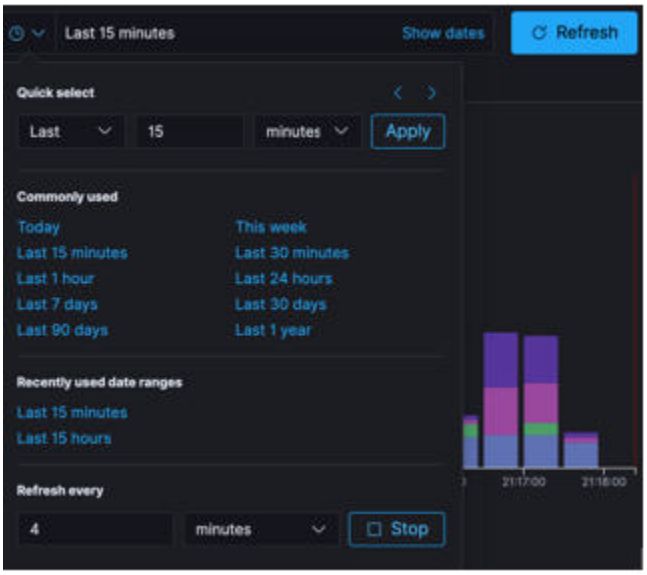
You can switch from one dashboard to another by selecting the appropriate dashboard from the right top bar menu. All dashboards have generic and specific fields.
The generic ones are:

- Title: Title is seen at the top left of the page. Title shows the dashboard that is displayed. For example: OpenStack Dashboard.
- Time bar: Time is seen at the top right of the page. Time indicates the time schedule for the log information. You can modify the time to indicate absolute, relative time in the past or specify automatically refresh rates.
- Filter bar: Search bar is an input field where you can enter a query in the Lucene syntax format to filter the logs by specific fields (which depend on the fields for the index being selected)
- Add a filter: Use this tab to introduce filters graphically.

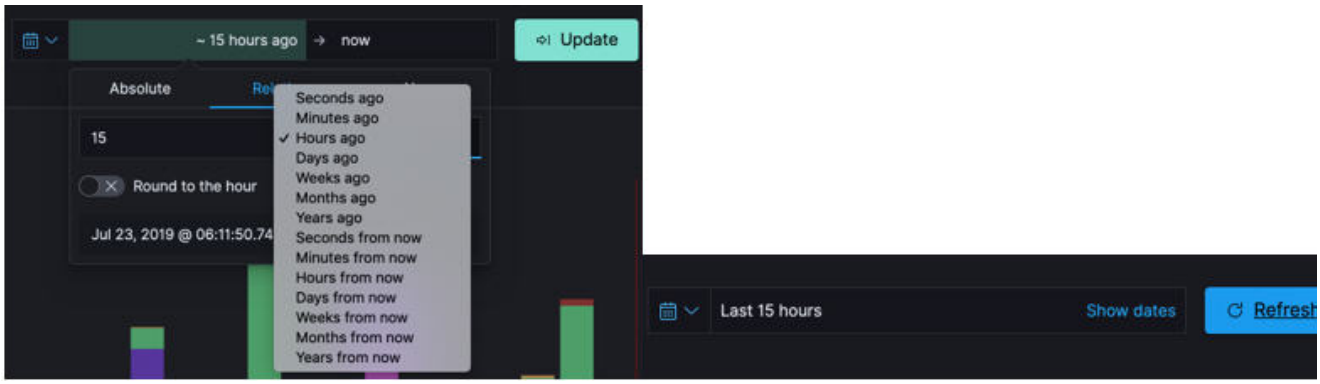
For more information on using Kibana, see the *Kibana documentation* (Version 5.5.1).
Cisco VIM stores the OpenStack logs in Elasticsearch. The Elasticsearch snapshots all the indices (where the data is stored) which are rotated on a periodic basis. You may not see the older data in Kibana, if the data is rotated out and/or deleted.
You can visualize the logs in Kibana when they are updated in Elasticsearch on the **Discover**. To debug something on Kibana, you can program the Kibana dashboard to auto-refresh at specific intervals (by default it is off).

To enable auto-refresh, click the Calendar drawing at the top right corner of the dashboard and program on **Refresh every** with desired value. Configure the desired value by clicking the **Start** and **Auto-refresh**.

Once you program a **Auto-refresh**, the Calendar drawing is replaced by a Clock. Then you can click **Stop** on the top navigator bar to pause the refreshing of logs events. You can also select intervals that you want to see the logs from.



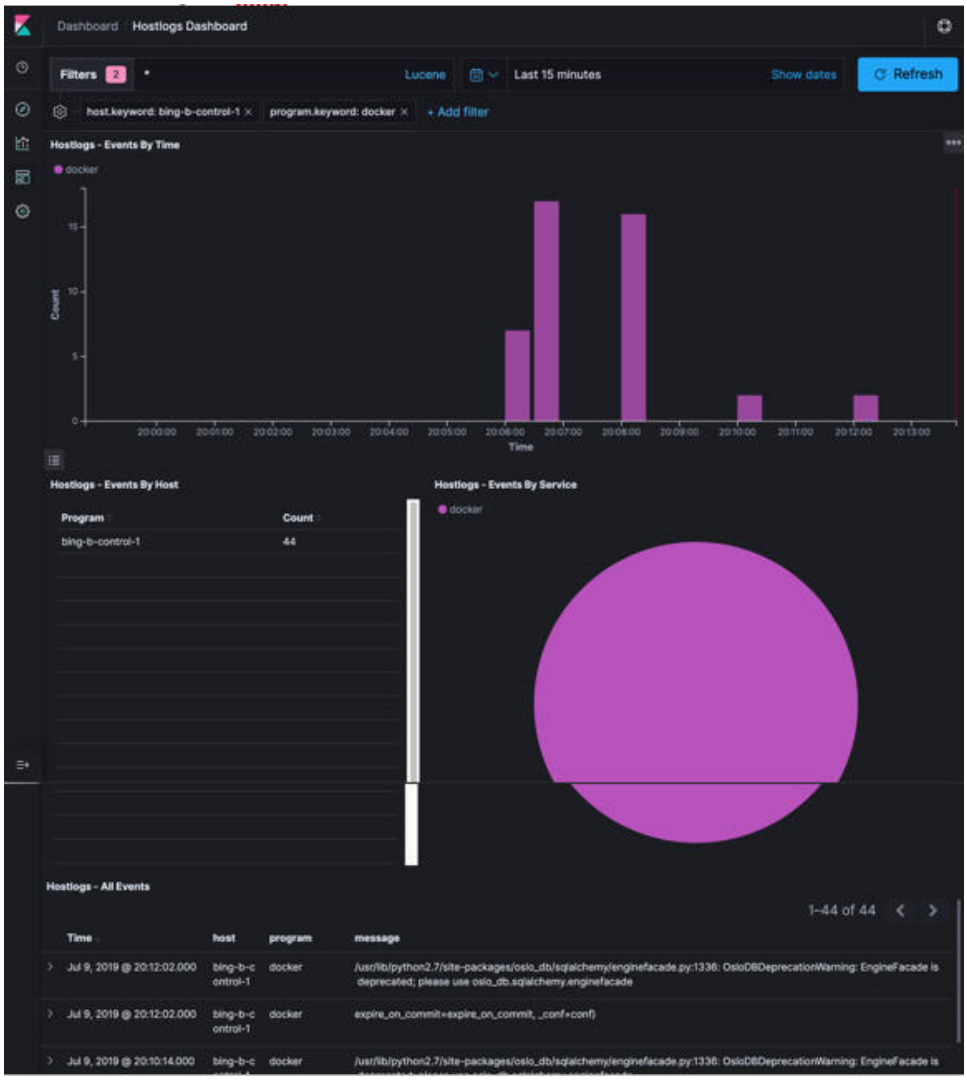
You can also select an absolute or relative interval:



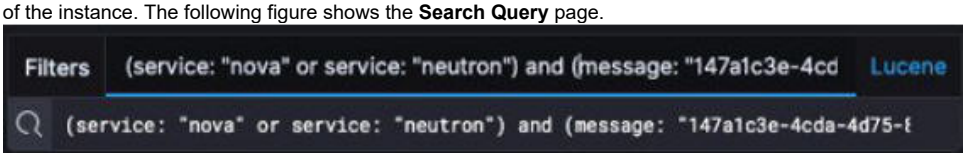
Using Dashboard Filters

1. On the **Hostlogs** Dashboard, in the **Events by Host** panel, choose a hostname and click the **+** or **-** symbol that appears close to the hostname to include or exclude that server from the filter. Then, click the desired slice on the **Events By Service** panel to add the docker service to the section.

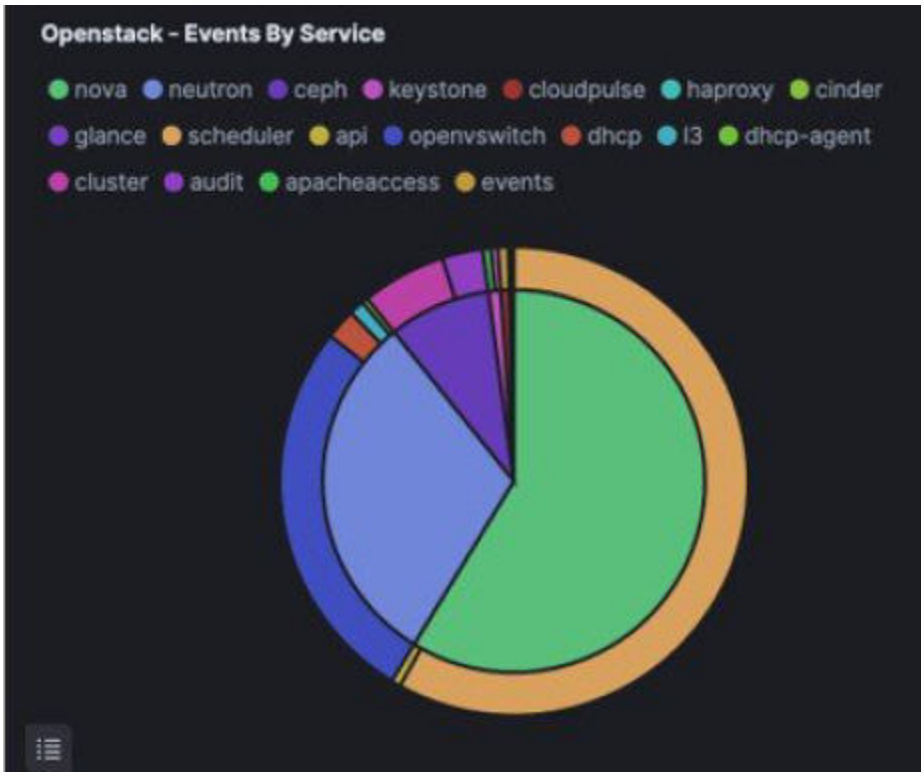
   Under **Filter**, you can see the included sections in green and excluded sections in red. The following figure shows the **Hostlogs** Dashboard:



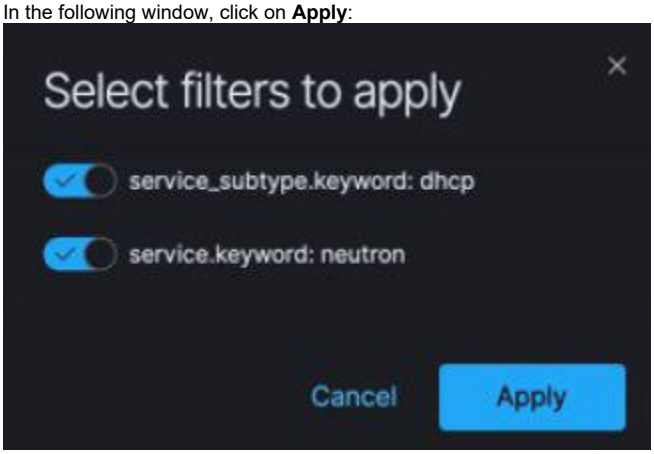
2. To know the log events in the Openstack for a given VM, enter the Lucene query (service: nova or service: neutron and message:<uuid>) in the **Filters** field which is on top of the Dashboard. where <uuid> is obtained from Horizon website or by executing openstack nova list for the identifier of the instance. The following figure shows the **Search Query** page.



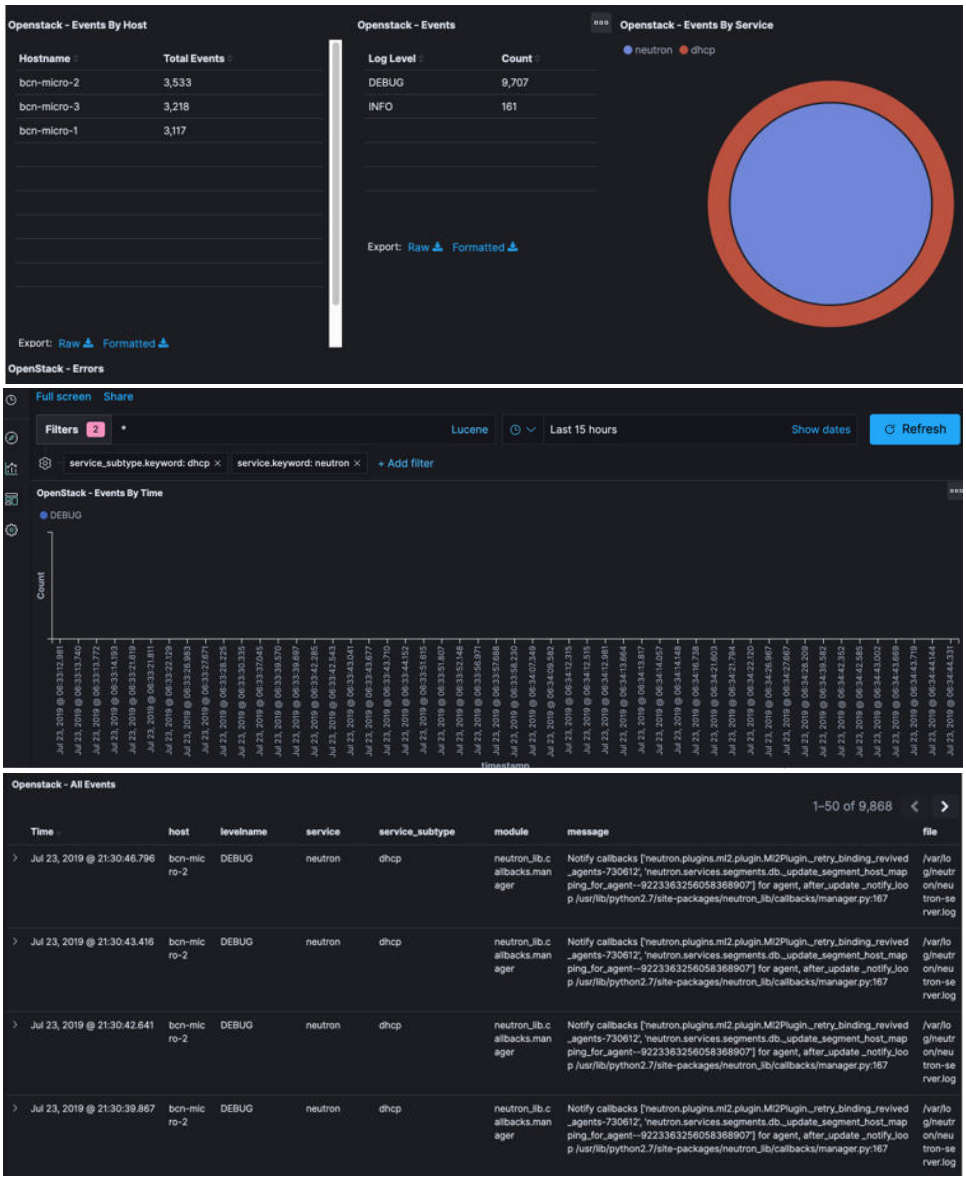
3. If you want to know about the DHCP events of the Openstack Neutron, select the filters by clicking outer circle of pie chart:
On the OpenStack Dashboard, the Openstack - Events By Service panel has a pie chart with the inner section for the services and the outer sections for the service_subtypes. To add filters for selecting all the events in a service (for example, neutron), click on the inner section of the pie. To add filters for selecting the service_subtypes (for example, dhcp), click on the outer circle of the pie. The following figure shows the **Events by Service** Panel.



In the following window, click on **Apply**:



4. You can scroll down the OpenStack Dashboard to see the OpenStack - Errors and the OpenStack - Events panel. The OpenStack - Errors panel displays the error messages. If there are no errors, the **Noresults found** message is displayed.

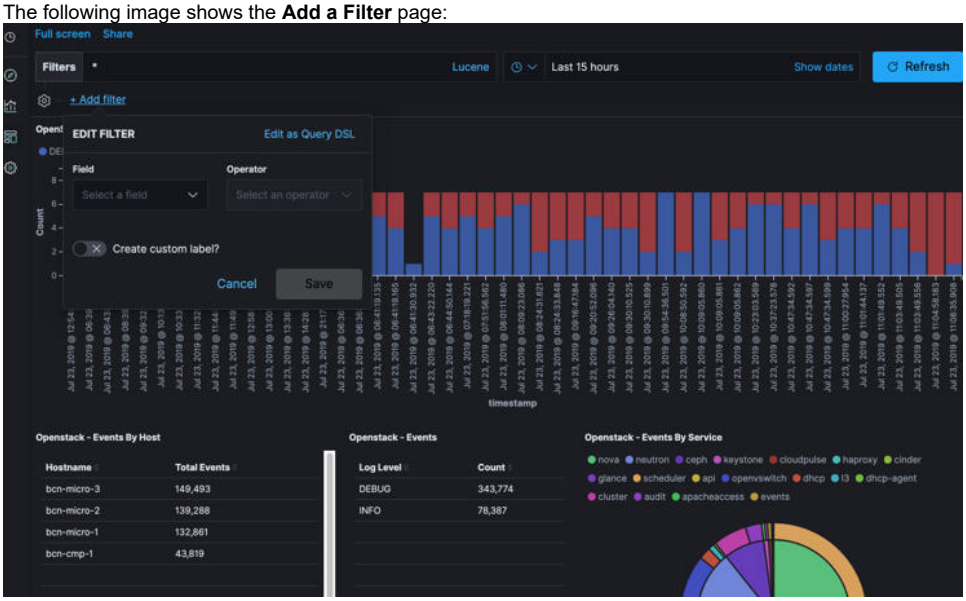


5. Without knowing the Lucene Syntax, you can set the filter criteria in the **Search** field using the **Add a filter +** option.

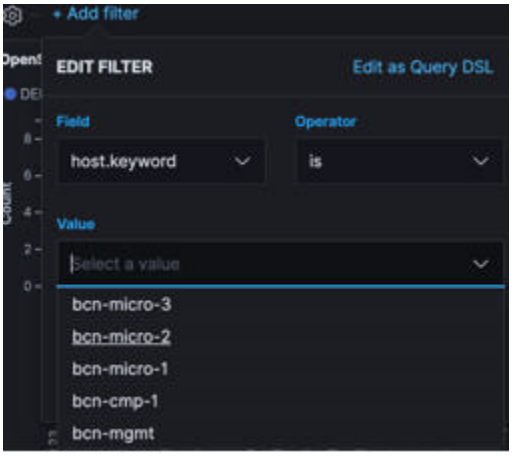
   To add a filter:

   - Click **Add a filter**.
   - Set the filter criteria by choosing appropriate label and operators from the drop-down lists, and entering keywords and click **Save**.

The following image shows the **Add a Filter** page:



6. To set the filter criteria, choose appropriate label and operators from the drop-down lists and enter the keywords in the following figure:



Rotation of Logs

Rotation of Cisco VIM Logs

Cisco VIM stores all logs in Elasticsearch. Elasticsearch indices are rotated on a periodic basis to prevent the disk space overflow by creating snapshots. The following lists show the Snapshots that are defined in openstack_config.yaml:

```
# vi ~/openstack-configs/openstack_config.yaml
...#
Elk rotation parameters
elk_rotation_frequency: "monthly"         # Available: "daily", "weekly", "fortnightly", "monthly"
elk_rotation_size: 2                              # Unit is in Gigabytes (float is allowed)
elk_rotation_del_older: 10                       # Delete older than 10 units (where units depends on the
value set on elk_rotation_frequency)
```

You can change the frequency of the rotation by changing the values. For more information on how to set the Elasticsearch parameters through VIM API or CLI, refer to the section *Reconfiguring Passwords and OpenStack Configurations*.

Cisco VIM uses the open source Elasticsearch Curator tool to manage the Elasticsearch indices and snapshots. For more information about Elasticsearch handles snapshots, look at the official information on Elastic.co (Version 5.4) https://www.elastic.co/guide/en/elasticsearch/client/curator/5.4/index.html.

Elasticsearch

Elasticsearch

Snapshot Manager Tool

The snapshot_mgr.sh tool wraps up the Elasticsearch Curator APIs. This tool helps you to access the snapshots of the logs that are maintained by the Elasticsearch.
Run the following command to view the snapshot logs available in the tools directory of the installer:

```
# ./tools/snapshot_mgr.py --help
usage: snapshot_mgr.py [options]

Snapshot Manager handles snapshot logs maintained by Elasticsearch

optional arguments:
-h, --help                                                  show this help message and exit
--list                                                          display all snapshots in Elasticsearch
--display                                                  GET_SS get details of the snapshot called <GET_SS>
--create                                                   create a snapshot
--restore RESTORE_SS                            restore snapshot named <RESTORE_SS>
--delete DELETE_SS                                    delete the snapshot called <DELETE_SS>
--autodelete threshold_warning threshold_low threshold_high autodelete snapshots until reach a disk space
threshold
```

Snapshot list gives you the details of the snapshot performed on the system like the UUID, the name of the snapshot, end time of the snapshot, the state and the indices where it was snapshotted:

```
# ./snapshot_mgr.py --list
+------------------------+------------------------+---------------------+---------
+-------------------------------------------------------------------------------------------------------------------
--------------------+----------+
| uuid                                          | snapshot_name                   | time_snapshot_ended |
state
|indices_snapshoted
| failures |
+------------------------+------------------------+---------------------+---------
+-------------------------------------------------------------------------------------------------------------------
--------------------+----------+
| 6WGVUnKjQbGtZYzfC0yeEg | curator-20180304140002 | 2018-03-04 14:00:04 | SUCCESS |hostlogs-
2018.03.02
| -        |
| U4IVWJNnQW6PdFWxpRUc-A | curator-20180304150001 | 2018-03-04 15:00:04 | SUCCESS |hostlogs-
2018.03.03
| -        |
| 5RxDuhnETC6TW4XSPDNZlw | curator-20180304160001 | 2018-03-04 16:00:24 | SUCCESS |installer-2018.03.03,
installer-2018.03.01, installer-2018.03.02, openstack-2018.03.02,hostlogs-2018.03.04, installer-2018.03.04   |
-        |
| k2gZYwLeRPO98bJZslI2pw | curator-20180305040002 | 2018-03-05 04:00:32 | SUCCESS |openstack-2018.03.03,
hostlogs-2018.03.04, installer-2018.03.04                                                                      |
-        |
```

To view the details of the individual snapshots, run the display option command:

```
# ./tools/snapshot_mgr.py --display curator-20180304140002
{ 'duration_in_millis': 1944,
  'end_time': '2018-03-04T14:00:04.019Z',
  'end_time_in_millis': 1520172004019,
  'failures': [],
  'indices': ['hostlogs-2018.03.02'],
  'shards': { 'failed': 0, 'successful': 5, 'total': 5},
  'snapshot': 'curator-20180304140002',
  'start_time': '2018-03-04T14:00:02.075Z',
  'start_time_in_millis': 1520172002075,
  'state': 'SUCCESS',
  'uuid': '6WGVUnKjQbGtZYzfC0yeEg',
  'version': '6.0.0',
  'version_id': 6000099}
```

To create a snapshot, run the following command:

```
# ./tools/snapshot_mgr.py --create
Executing: curl PUT
http://localhost:9200/_snapshot/es_backup/3a9b90c2979b46bf9c7b3f9223074d5d?wait_for_completion=true
-d
{'indices': 'installer-*,hostlogs-*,openstack-*,vmtp-*', 'ignore_unavailable': 'true',
'include_global_state': 'false'}
Response: {u'snapshot': {u'uuid': u'BSznQj1SQ9mjxxk9swTirQ', u'duration_in_millis': 46496,
u'start_time':
u'2018-03-06T16:37:49.774Z', u'shards': {u'successful': 35, u'failed': 0, u'total': 35},
u'version_id': 6000099,
u'end_time_in_millis': 1520354316270, u'state': u'SUCCESS', u'version': u'6.0.0',
u'snapshot': u'3a9b90c2979b46bf9c7b3f9223074d5d', u'end_time': u'2018-03-06T16:38:36.270Z',
u'indices': [u'installer-2018.03.06', u'vmtp-2018.03.02', u'hostlogs-2018.03.06',
u'hostlogs-2018.03.05',
u'installer-2018.03.05', u'openstack-2018.03.05', u'openstack-2018.03.06'],
u'failures': [], u'start_time_in_millis': 1520354269774}}
```

Run the following command to delete a snapshot:

```
# ./tools/snapshot_mgr.py --delete 3a9b90c2979b46bf9c7b3f9223074d5d
Executing: curl DELETE
http://localhost:9200/_snapshot/es_backup/3a9b90c2979b46bf9c7b3f9223074d5d -d None
Response: {u'acknowledged': True}
```

Restore the indices of a snapshot back to the Elasticsearch database by using the restore option. Run the following command to restore:

```
# ./snapshot_mgr.py --restore curator-20180306050001
Executing: curl POST
http://localhost:9200/hostlogs-2018.03.04,installer-2018.03.05,installer-2018.03.04,
openstack-2018.03.04,hostlogs-2018.03.05,openstack-2018.03.02/_close -d None
```

Remote NFS Backup for Elasticsearch Snapshots

Cisco VIM supports remote NFS backup of the Elasticsearch snapshots. This allows you to empty the disk space in the Elasticsearch snapshots. You can use the snapshot manager tool to manually create, list, show, and delete snapshots.
You can configure remote NFS backup by adding the following section to the setup_data.yaml configuration file:

```
ES_REMOTE_BACKUP: # Set if Elasticsearch backups can use a remote host
service: 'NFS' # Set if an remote NFS server is used
remote_host: <ip_addr> # IP of the NFS server
remote_path: /root/es_remote # Path to location of the backups in the remote server
```

Important considerations about the remote NFS directory on the remote server (specified by the remote_path config option):

- This directory allows the elasticsearch user (pid number 2020) and group mercury (pid 500) to read and write. Otherwise, Curator cannot copy the snapshots to the remote NFS directory.

- It is good if the folder is empty and is used only by Cisco VIM.
- Cisco VIM does not delete the information in this directory after unbootstrap.

You can enable or disable this feature by running reconfiguration commands. During reconfiguration, the remote_host ip or the remote_path can be changed.

CVIM-MON

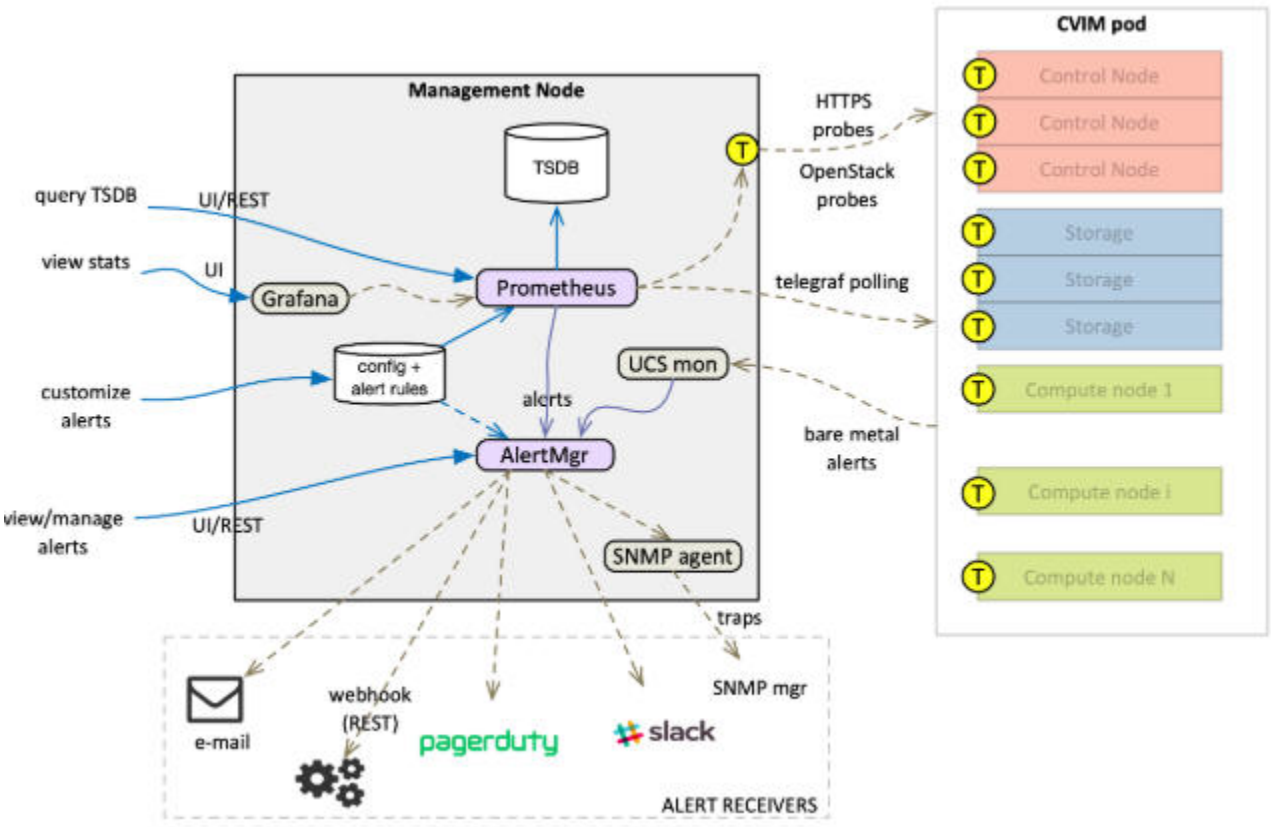
CVIM Monitor (CVIM-MON)

Overview of CVIM Monitor

The Cisco VIM Monitor (CVIM-MON) feature provides a comprehensive solution for monitoring the health and for tracking the usage of resources in the Cisco VIM pod infrastructure.
This solution is available as a configuration option and provides the following services:

- Infrastructure-level metric collection from all nodes in the pod.
- Metric aggregation into a time-series database (TSDB).
- Rule-based alerting engine integrated with the TSDB.
- Web UI with with pre-defined dashboards customized for Cisco VIM.
- REST API to query the TSDB.
- REST API to query and silence alerts.
- Alert notifications using SNMP traps or alternate alert notification protocols.
- User-configurable alerting rules.
- User-configurable web UI dashboards.

The following figure shows the architecture of CVIM-MON:



A CVIM-MON stack includes the following components:

- a metric collection and metric query server based on the Prometheus open source component.
- an alert manager that is in charge of routing alerts based on the Prometheus alert manager.
- a WEB UI server based on the Grafana open source component.
- an SNMP agent in charge of forwarding alerts to SNMP receivers
- a bare metal alert collector (*UCS mon* in the figure - only available for Cisco UCS servers)

The metrics are collected using a small process running on each node in the pod and is based on the Telegraf open source component (marked *T* in the figure).

The alerts are sent to a configurable number of receivers.

UI and REST services are provided to external applications or users.

CVIM-MON and NFVIMON

Both solutions allow monitoring of a Cisco VIM pod but differ in architecture, feature, and integration level with the Cisco VIM installer.

> From Cisco VIM 3.4.1, you can run NFVIMON along with CVIM-MON. This capability eases the transition from NFVIMON to CVIM-MON and allows operators to evaluate CVIM-MON while using NFVIMON.

Smart Metrics

The Cisco VIM deployment blueprint assigns different roles to different hardware or software resources for operational and optimization purposes. CVIM-MON leverages the metric labeling feature in Telegraf and Prometheus, to associate important contextual information with the metrics associated with the resources. This labeling enables monitoring of the pod in a precise manner than with traditional unlabelled metrics.

Node Type Label

The nodes in a Cisco VIM pod can play different roles based on the deployment model. All metrics originating from a node are labelled with the node type (*l abel name = node_type*) and the node name (*label name=host*).

The following table shows the node types and their metric sources.

Node Type	Source of Metric
mgmt	Management node
controller	Controller node
compute	Compute node
storage	Storage node
aio	all-in-one node(micro-pod deployment)
hc	hyper-converged node (hyper-converged deployment)
edge	edge node (same as aio but without local storage)

CPU Role Label

CPUs in a Cisco VIM pod are statically categorized to perform specific functions. This partitioning is critical to guarantee a proper level of service for each subsystem independent of the load in the other subsystem. For example, it is imperative to isolate the CPUs reserved for the VPP virtual switch, from any other activity on the same compute node, to guarantee the virtual switch forwarding performance. The CPU metrics are labeled with a role (*label name* = *role*) to indicate the function of each CPU. This allows to aggregate CPU metrics based on category, which is a lot more useful than aggregating all CPUs. This categorization cannot be done with unlabeled metrics (by reading CPU time series from a TSDB), due to the following reasons:

- Identification of CPU role based on the core number.
- Existence of multiple types of nodes.
- Each node type has a different CPU partitioning map. The CPU partitioning map may depend on the Cisco VIM release default mapping or customer-specific deployment configuration (for example, on a hyper-converged node, the number of cores reserved for CEPH can vary from deployment to deployment).

The following table shows the roles used by the CVIM-MON to label CPU metrics and their static CPU assignment:

Role	Static CPU Assignment
host	System and OpenStack tasks
ceph	CEPH OSD tasks (note that ceph-mon is in the host category)
vpp	VPP virtual switch
vm	VM vCPUs
mgmt	Management tasks on the management node

Metrics Collection

Telegraf Metrics

CVIM-MON collects hundreds of different metrics from each node through the Telegraf plugin. The metrics range from low-level kernel to infrastructure services. The interval between metrics collections is configurable between 10 seconds to 5 minutes.
The following table shows the list of Telegraf plugins installed as part of the CVIM-MON deployment:

Plug-in	Notes
ceph	Collects performance metrics from the MON and OSD nodes in a Ceph storage cluster
cpu	Detailed statistics for every CPU (with role label)
conntrack	Collects the statistics from Netfilter's conntrack-tools
net_stats	Detailed metrics for physical and virtual network interfaces in Cisco VIM environment
disk	Detailed statistics for every disk
diskio	Disk activity
docker	Detailed metrics on running docker containers
exec	Monitor EFK and Prometheus own storage usage
haproxy	HA proxy/ load balancer metrics for all HTTP services

http_response	Monitor HTTP services availability
hugepages	Monitors huge pages usage per NUMA node
internal	Collects metrics about the telegraf agent itself
ipmi_sensor	Bare metal metrics, including power usage, fan speeds, temperatures, and voltage
kernel	Linux kernel counters such as boot time, context switches, interrupts the node
libvirt	Nova and libvirt data and metrics from VMs running on compute or aio nodes
linkstate	Monitoring LACP, SRIOV links status
mem	Host level memory statistics
net	Metrics about network interface and protocol usage (only for interfaces used by Cisco VIM)
ntpq	NTP metrics
openstack	OpenStack related metrics (openstack services, hypervisors, servers)
processes	bare metal process metrics
rabbitmq	RabbitMQ metrics, currently disabled by default
swap	bare metal swap metrics
system	bare metal system load, uptime, and number of users logged in

Alerting Rules

CVIM-MON provides a list of predefined alerting rules that trigger the alerts based on the value of time series metrics polled by Prometheus. To avoid flapping caused by transient conditions, the rules have a grace period and an alert can be in one of the two states:

- Pending: Rule is triggered but the grace period has not expired.
- Fired: Rule is triggered for a period longer than the grace period.

You can monitor the alerts using the web user interface or API and can optionally convert the alerts into SNMP traps. You can configure CVIM-MON to send alerts as SNMP traps to any registered SNMP managers. The maximum number of SNMP managers supported is three, and a combination of SNMPv2 or v3 managers in different servers is supported. The following table shows the list of alerts, fault code and severity.

Alert Name	Fault Code	Severity	Description
instance_down	serviceFailure	critical	The node is not reachable or is down when the Prometheus server tries to scrape a target to retrieve its metrics. An instance down means that metrics from that target cannot be retrieved.
disk_used_percent	resourceThreshold	major	The storage device is used at over 90% capacity.
disk_filling_up_in_4h	resourceUsage	critical	The storage device is likely to run out of space in less than 4h.
docker_container_down	serviceFailure	critical	The docker container running a Cisco VIM infrastructure service is down. This event must never happen and indicates that an infrastructure container is failed or could not start.
link_down_lacp	hardwareFailure	warning	The LACP bonded link is in an error state, if one of the two bonded links is no longer operating properly. For example, the error may occur by the defective cable connection with the NIC, ToR, or a ToR port misconfiguration. The connectivity may still allow traffic to pass but at half the usual throughput. The defective link must be repaired quickly, to reinstate full bandwidth
link_down_sriov	hardwareFailure	warning	The SRIOV link is in down state. This usually indicates an issue with the physical cable wiring or a misconfiguration of the corresponding port on the ToR.
mem_available_percent	resourceThreshold	informational	There is less than 10% of available system memory. Regular 4K pages memory is used by both the system and OpenStack infrastructure services and does not include huge pages. This alert can indicate either an insufficient amount of RAM or abnormal memory usage by the system or infrastructure
memory_running_out_in_4h	resourceUsage	critical	This node is likely to run out of system memory in less than 4h. Based on the historical memory usage, this alert predicts that all the system memory is used up in less than 4h. This condition must never happen and requires immediate troubleshooting by TAC, before the system memory runs out.
swap_used_percent	resourceThreshold	warning	The node is using over 80% of the available swap space. Nodes should normally use only very little swap space. More than that the nodes will not use any swapping at all.
conntrack_percent	resourceThreshold	warning	The node is using more than 80% of the available conntrack objects. This is mostly useful for OVS deployments. This indicates the abnormal usage of host kernel conntrack resources.
reboot	hardwareFailure	warning	The node is rebooted in less than 10 minutes. Node reboots must be infrequent and be triggered only by the administrator when the node can safely be rebooted. Spontaneous and spurious node reboots must never happen.

system_n_users	resourceThreshold	warning	The node has more than 10 logged-in users.
ceph_error	serviceFailure	critical	The CEPH cluster is in error state and needs to be repaired immediately.
ceph_warning	serviceFailure	warning	The CEPH cluster is in a warning state. It requires attention for the repair to be done.
ceph_osdmap_num_in_osds	resourceThreshold	critical	The CEPH cluster has at least one OSD in the OUT state.
ceph_osdmap_num_up_osds	resourceThreshold	critical	The CEPH cluster has at least one OSD in the DOWN state.
ceph_pgmap_state_count	resourceUsage	critical	The CEPH cluster has at least one placement group that is not in active and clean state.
ceph_pgmap_bytes_avail_filling_up_in_4h	resourceUsage	critical	CEPH may run out of space within 4 hours.
ceph_pgmap_bytes_used_percent	resourceThreshold	warning	CEPH used capacity is over 70%.
ceph_pgmap_bytes_used_percent	resourceThreshold	critical	CEPH used capacity is over 80%.
haproxy_plugin_data_absent	other	informational	Not receiving any metrics from HAproxy for 10 minutes or more (should never happen).
haproxy_active_servers_down	serviceFailure	critical	Indicates that one or more HAProxy active server is not in the UP state.
haproxy_active_servers_backend	serviceFailure	critical	The number of haproxy active server backends is not three.
haproxy_active_servers_galera	serviceFailure	critical	The number of haproxy active galera servers is not one.
haproxy_backup_servers_galera	serviceFailure	critical	The number of haproxy backup galera servers is not two.
http_service_unavailable	serviceFailure	warning	The infrastructure HTTP service at given URL is not responding or is not reachable. This should never happen and may indicate an issue with the availability of the infrastructure service.
rabbitmq_node_running	serviceFailure	critical	At least one of the three rabbitMQ nodes is not running.
rabbitmq_node_mem_used_percent	resourceThreshold	critical	Memory used by rabbitMQ is at 90% of its configured maximum limit.
rabbitmq_queue_consumers	resourceThreshold	critical	One or more rabbitMQ queues have no consumer.
rabbitmq_queue_messages	resourceUsage	critical	The number of queued or unread ready and unacknowledged messages is over 300.
ntpq_offset	resourceThreshold	warning	The mean offset (phase) in the times reported between the local host and remote peer or server is over 2500 milliseconds.
cp_openstack_service_down	serviceFailure	critical	The indicated OpenStack service is not reachable and likely to be down.
cp_hypervisor_down	serviceFailure	critical	The Nova hypervisor is down.
certificate_expiring_5d	other	critical	The certificate expires in less than five days and must be replaced.
certificate_expiring_10d	other	warning	The certificate expires in less than 10 days.
certificate_expiring_45d	other	informational	The certificate expires in less than 45 days.

CVIM-MON Web User Interface

The CVIM-MON graphical user interface allows the pod administrator to monitor the status of the pod using any web browser. This interface is based on Grafana and comes with a set of predefined dashboards.

Access Login

The CVIM-MON web user interface is available by pointing a web browser to the management node IPv4 or IPv6 address (br_api) at port 3000 using https.

Two users are created by default:

- admin: Can create and edit dashboards . It is reserved only for dashboard customization.
- cvim: It is read-only and cannot modify dashboards. This read-only user is preferred for majority of use cases.

The passwords for these two users are auto-generated at the time of deployment and can be retrieved from the Cisco VIM password repository (*openstack-configs/secrets.yaml* file) in the CVIM_MON_PASSWORD entry (*admin* user) and *CVIM_MON_READ_ONLY_PASSWORD (cvim* user*)*.

Additionally, it is possible to configure LDAP users for accessing the Grafana UI.

To change password, you must use the password reconfigure CLI. Ensure that you do not use the following for changing the password:

- The **Forgot your password?** option in the Grafana login page.
- The **Change Password** menu item on the Grafana user interface. This feature works but not persistent across restarts/backup-restore.

Pod <pod-name> Dashboard

The pod dashboard is named as Pod <*pod-name*> where <*pod-name*> is configured in *setup_data.yaml* under the option PODNAME to provide the following:

- High level view of the pod.
- Total number of nodes grouped by node type.
- Total number of cores grouped by role.
- Total load in the pod or sum of the load for all nodes.
- Average usage of all the CPUs reserved for VMs.
- Hardware information of the pod.
- Dataplane statistics of the pod (Networking metrics like throughput, errors and packet sizes)

Node Level Metrics Dashboard

This dashboard provides a detailed view of the state of the most important resources for any node in the pod including the management node. A list of drop-down menus allows to select:

- Node to display (only one)
- Disk devices to display (all or any selection)
- Network interfaces to display (all or any selection)
- CPUs to display (all or any selection)

The dashboard provides the utilization charts for the following parameters:

- Alerts
- System
- CPU
- Memory
- Processes
- Disks
- Network interfaces

Pod Level Metrics Dataplane Statistics Dashboard

This dashboard provides a detailed view of the networking metrics and data coming from the *libvirt* and *cvim_net_stats* telegraf plugins. The following panels are available as part of the data plane statistics:

Statistics	Description
Top 5 nodes drop rate	Top nodes with physical interfaces TX/RX drops rate out of all TX/RX packets in a 20 minute time slot.
Top 10 VMs drop rate	Top VMs with virtual interfaces TX/RX drops rate out of all TX/RX packets in a 20 minute time slot.
Pod throughput in packet-per-second (pps)	Total throughput in pps on all physical interfaces.
Top 5 nodes throughput in pps	Top nodes throughput in pps on node physical interfaces.
Top 10 VMs throughput in pps	Top VMs throughput in pps on VM virtual interfaces.
Pod throughput in bits-per-second (bps)	Total throughput in bps on all physical interfaces.
Top 5 nodes throughput in bps	Top nodes throughput in bps on node physical interfaces.
Top 10 VMs throughput in bps	Top VMs throughput in bps on VM virtual interfaces.

Top 5 Nodes error rate	Error rate on physical interfaces TX/RX out of all TX/RX packets in a 20 minute timeslot.
Average pod packet size	Size calculated from total per-interface bytes divided by total packets on all pod physical interfaces.

Node Dataplane Statistics Dashboard

This dashboard provides per node and per VM view of networking metrics and data coming from the libvirt and cvim_net_stats telegraf plugins. The following panels are available as part of the node data plane statistics dashboard:

- Two gauges with aggregated (all TX+RX) throughput in PPS and bps across physical interfaces on the specific node.
- One gauge with total virtual interfaces (attached to VMs) running on the specific node.

Statistics	Description
Specific VM drop rate	Specific VMs virtual interfaces TX/RX drops rate out of all TX/RX packets on that VM in a 20 minute time slot.
Node throughput in packet-per-second (pps)	Total throughput in pps on all physical interfaces on that specific node.
Node throughput in bits-per-second (bps)	Total throughput in bps on all physical interfaces on that specific node.
Average Node packet size	Size calculated from total per-interface bytes divided by total packets on all node's physical interfaces.
VM throughput in packet-per-second (pps)	Total throughput in pps on all physical interfaces on that specific VM and per VM interface.
VM throughput in bits-per-second (bps)	Total throughput in bps on all physical interfaces on that specific VM and per VM interface.
Average VM packet size	Size calculated from total per-interface bytes divided by total packets on all VM's virtual interfaces.
VM error rate	Error rate on virtual interfaces TX/RX out of all TX/RX packets in a 20 minute time slot.

Specialized Dashboards

The following table provides the list of specialized dashboards:

Dashboard Name	Description
VM Inventory	Shows all the VM running in the pod or on external servers
Capacity Usage	Shows overall resources used by OpenStack projects, by hypervisors and overall CEPH resource usage
Project Dashboard	Shows detailed resources used by each OpenStack project
OpenStack services	Chart shows the state of all OpenStack services, infrastructure containers, and hypervisors.
Alerts	Alerts that are triggered passed the grace period or pending (triggered but still within their grace period).
HTTP Servers Stats	Chart to monitor all internal and external HTTP services in the pod.
CEPH	CEPH storage chart, for example, overall OSD CPU load.
NTP	Chart to monitor NTP on the pod.
RabbitMQ	Chart related to rabbitMQ
Etcd	Chart related to etcd. Only available for ML2/VPP deployments.
Advanced Metrics	Chart that monitors the management node activity such as: • Prometheus and Elasticsearch disk usage • Prometheus scraping statistics
IPMI	Chart that presents bare metal sensor and counters: • Temperature • Voltage • Fan Speed • Power • Error counters

SNMP for Monitoring

Along with CVIM-MON, you can enable SNMP in Cisco VIM to send SNMP Traps to the remote SNMP managers. The SNMP traps are identified from the following, only when the SERVER-MON is enabled in the setup_data.yaml file.

- Alerts collected on Prometheus
- Faults reported by the CIMC of the Cisco C-series servers (via SERVER-MON Option)

The SNMP trap sends a notification when the fault occurs or gets resolved. The notification types are listed below:

- cvimFaultActiveNotif: Notification sent when the fault gets triggered.
- cvimFaultClearNotif: Notification sent when the fault gets resolved.

The SNMP trap contains the following information:

1. cvimPodID: PODNAME configured in *setup_data.yaml* file
2. cvimNodeID: Node that generated the fault, or N/A
3. cvimFaultSource: Component name that generated the fault
4. cvimFaultSeverity: Severity of the fault following the guidelines:
    - emergency (1): System level fault impacting multiple services.
    - critical (2): Critical fault specific to a service.
    - major (3): Component level fault within a service.
    - alert (4): Warning condition for service. It may eventually impact the service.
    - informational (5): Informative message and does not impact any service
5. cvimFaultCode: Code. Guidelines followed for code:
    - other(1): Type of event not specified in the other labels.
    - resourceUsage(2): Resource usage exhausted event.
    - resourceThreshold(3): Resource threshold reached event.
    - serviceFailure(4): Software failure service event.
    - hardwareFailure(5): Hardware failure event.
    - networkConnectivity(6) :Networking issues

For more details, see CISCO-VIM-MIB.my.4.0 definition of the MIB at ftp://ftp.cisco.com/pub/mibs/v2/.
CVIM-MON is integrated into Cisco VIM as an optional component and offered as an add-on with an additional license. CVIM-MON is enabled by extending the *setup_data.yaml* file with relevant information. To enable CVIMON, see Enabling CVIM-MON on Cisco VIM

You can enable CVIM-MON on an existing pod through the reconfigure option, if the pod is fresh installed with Cisco VIM 2.4.3 or later versions. To reconfigure through Unified Management, refer to Reconfiguring Optional Services. Then, add the pod as a new VIM resource to be monitored so that it is available through the Unified Management portal.

Monitoring External Servers Using CVIM-MON

The Telegraf agent that is installed on the external servers have the following plugins enabled:

- cpu
- disk and diskio
- net
- mem
- ipmi_sensor
- kernel
- processes
- swap
- system
- linkstate
- ntpq
- conntrack
- internal: Monitors the health of the Telegraf agent and enabled input plugins
- libvirt: Collects metrics related to any virtual machines running on the external server
- prometheus_client: Provides scraping access to any Prometheus compatible scraper
- x509_cert
- hugepages
- diskmon

Some plugins such as *libvirt* and *x509_cert* are disabled during installation time of external server.

These metrics are integrated in the Prometheus TSDB with the following arrangement:

- Metrics collected from external servers are distinguished from Cisco VIM pod metrics by a node_type label value of *external* (outside of the host name being different)
- Metrics for all CPUs have the label *tag* set to *host* by default. You can customize this with additional steps during installation.
- Default built-in alerting rules and custom alerting rules equally apply to external nodes (unless restricted to certain node types in the rule).
- External servers are considered as part of the attached Cisco VIM pod.
- For central monitoring, external servers are assigned the same region or metro as the attached Cisco VIM pod.

In the Grafana dashboard, all counters such as node count per type, alert counters, power consumption aggregates and so on, include external servers as applicable.

Inventory Discovery

Inventory Discovery

API Client

API Client

By default, *Inventory_Discovery* API is running on TCP port 8747 on the Cisco VIM controller nodes, accessed through the *external_lb_vip_address,* which provides HA across multiple controllers.

The pod administrator can use the below tools offered on the management node:

- API client: *calipso_client*
- Data replication client: *calipso_replication_client*

The API client provides options to interact with the Inventory API on any Cisco VIM pod.

On the Cisco VIM management node, aliases are available for both clients that run with *calipso_client* and *calipso_replication_client.* You can use them on desktop and any Cisco VIM node, if the following pre-requisites are met:

- python 2.7 or 3.5
- python requests

You can use any common REST query tool against the Inventory_Discovery API like curl, postman, httpie, and so on.
As the client source code is available, you can use it to understand the API and build similar client using other languages. The main library used is *requests* which can be obtained for more capabilities from https://pypi.org/project/requests/

Running *calipso_client* --help provides details of the options available with API client.

Listed below are the key parameters of the tool:

- api_server API_SERVER - FQDN or IP address of the API Serve (default=localhost)
- api_port API_PORT - TCP Port exposed on the API Server (default=8747)
- api_password API_PASSWORD - API password (secret) used by the API Server (default=calipso_default)
- environment ENVIRONMENT - Specify environment (pod) name configured on the API server (default=None, typical name will be *cvim-<PODNAME>)*
- scan section- Actively discovers the specific cloud environment. For more details, run *calipso_client scan -h*.
- call section – Grabs the inventory details from various API endpoints. For more details, run *calipso_client call -h.*
- scan_recurrence: NOW/HOURLY/DAILY/WEEKLY/MONTHLY/YEARLY (default=None)
- method METHOD - Method to use on the API server - options: get/post/delete/put (default=None)
- endpoint ENDPOINT - Endpoint url extension to use on the API server - options: see API documentation for endpoints (default=None)
- payload PAYLOAD - 'dict' string with parameters to send to the API - options: see API documentation per endpoint (default=None)
- page PAGE - a page number for retrieval (default=0)
- page_size PAGE_SIZE - a number of total objects listed per page (default=1000)
- version - Provides a reply back with *calipso_client* version.
- verify_tls - Verifies the full certificate chain from server (default=False)

The default parameter for api_server (localhost) is only used for cases where the client is running on the same node as the API server .

For other cases, more specific details are needed for releases starting from Cisco VIM 3.4.3, the inventory API server is running under *ha-proxy* on the controller nodes.

Environment name is used to describe the cloud facility endpoints managed by a specific entity. This naming convention is used to support multiple cloud types.

Obtain the api_password either through *cat /root/openstack-configs/secrets.yaml | grep CALIPSO_API_SERVICE_PWD* or retrieve using vault api when VAULT is used in *setup_data:*

1. Get the vault data from *source /var/lib/calipso/calipso_config* as the vault token is rendered in *calipso_configuration* in place of passwords, if vault is defined.
2. Fetch the Mongo password from *curl http://$MGMT_IP:8200/v1/secret/data/cvim-secrets/CALIPSO_MONGO_SERVICE_PWD -H "X-Vault-Token: $VAULT_TOKEN*

Environments

Environments

The ‘environment’ is a generic cloud facility of many types to be discovered by the scanning server. In Cisco VIM, the environment definition holds all the configurations needed to interact with the cloud and discover its content, for example the API endpoints, the admin passwords, the DB passwords, the SSH passwords/keys, the Message-BUS access URL and credentials, and so on.

To obtain the list of environments available on a specific API server, use the examples below using curl or calipso_client:

The x-token is grabbed per session to allow one-time password for secure communication with the server using any 'FQDN' or IP for API server:

Token request using curl

Request

```
curl -i -H "Content-Type: application/json" -H "Accept: application/json" -X POST -d '{"auth": {"methods":
["credentials"], "credentials": {"username": "calipso","password": "<CALIPSO_API_SERVICE_PWD> "}}}'
http://localhost:8747/auth/tokens
```

Response

```
{"issued_at": "2019-06-17T09:13:17.388124", "method": "credentials", "expires_at":
"2019-06-18T09:13:17.388124",
"token": "a1fcff2023894061898a80fea6d5dd52", "_id": "5d0759ad6d07b1001214934b"}
```

As the underlying data is always json, it is recommended that each request contains those two headers: *Content-Type application/json* and *Accept application/json.*

- Post request requires data in json format (-d in curl)
- Get requests need to include attributes in the url.

For the duration of the session ('expires_at' is returned), the value of the token must be used for all requests to the API server in a X-Auth-Token header, For example:

Environment request using curl

Request

```
curl -i -H "Content-Type: application/json" -H "Accept: application/json" -H "X-Auth-Token:
a7d13511ad44406281362d18366d99fc" -X GET http://localhost:8747/environment_configs
```

Response

```
{"environment_configs": [{"name": "cvim-cloud", "distribution": "Mercury"}]}
```

In the above example, GET is used and url contains the values in case of the endpoint of environment_configs.

The calipso_client handles all security needs automatically per request, and defaults to *localhost* with default port and default username. You can give the API secret in a single call to get the same response.

Environment request using calipso_client

Request:

```
calipso_client --api_server <external_lb_vip_address> --api_password <CALIPSO_API_SERVICE_PWD> call --method
GET --endpoint environment_configs
```

Response:

```
{"environment_configs": [{"name": "cvim-cloud", "distribution": "Mercury"}"}]}
```

Once the name of the environment is known, you can make a SCAN request to discover cloud content.

Scans

Scans

Discovering the details (inventory and dependencies) of a specific environment is handled through scan requests. You can make scan requests once (automated as needed) or can schedule them in advance.

A prerequisite for any scan request is the existence of an environment_config parameter. It is advised to kick off a scan request once some configurations (instances, flavors, networks) are made on the OpenStack environment.

You must make a scan request and ensure that it is successfully completed with full discovery before any other query is made against the underlying data.

Here is an example of a one-time scan request:

Scan environment with calipso client

Request

```
calipso_client --api_server <external_lb_vip_address> --api_password <CALIPSO_API_SERVICE_PWD> scan --
environment cvim-cloud
```

Response

```
Scan request posted for environment cvim-cloud
Waiting for scan to complete, scan status: pending
Waiting for scan to complete, scan status: running
Waiting for scan to complete, scan status: running
Waiting for scan to complete, scan status: running
```

Waiting for scan to complete, scan status: runningYou must specify an environment parameter for scan request.

A scan can take a while, depending on the size of the resources deployed on the OpenStack environment. If scan_status returns error, you must debug in the calipso_scan container (hint: look at the logs).

If the scan_status is *completed* and “all the inventory, links and Cliques are discovered”, you can start using the API to grab data for analysis.

You can schedule the scan in advance as shown in the below example:

Scheduled-scan environment with calipso client

Request

```
calipso_client --api_server <external_lb_vip_address> --api_password <CALIPSO_API_SERVICE_PWD> scan --
environment cvim-cloud --scan_recurrence WEEKLY
```

Response

```
Scheduled scan at: 2019-06-24T12:49:35.332000
Submitted at: 2019-06-17T05:49:34.426000
Scan frequency: WEEKLY
```

For scheduled-scan, the reply above provides the details about the submitted time and the time of the next scheduled scan. The scan is repeated at the frequency defined in the request.

To watch the details of any previously submitted scan request, use the */scans* or */scheduled_scans* as endpoint for the request. Also the environment name is mandatory to get scans per that environment:

Get historical scan and scheduled scans with calipso_client

Request

```
calipso_client --api_server <external_lb_vip_address> --api_password <CALIPSO_API_SERVICE_PWD> call --method
GET --endpoint scans --environment cvim-cloud
```

Response

```
{
"scans": [
        {
                "environment": "cvim-cloud",
                "id": "5cdd9d7c6d07b10013ade7f2",
                "status": "completed"
        },
        {
                "environment": "cvim-cloud",
                "id": "5cddb2726d07b10013ade7ff",
                "status": "completed"
        },
        {
                "environment": "cvim-cloud",
                "id": "5cdff1476d07b10013ade80f",
                "status": "running"
        },
        ]
}
```

Request

```
calipso_client --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint scheduled_scans --
environment cvim-cloud
```

Response

```
{
        "scheduled_scans": [
        {
                "environment": "cvim-cloud",
                "freq": "WEEKLY",
                "id": "5ce2f78e6d07b10013ade824",
                "scheduled_timestamp": "2019-06-17T18:53:04.519000"
        },
        {
                "environment": "cvim-cloud",
                "freq": "WEEKLY",
                "id": "5d078c5e6d07b10012149382",
                "scheduled_timestamp": "2019-06-24T12:49:35.332000"
        },
        {
                "environment": "cvim-cloud",
                "freq": "WEEKLY",
                "id": "5d078f3a6d07b10012149385",
                "scheduled_timestamp": "2019-06-24T13:01:46.794000"
        }
        ]
}
```

Ensure that schedules are well-known and are not overlapping or too frequent scans running against the same pod. A scan can take sometime and the data is cleared by default during scanning.

Paging

Paging

Each Inventory Discovery API server can hold many objects, depending on the customer deployment.

A mechanism of paging supporting page number and page size is available for all API queries to the server.

You can use this mechanism to request a certain page from a list of items on the server and request total number of items to be listed per page (page_size).

Here is an example of request using paging.

This example runs against the scans endpoint:

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
scans --environment cvim-cloud --page 0 --page_size 1
```

Response

```
{
"scans": [
        {
                "environment": "cvim-cloud",
                "id": "5cdd9d7c6d07b10013ade7f2",
                "status": "completed"
        }
  ]
}
```

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
scans --environment cvim-cloud --page 0 --page_size 2
```

Response

```
{
"scans": [
 {
        "environment": "cvim-cloud",
        "id": "5cdd9d7c6d07b10013ade7f2",
        "status": "completed"
 },
 {
        "environment": "cvim-cloud",
        "id": "5cddb2726d07b10013ade7ff",
        "status": "completed"
 }
]
}
```

Inventory

Inventory

Each inventory discovery API server runs on a specific pod/environment and holds the latest scan results for all objects and resources on that specific environment in the mongo DB named *calipso* in a special collection called *inventory*

A query for inventory collection must contain the environment name and the common *GET* method.

Use a logical query to get the list of all the objects in that environment of a specific type. Get the list of supported object types from constants.

Here is the latest output for 3.4.3 release, with embedded explanations for the different types:

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
constants --payload "{'name': 'object_types'}"
```

Response

```
{
        "_id": "5cdd5f92bac311001dfbdbca",
        "data": [
        {
                "label": "vnic", --> virtual NIC attached to a VM or a Namespace (ex: tap
                interface, virtualEthernet interface)
                "value": "vnic"
        },
        {
                "label": "vconnector", --> Local Bridge connecting VMs running inside the same node )ex:
linux_bridge , bridge_domain)
                "value": "vconnector"
        },
        {
                "label": "vedge", --> The device connecting VMs running inside a node to the physical network
(ex: VPP, OVS, SR-IOV)
                "value": "vedge"
        },
        {
                "label": "instance", --> VM
                "value": "instance"
        },
        {
                "label": "container", --> Container
                "value": "container"
        },
        {
                "label": "pod", --> K8s Pod
                "value": "pod"
        },
        {
                "label": "vservice", --> a Namespace, a process/device providing networking services (ex: DHCP,
Router, Proxy)
                "value": "vservice"
        },
        {
                "label": "host_pnic", --> physical NIC on a node/host
                "value": "host_pnic"
        },
        {
                "label": "switch_pnic", --> physical NIC on a switch
                "value": "switch_pnic"
        },
        {
                "label": "network", --> the logical representation of an end-to-end communication, like an
OpenStack network
                "value": "network"
        },
```

```
        {
                "label": "switch", --> physical switching device
                "value": "switch"
        },
        {
                "label": "port", --> endpoint on a network
                "value": "port"
        },
        {
                "label": "otep", --> overlay tunneling endpoint, of many types (gre, vxlan, geneve etc ...)
                "value": "otep"
        },
        {
                "label": "agent", --> a process running on a host for control (ex: ovs agent, dhcp agent etc)
                "value": "agent"
        },
        {
                "label": "host", --> the node, physical server (or VM in nested environments)
                "value": "host"
        },
        {
                "label": "project", --> openstack's tenant
                "value": "project"
        }
        ],
                "id": "5cdd5f92bac311001dfbdbca",
                "name": "object_types
}
```


Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
inventory --payload "{'type': 'vservice'}"
```

Response

```
{
    "objects": [
        {
            "environment": "cvim-PODNAME",
            "id": "minnesota-aio-3-qrouter-a01a8c25-24e7-4f14-8cfe-7fd54098d3d2",
            "name": "qrouter-min-r1",
            "name_path": "/cvim-minnesota/Regions/RegionOne/Availability Zones/AIO-ZONE/minnesota-aio-3
/vServices/Gateways/qrouter-min-r1",
            "type": "vservice"
        },
        {
            "environment": "cvim-PODNAME",
            "id": "minnesota-aio-3-qdhcp-5fa33dd8-90a3-4f7c-b603-2af8c4d43c10",
            "name": "qdhcp-regular-net0",
            "name_path": "/cvim-minnesota/Regions/RegionOne/Availability Zones/AIO-ZONE/minnesota-aio-3
/vServices/DHCP servers/qdhcp-regular-net0",
            "type": "vservice"
        },
        {
            "environment": "cvim-PODNAME",
            "id": "minnesota-aio-1-qrouter-a01a8c25-24e7-4f14-8cfe-7fd54098d3d2",
            "name": "qrouter-min-r1",
            "name_path": "/cvim-minnesota/Regions/RegionOne/Availability Zones/AIO-ZONE/minnesota-aio-1
/vServices/Gateways/qrouter-min-r1",
            "type": "vservice"
        },
        {
            "environment": "cvim-PODNAME",
            "id": "minnesota-aio-2-qrouter-a01a8c25-24e7-4f14-8cfe-7fd54098d3d2",
            "name": "qrouter-min-r1",
            "name_path": "/cvim-minnesota/Regions/RegionOne/Availability Zones/AIO-ZONE/minnesota-aio-2
/vServices/Gateways/qrouter-min-r1",
            "type": "vservice"
        },
        {
            "environment": "cvim-PODNAME",
            "id": "minnesota-aio-2-qdhcp-5fa33dd8-90a3-4f7c-b603-2af8c4d43c10",
            "name": "qdhcp-regular-net0",
            "name_path": "/cvim-minnesota/Regions/RegionOne/Availability Zones/AIO-ZONE/minnesota-aio-2
/vServices/DHCP servers/qdhcp-regular-net0",
            "type": "vservice"
        }
    ]
}
```

Querying for Object Details

Querying for Object Details

To query the MongoDB for objects, you need the following information:

- type of the specific object
- specific id of the object

Use the query to inventory endpoint to get the list of available objects of certain type with their names, IDs and some generic attributes, for a paged list of certain object type, for example, instances, 5 per page:

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --environment cvim-cloud
--method GET --endpoint inventory --page_size 5 --payload "{'type': 'instance'}"
```

Response


```
{
 "objects": [
        {
                "environment": "cvim-cloud",
                "id": "3959f44c-5e76-4648-a8b7-86039f6f9372",
                "name": "gold-vm-1",
                "name_path": "/cvim-cloud/Regions/RegionOne/Availability Zones/aio-zone/cloud-aio-2/Instances
/gold-vm-1",
                "type": "instance"
        },
        {
                "environment": "cvim-cloud",
                "id": "5a3cb117-714a-4086-a414-c162dab583cc",
                "name": "gold-vm-4",
                "name_path": "/cvim-cloud/Regions/RegionOne/Availability Zones/aio-zone/cloud-aio-2/Instances
/gold-vm-4",
                "type": "instance"
        }
]
```


Request

All objects in the API have a unique id which is listed in the query for any object type. Use this query to grab more detailed data available for specific object, for example:

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --environment cvim-cloud
--method GET --endpoint inventory --payload "{'id': '3959f44c-5e76-4648-a8b7-86039f6f9372'}"
```

Response

```
{
        "_id": "3959f44c-5e76-4648-a8b7-86039f6f9372",
        "accessIPv4": "",
        "accessIPv6": "",
        "addresses": {
               "flat-network": [
                       {
                               "OS-EXT-IPS-MAC:mac_addr": "fa:16:3e:db:29:4a",
                               "OS-EXT-IPS:type": "fixed",
                               "addr": "192.168.90.4",
                               "version": 4
                       }
               ]
},
etc...
```


Inventory retrieves data from OpenStack APIs , databases, and host-level CLI tools.

Links

Links

Links represent relationship or certain dependency between specific object and another object. For example, an instance connected to its vnic or a host_pnic connected to a network.
Each inventory discovery API server runs on a specific pod/environment and holds the latest scan results for all links on that specific environment in the mongoDB *calipso* in a special collection called links.
Query for link collection requires an environment name and the common *get* method. The first logical query is to get a list of all links in that environment of a specific *link_type*.

You can get the list of supported link_types from constants and then query the 'links' collections for a specific link type.

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
constants --payload "{'name': 'link_types'}"
```

Response

```
{
        "data": [
                {
                        "label": "instance-vnic",
                        "value": "instance-vnic"
                },
                {
                        "label": "vnic-instance",
                        "value": "vnic-instance"
                },
                {
                        "label": "vnic-vconnector",
                        "value": "vnic-vconnector"
                },
{"label": "host_pnic-switch_pnic", "value": "host_pnic-switch_pnic"
etc..
```

Querying for Link Details

Querying for Link Details

To query the MongoDB for links, you need the following information:

- link_type of the specific link.
- specific ID of the link.

You can use the query to link endpoint, to get the list of available links of a certain type with their names, IDs, and some generic attributes, for a paged list of certain link type. The below example shows how to find *instance-vnic* links 5 per page:

Request

```
calipso_client --api_server <ext_vip_ip>  --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
links --payload "{'link_type': 'instance-vnic'}"
```

Response

```
{
    "links": [
        {
            "environment": "cvim-cloud",
            "host": "minnesota-aio-3",
            "id": "5e627c09ef75d3e50d765604",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-aio-1",
            "id": "5e627c09ef75d3e50d765609",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-aio-1",
            "id": "5e627c09ef75d3e50d76560e",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-aio-1",
            "id": "5e627c09ef75d3e50d765613",
            "link_name": "sriov-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-aio-2",
            "id": "5e627c09ef75d3e50d765618",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-aio-2",
            "id": "5e627c09ef75d3e50d76561d",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-compute-1",
            "id": "5e627c09ef75d3e50d765622",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-compute-2",
            "id": "5e627c09ef75d3e50d765627",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        },
        {
            "environment": "cvim-minnesota",
            "host": "minnesota-compute-2",
            "id": "5e627c09ef75d3e50d76562c",
            "link_name": "regular-net0",
            "link_type": "instance-vnic"
        }
    ]
}
```

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET -- endpoint
links --environment cvim-PODNAME --payload "{'id': ' 5e627c09ef75d3e50d76562c'}"}"
```

Response


```
{
    "_id": "5e627c09ef75d3e50d76562c",
    "attributes": {
        "network": "5fa33dd8-90a3-4f7c-b603-2af8c4d43c10",
        "vedge_type": "VPP"
    },
    "environment": "cvim-minnesota",
    "host": "minnesota-compute-2",
    "id": "5e627c09ef75d3e50d76562c",
    "implicit": false,
    "last_scanned": "2020-03-06T08:36:25.732000",
    "link_name": "regular-net0",
    "link_type": "instance-vnic",
    "link_weight": 0,
    "source": "5e627bf4ef75d3e50d765257",
    "source_id": "326cb1f5-b39d-4425-9bf1-64e73c71b909",
    "source_label": "",
    "state": "up",
    "target": "5e627c06ef75d3e50d765493",
    "target_id": "minnesota-compute-2|VirtualEthernet0.0.0",
    "target_label": ""
}
```

Inventory API

Inventory API

Overview

CVIM-MON offers Inventory Discovery API with the ability to extract details from worker level objects, and to analyze data for links and dependencies. Inve ntory Discovery API is a RESTful web API over HTTPS, built to offer detailed inventory and analysis.

Command Line Interface

calipso_client : API client

calipso_csv_tool: Dump chosen Inventory data to CSV

calipso_replication_client: Moves mongoDB collections from any remote CVIM pods to a central location

Use CLI with --version to ensure that you are using latest release (currently: 0.8.0). Help is provided with the tool:

```
calipso_client -h

usage: calipso_client.py [-h] [--api_server API_SERVER] [--api_port API_PORT]
                         [--api_password API_PASSWORD] [--verify_tls]
                         [--guide] [--version]
                         {scan,call} ...

positional arguments:
  {scan,call}           Request modes
    scan                Scan request mode
    call                API endpoints mode

optional arguments:
  -h, --help            show this help message and exit
  --api_server API_SERVER
                        FQDN or IP address of the API Server
                        (default=localhost)
  --api_port API_PORT   TCP Port exposed on the API Server (default=8747)
  --api_password API_PASSWORD
                        API password (secret) used by the API Server
  --verify_tls          verify full certificate chain from server
                        (default=False)
  --guide               get a reply back with API guide location
  --version             get a reply back with calipso_client version


calipso_client scan -h

usage: calipso_client.py scan [-h] --environment ENVIRONMENT
                              [--scan_at SCAN_AT]
                              [--scan_recurrence {ONCE,HOURLY,DAILY,WEEKLY,MONTHLY,YEARLY}]
                              [--es_index]

optional arguments:
  -h, --help            show this help message and exit
  --environment ENVIRONMENT
                        specify environment name(typically 'cvim-<pod_name>')
                        configured on the API server Note: scan request always
                        requires an environment)
  --scan_at SCAN_AT     specify the local time for the first scan in a
```

```
                        recurring series in 'yyyy-mm-ddThh:mm' format
                        (optional with --scan_recurrence flag) (default='NOW')
  --scan_recurrence {ONCE,HOURLY,DAILY,WEEKLY,MONTHLY,YEARLY}
                        specify the recurring series of scheduled scan
                        requests - can be used with optional --scan_at
                        argument (options:
                        ONCE/HOURLY/DAILY/WEEKLY/MONTHLY/YEARLY)
                        (default=None)
  --es_index            index environment inventory, links and cliques on
                        ElasticSearch DB options: boolean (default=False)


calipso_client call -h

usage: calipso_client.py call [-h] --endpoint
                              {clique_constraints,clique_types,cliques,constants,environment_configs,health,
inventory,links,messages,scans,scheduled_scans,search,timezone,tree}
                              [--method {GET,POST,PUT,DELETE}]
                              [--environment ENVIRONMENT] [--payload PAYLOAD]
                              [--page PAGE] [--page_size PAGE_SIZE]

optional arguments:
  -h, --help            show this help message and exit
  --endpoint {clique_constraints,clique_types,cliques,constants,environment_configs,health,inventory,links,
messages,scans,scheduled_scans,search,timezone,tree}
                        endpoint url extension to use on the API server -
                        options: please see API documentation for endpoints
                        (default=None)
  --method {GET,POST,PUT,DELETE}
                        method to use on the API server - options:
                        GET/POST/PUT/DELETE (default='GET')
  --environment ENVIRONMENT
                        specify environment name(typically 'cvim-<pod_name>')
                        configured on the API server Note: call request
                        requires an environment for the following endpoints:
                        [messages, links, inventory, scans, scheduled_scans,
                        search, tree] (default=None)
  --payload PAYLOAD     json string with parameters to send to the API -
                        options: please see API documentation per endpoint
                        (default=None)
  --page PAGE           a page number for retrieval (default=0)
  --page_size PAGE_SIZE
                        a number of total objects listed per page
                        (default=1000))
```

The communication with the Inventory API is available to port 8747 on the controller nodes through ha-proxy, using the external_lb_vip_address, that is secured with SSL and authenticated with the *calipso_api_service_pwd* secret

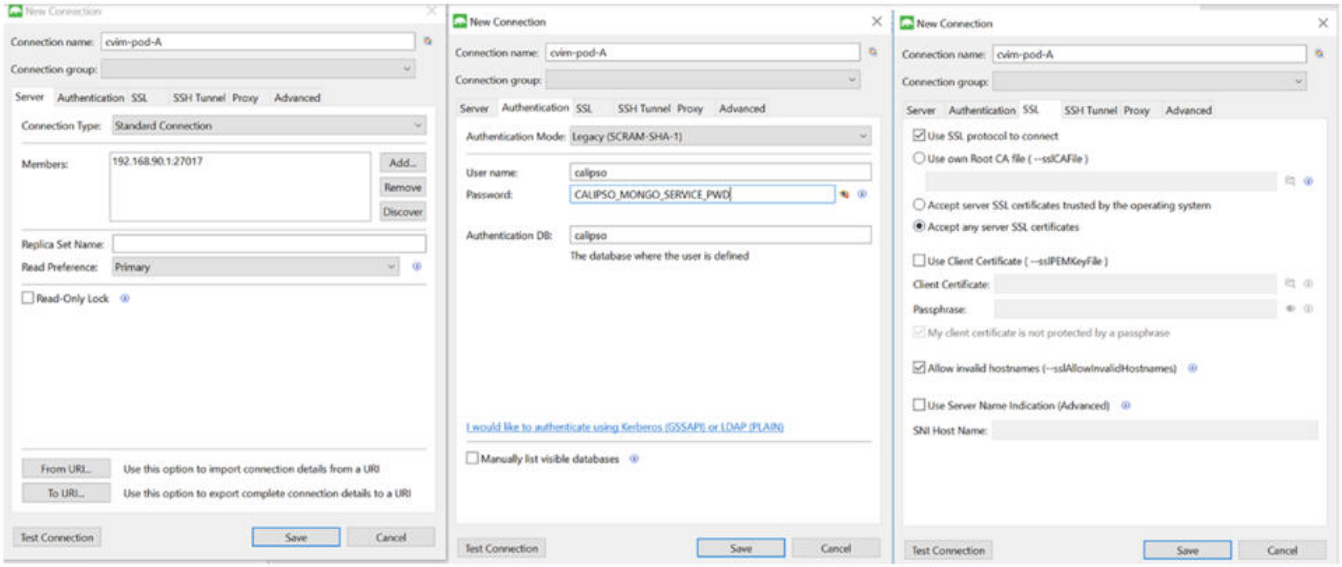
To get the secrets on the management node, you can use list-secrets:

```
ciscovim list-secrets --getpassword CALIPSO_API_SERVICE_PWD

+-------------------------+------------------+
| Secret Key              | Secret Value     |
+-------------------------+------------------+
| CALIPSO_API_SERVICE_PWD | <secret>         |
+-------------------------+------------------+
```

GUI Interface

The communication with the Inventory mongoDB is available to port 27017 on the controller nodes through ha-proxy, using the external_lb_vip_address, that is secured with SSL and authenticated with the *calipso_mongo_service_pwd* secret.

To browse mongoDB inventory details, you can use MongoDB client like *Studio3T community* to add a new connection with authentication parameters



After saving this connection, you can double-click that pod connection name to access all inventory document. You can add as many remote pod connections as needed.

Scan

If your pods have customer deployment (open-stack hosts, projects, instances, storage, networks, security, and so on), you can use *calipso_client* to scan your pod.

> ⚠ You can use *calipso_client* on the management node, server, or personal computer.

The minimum requirements are python 2.7/python 3.5 with python ***requests***. The following example uses the defaults and runs on the management node:

Scan with calipso_client

```
calipso_client --api_password <secret> --api_server <external_vip_ip> scan --environment cvim-<PODNAME>

Scan request posted for environment cvim-minnesota
Wait for scan to complete, scan status: pending
Wait for scan to complete, scan status: running
...
Wait for scan to complete, scan status: completed


Note: typically environment name will be 'cvim-<PODNAME>
```

Move

Use *calipso_replication_client* with a configuration file to move any pod's data to a MongoDB central server.

> ⚠ You can use *calipso_replication_client* on the management node, server, or personal computer,

The minimum requirements are python 2.7/python 3.5 with python *pymongo* and *six.moves*.

Configure

Use the following configuration file to instruct the replication client on how to move data.

replication_config single remote

```
{
"remotes":[
   {
   "host": "some-podA-ext-vip-ip",
   "mongo_pwd": "<podA_mongo_secret>"
   }
],
"central":{
   "host": "some-remote-server.domain.com",
   "mongo_pwd": "<mongo_secret>"
   }
}
```

You can add several remotes to replicate data from multiple remote pods into central. The following example shows the replication from three pods into central:

replication_config many remotes

```
{
"remotes":[
   {
   "host": "<ip_address_1>",
   "mongo_pwd": "IBnr09GzdUOVe58q"
   },
   {
   "host": "<ip_address_2>",
   "mongo_pwd": "iSpv71Iitt7eN48G"
   },
   {
   "host": "<ip_address_3>",
   "mongo_pwd": "FWfN0u86PDMIDX9q"
   }
],
"central":{
   "host": "fqdn",
   "mongo_pwd": "<some_secret>"
   }
}
```

Replicate

You can use the replication client on any server or personal computer. In the following example, the scanned data is moved from a pod to a central server:

Move data with replication_client

```
calipso_replication_client --config replication-config.json


Clearing collection environments_config from <ip_address>...
Clearing collection inventory from <ip_address>...
Clearing collection links from <ip_address>...
Clearing collection messages from <fqdn_name>...
Clearing collection scans from <fqdn_name>...
Clearing collection scheduled_scans from <fqdn_name>...
Clearing collection cliques from calipso-central.cisco.com...
Getting the environments_config Collection from <ip_address>...
Pushing the environments_config Collection into <fqdn_name>...
Inserted 'environments_config' collection in central DB, Total docs inserted: 1
Getting the inventory Collection from <ip_address>...
Pushing the inventory Collection into calipso-central.cisco.com...
Inserted 'inventory' collection in central DB, Total docs inserted: 341
Getting the links ...etc ...
```

View

The central DB with multiple pods data can be accessed through the same *MongoDB* client. The parameter *environment* is added to each pod's document for uniqueness.

Dependency Analysis

Dependency Analysis

Link Connectivity Overview

Link Connectivity Overview

All links in the API have a unique ID which is listed in the query for any link type list. Use this query to grab more detailed information available for specific link, for example:

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --environment cvim-cloud
--method GET --endpoint links --payload "{'id': '5d078b4184c6929f454705b2'}"
```

Response


```
{
        "attributes": {
        "network": "12772133-b894-4a06-8cfb-1f01154721f1"
},
        "environment": "cvim-cloud",
        "host": "cloud-aio-1",
        "id": "5d078b4184c6929f454705b2",
        "implicit": false,
        "link_name": "flat-network",
        "link_type": "instance-vnic",
        "link_weight": 0,
        "source": "5d078b2184c6929f454701d8",
        "source_id": "fb7cb28a-08aa-497e-9d70-5dae755c18a2",
        "source_label": "",
        "state": "up",
        "target": "5d078b3a84c6929f45470404",
        "target_id": "cloud-aio-1-gold-vm-2-vhostuser-fa:16:3e:db:29:4a",
        "target_label": ""
}
}
```


Response is always a JSON and can be filtered using grep command.

One important detail on any link is whether it is 'implicit' or explicit. Implicit implies that it is analyzed after discovery for end-to-end dependency, whereas explicit implies that it is discovered from real-time data on the objects.

Each link have a *target_id* and a *source_id* which represents the 'IDs' of certain objects on the inventory collection. You can get these IDs from inventory. For more information on inventory, see Inventory

Cliques

Cliques

Cliques represent a more complex concept for analysis purposes or dependencies for a certain object.

The object is a focal_point (object of interest) and it refers to an array of links representing the dependency tree (or topology tree) for that specific object, for example an instance connected to its vnic, then to a bridge, ovs, vxaln, and host_pnic.

Each inventory discovery API server runs on a specific pod/environment and holds the latest scan results for all cliques and their resources on that specific environment in the mongoDB calipso in a special collection called *cliques*.

Query for cliques collection requires an environment name and the common *get* method.

The first logical query must be to get a list of all clique_types in that environment for each specific *focal_point_type.*

Clique_types are specific for cloud type and depend on attributes like distribution type, type_driver, and mechanism_driver in use.

When analyzing the data for cliques, a match is made between the attributes of the below clique_types (for example - the distribution value) and the value on the specific environment_config For more information on environment_config, see Environments.

You can get the list of supported clique types from a specific endpoint called clique_types. Here is the sample output with explanations for the different types:

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
clique_types
```

Response

```
{
        "clique_types": [
        {
                "environment": "ANY", --> this list of links for this focal_point_type is used if a more
specific one is not matched.
                "focal_point_type": "instance", --> this object type (instance) will depend on the below list
of link_types
                "id": "5cdd5f92bac311001dfbdbaa",
                "link_types": [
                "instance-vnic",
                "vnic-vconnector",
                "vconnector-vedge",
                "vedge-otep",
                "otep-vconnector",
                "vconnector-host_pnic",
                "host_pnic-network"
        ],
                "name": "instance"
        },
        {
                "environment": "ANY", --> this list of links for this focal_point_type are used if more
specific one is not matched.
                "focal_point_type": "vservice", -> this object type (vservice) depends on the below list of
link_types.
                "id": "5cdd5f92bac311001dfbdbab",
                "link_types": [
                "vservice-vnic",
                "vnic-vedge",
                "vedge-otep",
                "otep-vconnector",
                "vconnector-host_pnic",
                "host_pnic-network"
        ],
                "name": "vservice"
        }{
                "distribution": "Mercury", --> for a more specific distribution of this type (Mercury) the
below links will be used for this focal_point_type
```

```
                "environment": "",
                "focal_point_type": "instance",
                "id": "5cdd5f92bac311001dfbdbb2",
                "link_types": [
                "instance-vnic",
                "vnic-vconnector",
                "vconnector-vedge",
                "vedge-host_pnic",
                "host_pnic-network"
        ],
                "name": "instance_vconnector_clique"
        },
        {
                "distribution": "Mercury",
                "environment": "",
                "focal_point_type": "vservice",
                "id": "5cdd5f92bac311001dfbdbb3",
                "link_types": [
                "vservice-vnic",
                "vnic-vconnector",
                "vconnector-vedge",
                "vedge-host_pnic",
                "host_pnic-network"
        ],
                "name": "vservice_vedge_clique"
        },
        {
                "distribution": "Mercury",
                "environment": "",
                "focal_point_type": "network",
                "id": "5cdd5f92bac311001dfbdbb4",
                "link_types": [
                "network-host_pnic",
                "host_pnic-vedge",
                "vedge-vconnector",
                "vedge-vnic",
                "vconnector-vnic",
                "vnic-instance",
                "vnic-vservice"
                ],
                "name": "network"
                }, etc...etc...
        }
        ]
}
```


Querying for Clique Details

To query the MongoDB for cliques, you need the following information:

- focal_point_type for the specific clique.
- specific focal_point_object_id of the clique.
- id of the specific clique.

The actual logical flow of getting full clique details is listed below:
Use the query to cliques endpoint to get the list of available cliques with the specific focal_point ids and generic attributes, for a paged list of certain clique type. For example, instance as focal_point and list 5 per page:

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> call --method GET --endpoint
cliques --environment cvim-cloud --payload "{'focal_point_type': 'instance'}" --page_size 5
```

All objects in the API have a unique id that is listed in the query for any clique type list. Use this query to grab the more detailed information for specific clique.

Response

(all links that are part of instace focal point)

Request

```
calipso_client --api_server <ext_vip_ip> --api_password <CALIPSO_API_SERVICE_PWD> --environment cvim-cloud --
method GET--endpoint cliques --payload "{'id': '5d07d78084c6929f454a99fa'}"
```

Response

```
response:
{
        "clique_type": "5cdd5f92bac311001dfbdbb2",
        "constraints": {
                "network": [
                        "e4ab9d18-21a3-4241-b220-5070753251ec"
        ]
        },
        "environment": "cvim-cloud",
        "focal_point": "5d07d76784c6929f454a881a",
        "focal_point_object_id": "ae3fa0a0-e21b-47c1-b531-9a86f7cdd602",
        "focal_point_type": "instance",
        "id": "5d07d78084c6929f454a99fa",
        "links": [
                "5d07d77e84c6929f454a8ba1",
                "5d07d77e84c6929f454a8c50",
                "5d07d77e84c6929f454a8d4c",
                "5d07d77e84c6929f454a8d52",
                "5d07d77e84c6929f454a8d5f",
                "5d07d77e84c6929f454a8d64",
                "5d07d77e84c6929f454a8d6e",
                "5d07d77e84c6929f454a8ecb",
                "5d07d77e84c6929f454a8ed0",
                "5d07d77e84c6929f454a8ec6",
                "5d07d77e84c6929f454a8ed5"
        ],
        "links_detailed": [
        {
                "_id": "5d07d77e84c6929f454a8ba1",
                "attributes": {
                "network": "e4ab9d18-21a3-4241-b220-5070753251ec"
        },
                "environment": "cvim-cloud",
                "host": "cloud-compute-1",
                "implicit": false,
                "link_name": "my-network",
                "link_type": "instance-vnic",
                "link_weight": 0,
                "source": "5d07d76784c6929f454a881a",
                "source_id": "ae3fa0a0-e21b-47c1-b531-9a86f7cdd602",
                "source_label": "",
                "state": "up",
                "target": "5d07d77a84c6929f454a8a44",
                "target_id": "cloud-compute-1-test-vm-2-vhostuser-fa:16:3e:0b:6e:b2",
                "target_label": ""
        }, etc...etc..
        ],
        "nodes": [
                "5d07d76b84c6929f454a884c",
                "5d07d77a84c6929f454a8a44",
                "5d07d77b84c6929f454a8aaf",
                "5d07d77b84c6929f454a8ab6",
                "5d07d77b84c6929f454a8aa8",
                "5d07d77b84c6929f454a8abd",
                "5d07d74384c6929f454a8398",
                "5d07d76b84c6929f454a885a",
                "5d07d76784c6929f454a881a"
        ]
}
```

Collections Scheme

Collections Scheme

Each object based on its type can hold attributes specific to its technology domain and other mandatory attributes on the server, for accuracy, analysis and UI/front-end common requirements.
The following main collections are always deployed with the DB for inventory discovery:

- api_tokens - not exposed externally and used to hold session tokens for interaction with the DB.
- attributes_for_hover_on_data - not exposed externally and used for UI to control the display of specific attributes from a specific object.
- clique_constraints - not exposed externally and defines the depth of the topology discovery (see *constraints* in clique attributes).
- clique_types - exposed externally and defines the type of topology/dependency tree available on each cloud/environment type.
- cliques - exposed externally and holds the details of each dependency tree for each object in the inventory.
- connection_tests - not exposed externally and holds the requests for testing a connection to API endpoints, databases, and CLI on hosts.
- constants - exposed externall and holds the list of all supported objects and their attributes for different clouds.
- environment_options - not exposed externally and holds the lists of all supported environment configurations used by UI.
- environments_config - exposed externally and provides the real time details on how to interact and communicate with a specific cloud /environment.
- inventory - exposed externally and holds the list of all object discovered in real time from the cloud environment.
- link_types - exposed externally and holds the list of all supported link types.
- links - exposed externally and holds the list of all links discovered in real time from the cloud environment.
- messages - exposed externally and holds the list of all messages and events discovered in real time from the cloud environment.
- monitoring_config - not exposed externally and holds the list of actual monitoring configurations for different clouds.
- monitoring_config_templates - not exposed externally and holds the list of supported monitoring configurations templates for different clouds.
- network_agent_types - not exposed externally and holds the list of all supported network agents per cloud release.
- roles - not exposed externally and used for role definitions for RBAC to access the system with LDAP.
- scans - exposed externally and holds the list of requested scans to discover per cloud environment.
- scheduled_scans - exposed externally and holds the list of requested scheduled scans to discover per cloud environment.
- statistics - not exposed externally and holds the list of metrics and statistics over time for TSDB cases.
- supported_environments - not exposed externally and holds the list of all supported variances for different clouds (distributions, type_drivers, and so on).
- user_settings - not exposed externally and used for user authorization definitions for RBAC to access the system internally or with LDAP.
- users - not exposed externally, used for user definitions for RBAC to access the system internally or with LDAP.

Mandatory Attributes

Mandatory Attributes

Inventory Object

The following attributes are mandatory per collection, while each object, link, and clique based on its type have more additional attributes:

- environment - Name of the cloud environment where this object is discovered.
- id - Unique identification across the inventories.
- type - Specific type of the object like instance, switch, host, and so on.
- name and object_name - Non-unique identification as name and per-environment unique name as the object_name.
- show_in_tree - Boolean. If object, must be presented in a tree.
- name_path - Clear placement in the hierarchical tree, per environment/cloud type, based on names.
- id_path - Clear placement in the hierarchical tree, per environment/cloud type, based on IDs.
- parent - Name of the parent object like instances under a certain host, ports under a certain network, and containers under a certain pod.
- parent_id - ID of the parent object.
- parent_type - Object type of the parent object.
- launched_at -When this object is discovered last.
- created_at - When this object is created.
- state - Several values apply per type for monitoring purposes.
- host/switch - One of them is mandatory. It is the physical device that runs this object (more attributes apply for nested environments).

Links

- environment - Name of cloud environment where this link is discovered.
- id - Unique identification across all the links.
- link_type - Specific link type of the link. For example, instance-vnic and switch_pnic-host_pnic per supported link_types in constants.
- link_name - Unique name for the link per environment.
- state - Several values apply per type for monitoring purposes.
- source_id - ID of the source object of link.
- link_weight - Level of importance per clique, defaults to 0.
- implicit - Boolean value represents whether the link is real-time discovered per data presented in inventory or analyzed through other links.
- host/switch - One of them is mandatory. It is the physical device that runs this link (more attributes apply for nested environments).

Cliques

- environment - Name of cloud environment where this link is discovered.
- id - Unique identification across all the links.
- focal_point - mongoDB id of the specific *object of interest*, which is the source of the listed links. For example, instance is a start of a list of links: instance-vnic, vnic-vconnector etc) per supported clique_types.
- focal_point_object_id - Inventory id of the specific focal_point on the inventory.
- nodes - Objects that are part of the clique for UI graphing purposes.
- links - Links that are part of the clique for UI graphing purposes.
- clique_type - Type of the clique per supported clique_types.
- links_detailed - All details per link.
- constraints - Denotes the object type which is the lowest or last object in the specific topology tree.

Network Performance Test

Network Performance Test

NFVBench is a network performance benchmarking tool integrated with Cisco VIM. For more details, refer to Setting up NFVbench.

UM Blueprints

Unified Management (UM) Blueprints

Overview of UM Blueprint

Overview of UM Blueprint

Blueprints contain the configuration metadata required to deploy an OpenStack system through a Cisco VIM pod in Cisco VIM Unified Management.

You can create a blueprint in UM or you can upload a *yaml* file that contains the metadata for a blueprint. You can also create a blueprint from an existing OpenStack system that you are configuring as a Cisco VIM pod. The configuration in the blueprint is specific to the type of Cisco UCS server in the OpenStack system.

A blueprint for a C-series server-based OpenStack system cannot be used to configure a B-series server-based OpenStack system. Cisco UM displays an error, if the blueprint does not match the configuration of the OpenStack system.
Using blueprint, you can quickly change the configuration of an OpenStack system. While only one blueprint can be active, you can create or upload multiple blueprints for a Cisco VIM pod. If you change the active blueprint for a pod, you must update the configuration of the OpenStack system to match the new blueprint.
You can modify and validate an existing blueprint, or delete the blueprint. However, you cannot modify any of the configuration metadata in the active blueprint for a Cisco VIM pod.

UM Blueprint Activation

UM Blueprint Activation

A blueprint becomes active when used after the successful installation of a Cisco VIM pod. Other blueprints that you created or uploaded to that pod are in non-active state.
The upload or creation of a blueprint does not activate that blueprint for the pod. Install a blueprint through the **Cisco VIM Suite** wizard. If the installation is successful, the selected blueprint becomes active.

> ⚠ If you want to activate a new blueprint in an existing pod, you must delete certain accounts and credential policies for that pod before you activate the blueprint. See Activating Blueprint in Existing Pod

Viewing UM Blueprint

Viewing UM Blueprint Details

To view blueprint details:

1. Log in to **Cisco VIM Unified Management** as pod user.
2. Choose the Cisco VIM pod with the blueprint that you want to view.
3. Click **Menu** at the top left corner to expand the navigation pane.
4. Choose **Pre-Install** > **Blueprint Management**.
5. Choose a blueprint from the list.
6. Click **Preview** and download YAML.

Blueprint Creation Using Upload Functionality

Creating a Blueprint Using Upload Functionality

Before you begin

- You must have a *yaml* file (B series or C Series) on your system.
- You can upload only one blueprint at a time. To create a blueprint offline, refer to the *setup_data.yaml.B_Series_EXAMPLE* or *setup_data.yaml.C_Series_EXAMPLE*.
- Keys in the sample *yaml* must match with each other. In case of mismatch, the corresponding pane does not get populated during the upload.

1. Log in to **Cisco VIM UM**.
2. In the navigation pane, expand the **Pre-Install** section and click **Blueprint** setup.
3. Click **Browse** in the **Blueprint Initial Setup**.
4. Click **Select**.
5. Click **Load** in the **Unified Management UI Application**. All the fields present in the *yaml* file is uploaded to the respective fields in the UI.
6. Provide a **Name for the Blueprint** and must be unique.
7. Click **Offline Validation**. If all the mandatory fields in the UI are populated, the offline validation of the blueprint is commenced, otherwise a pop-up message indicating the blueprint section with missing information is displayed.
8. If offline validation is successful, the **Save Blueprint** and **Cancel** are enabled. You are redirected to the Blueprint Management Page.

   If the blueprint validation fails, only the **Cancel** button is enabled.

9. On the Blueprint Management page, you can select the recently added valid Blueprint and click **Install** which is disabled by default. A pop-up message is generated 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 installation. In case of incremented installation, you must select stages in the order. For example, if you select validation stage the second stage management node orchestration is enabled. You cannot skip stages and run a deployment.
10. To initiate the cloud deployment, click **Proceed**. You can view the progress from **Dashboard**.

    Once the blueprint is in **Active** State, the **Post-Install** features listed in navigation bar are set to **Active** stage.

B-Series Blueprint Creation

B-Series Blueprint Creation

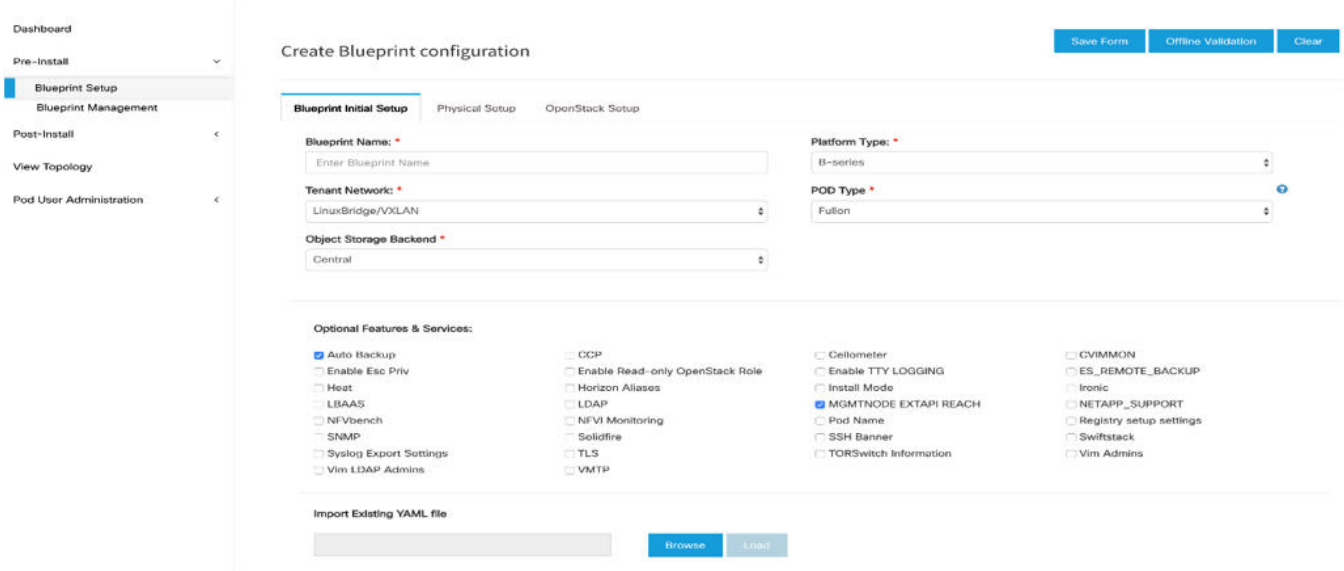
Creating Blueprint for B-Series

Creating Blueprint for B-Series

1. Log into **Cisco VIM Unified Management** or **Insight**.
2. In the navigation pane, choose **Pre-Install** > **Blueprint Setup**. For blueprint setup, click Blueprint Initial Setup Tab
3. For operations related to physical setup, click Physical Setup Tab
4. For operations related to OpenStack setup, click OpenStack Setup Tab
5. For operations on service setup, click Service Setup Tab.

Blueprint Initial Setup Tab

Blueprint Initial Setup Tab



On the **Blueprint Initial Setup** pane of the Cisco VIM Unified Management or insight, enter the following:

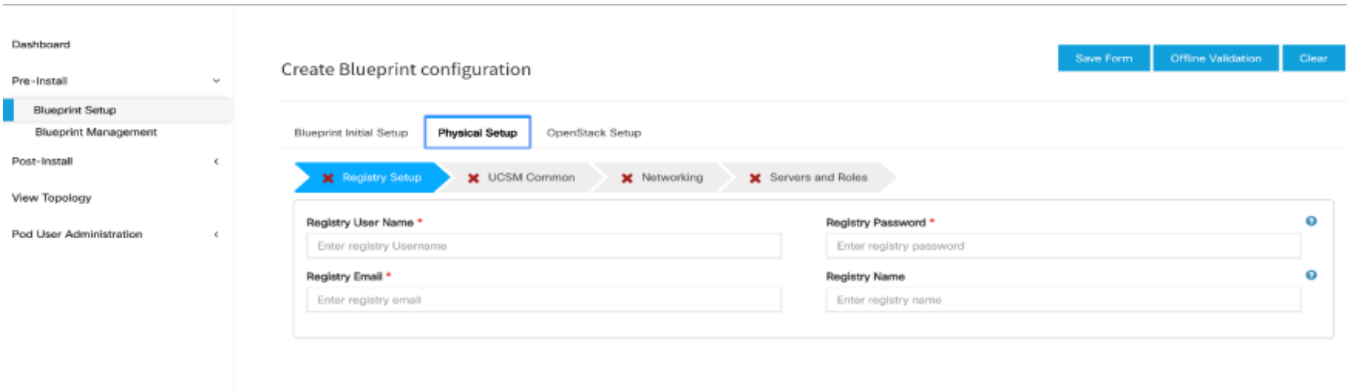
Fields	Description
Blueprint Name	Enter blueprint configuration name.
Platform Type	Choose one of the following platform types: • B-Series (By default) choose B series for this section. • C-Series
Tenant Network	Choose one of the following tenant network types: • Linuxbridge/VXLAN • OVS/VLAN
Pod Type	Choose one of the following pod types: • Fullon(By Default)
Ceph Mode	Choose one of the following Ceph types: • Dedicated • Central (By Default) - Not supported in Production
SSH Banner	An optional parameter ssh_banner is available in the setup_data, to accept a string or message that is to be displayed before the login prompt. This message indicates a warning consistent with a company's IT policies.
Optional Features and Services	Swiftstack, LDAP, Syslog Export Settings, Install Mode, ToR Switch Information, TLS, NFVMON, Pod Name, VMTP, NFV Bench, Auto-backup, Heat, Ceilometer, 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 CVIM-MON to be enabled. By default, all features are disabled except Auto-backup and Management Node_CloudAPI_Reachability. Select **Enable Read-only OpenStack Admins** to add a custom role with read-only admin privileges to OpenStack resources.

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.

Physical Setup Tab

Physical Setup Tab

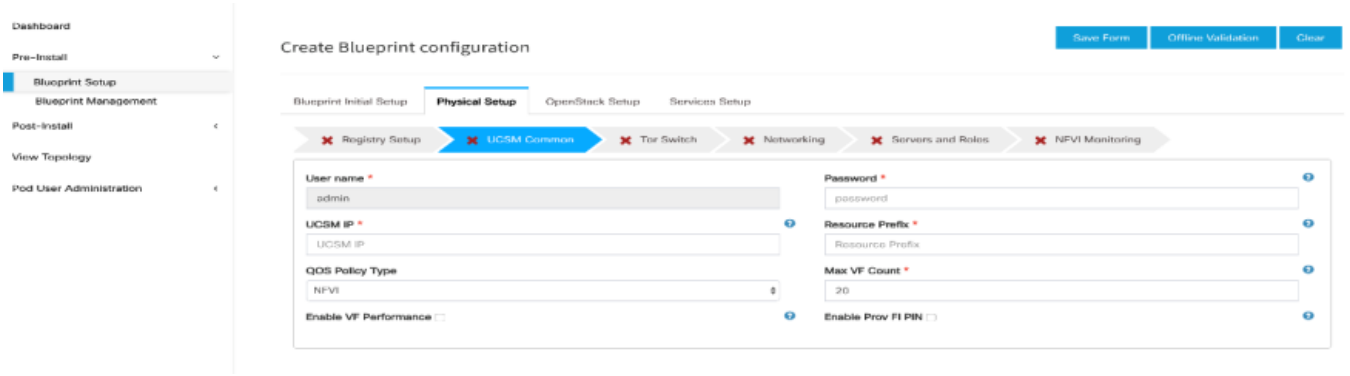
Registry Setup Tab



Fields	Description
Registry User Name	It is a mandatory field. Enter the User-Name for Registry.
Registry Password	It is a mandatory field. Enter the Password for Registry .
Registry Email	It is a mandatory field. Enter the Email ID for Registry.

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

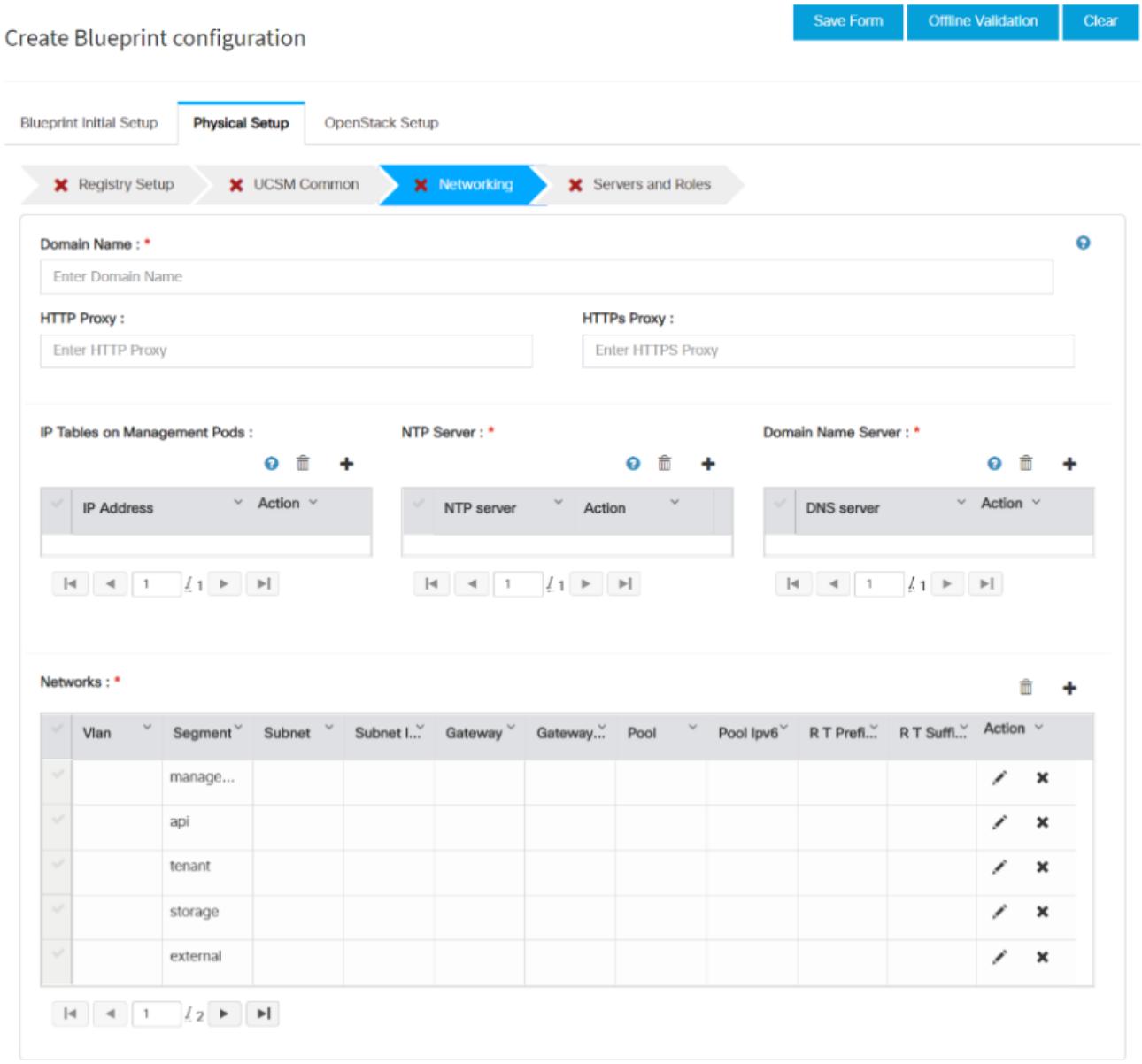
UCSM Common Tab



Fields	Description
User name	By default the value is Admin. Disabled field
Password	It is a mandatory field. Enter Password for UCSM Common.
UCSM IP	It is a mandatory field. Enter IP Address for UCSM Common.
Resource Prefix	It is a mandatory field. Enter the resource prefix.

QOS Policy Type	Choose one of the following types: • NFVI (Default) • Media
Max VF Count	Select the Max VF Count. <1-54> Maximum VF count 54, default is 20. If VF performance is enabled, ensure that you keep MAX_VF_COUNT to 20 otherwise it may fail on some VICs like 1240.
Enable VF Performance	Default is false. Set to true to apply adapter policy at VF level.
Enable Prov FI PIN	Default is false.
MRAID-CARD	Enables JBOD mode to be set on disks. Applicable only if you have RAID controller configured on storage C240 rack servers.
Enable UCSM Plugin	Visible when Tenant Network type is OVS/VLAN.
Enable QoS Policy	Visible only when UCSM plugin is enabled. If UCSM plugin is disabled, this option is set to False.
Enable QOS for Port Profile	Visible only when UCSM plugin is enabled.
SRIOV Multi VLAN Trunk	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.

Networking Tab

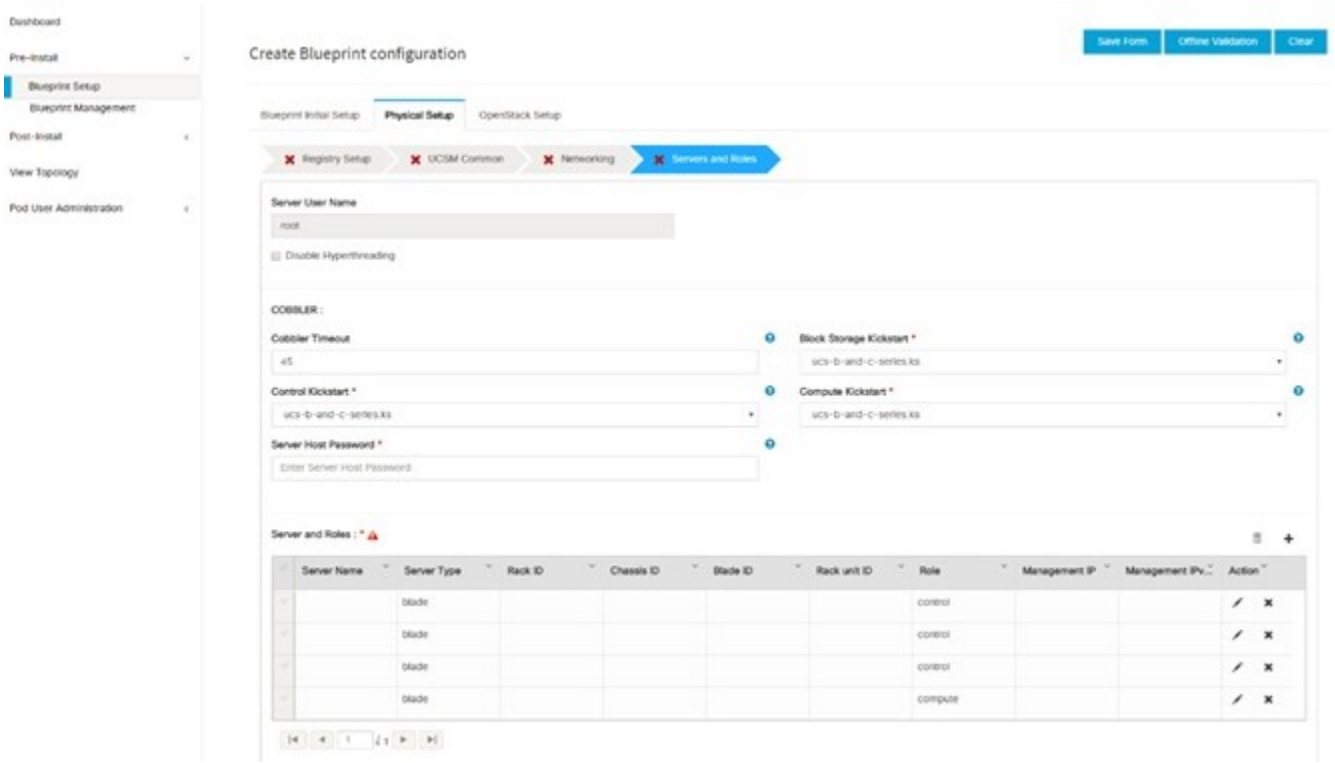


Fields	Description
Domain Name	Enter the domain name. It is a mandatory field.
HTTP Proxy Server	If your configuration uses an HTTP proxy server, enter the IP address of the server.
HTTPS Proxy Server	If your configuration uses an HTTPS proxy server, enter the IP address of the server.
IP Tables on Management 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.

Network options	This section is accessible only if ToR type is Cisco NCS 5500. **vxlan-tenant:** • Provider network name: It is a unique name. • BGP AS num: Takes value between 1 and 65535. • BGP Peers: Enter the peer route reflector IPs (IPs to be comma separated) • BGP router ID: The router ID is used for local GoBGP cluster. • Head-end replication (Optional) : You can add VTEP IP address and comma separated VNI IDs. Multiple entries are allowed. ⚠ VXLAN-TENANT is allowed only when NETWORK_OPTIONS is vxlan network. The IPs defined belong to the vxlan-tenant network, but are not part of the vxlan-tenant network pool **VXLAN-ECN:** • Provider network name: It is the unique name. • BGP AS num: It takes the value between 1 and 65535. • BGP Peers: Enter the peer route reflector IPs. (IPs to be comma separated) • BGP router ID: The router ID is used for local GoBGP cluster. • Head-end replication (Optional) : You can add VTEP IP address and comma separated VNI IDs. Multiple entries are allowed. ⚠ • You cannot have VXLAN-ECN without vxlan-tenant segment defined, however vxlan-tenant can be defined s tandalone. • Ensure that you take care while choosing single or multi-VXLAN (two-VXLAN) option as this is a day-0 config uration. • VXLAN_ECN is allowed only when NETWORK_OPTIONS is vxlan network. The IPs defined belong to the vxlan-ecn network, but are not part of the vxlan-ecn network pool.
Networks table	Network table is pre-populated with segments. To add Networks you can either clear all the table using **Delete All** or click **Edit** icon for each segment and fill in the details. Click **+** to enter new entries (networks) to the table. Specify the following fields in the **Edit Entry to Networks** dialog box.
VLAN	Enter the VLAN ID. For Segment - Provider, the VLAN ID value is always *none*.
Segment	You can select any one segment from the drop-down list. • API • Management/Provision • Tenant • CIMC • Storage • External • Provider (optional) ⚠ Some segments do not need some of the values listed in the preceding points.
Subnet	Enter the IPv4 address for the subnet.
IPv6 Subnet	Enter IPv6 address. This field is available only for Management provision and API.
Gateway	Enter the IPv4 address for the gateway.
IPv6 Gateway	Enter IPv6 gateway. This field is available only for Management provision and API network.
Pool	Enter the pool information in the following format. For example: 10.30.1.1 or 10.30.1.1 to 10.30.1.12
IPv6 Pool	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.
Save	Saves the entered information.

Servers and Roles Tab

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



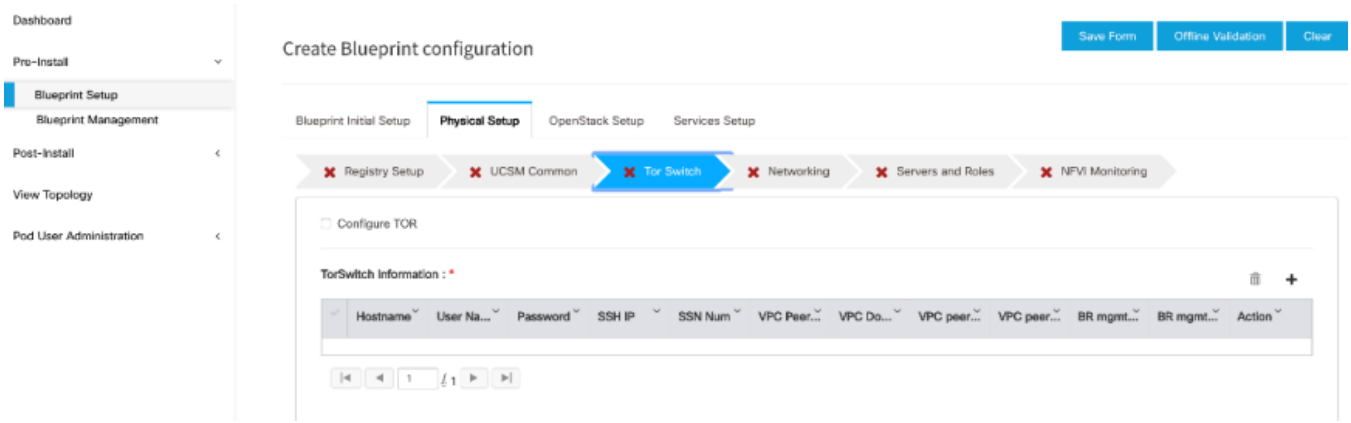
If you choose mechanism driver as OVS or ACI, VM_HUGEPAGE_PERCENTAGE is available for compute nodes, where you can fill values from 0 to 100% when NFV_HOSTS: ALL is chosen. Also, option of NIC Level Redundancy appears only when Intel NIC support is set to True. This is applicable only for M5-based pods.

Fields	Description
Server User Name	Enter the username of the server.
Disable Hyperthreading	Default value is false. You can set it as true or false.
Vendor	Set vendor type at the global level
Roles	Set Vendor type at per role level in the roles table
Cobbler	Enter the Cobbler details in the following fields:
Cobbler Timeout	The default value is 45 minutes. This is an optional parameter. Timeout is displayed in minutes, and its value ranges from 30 to 120.
Block Storage Kickstart field	Kickstart file for Storage Node.
Admin Password Hash	Enter the Admin Password. Password must be alphanumeric. Password should contain minimum of 8 characters and maximum of 32 characters.
Cobbler Username	Enter the cobbler username to access the cobbler server.
Control Kickstart	Kickstart file for control node.
Compute Kickstart	Kickstart file for compute node.
Cobbler Admin Username	Enter the admin username of the Cobbler.
Add Entry to Servers and Roles	Click **Edit** or **+** to add a new server and role to the table.
Server Name	Enter a server name.
Server Type	Choose Blade or Rack from the drop-down list.

Rack ID	The Rack ID for the server.
Chassis ID	Enter a Chassis ID.
Rack Unit ID	If Rack is chosen, the **Rack Unit ID** field is displayed. Enter a Rack Unit ID.
Blade ID	If Blade is chosen, the **Blade ID** field is displayed. Enter a Blade ID.
Role	Select the **Role** from the dropdown list. If Server type is Blade, select **Control and Compute**. If server is Rack, select **Block Storage**.
VIC Admin FEC mode	Applicable only for Cisco VIC that supports to change the admin FEC mode. Can be auto/off/cl74/cl91
VIC Port Channel Enable	Optional. By default, it is true. Can be either true or false.
Secure Computing mode	Optional. By default, it is set to 1, if not defined. Can be either 0 or 1.
Nova CPU Allocation Ratio	Optional. This configuration overrides the NOVA_CPU_ALLOCATION_RATIO configuration defined in the *openstack_config.yaml* file. The range is from 0.958 to 16.0.
Nova RAM Allocation Ratio	This configuration overrides the NOVA_RAM_ALLOCATION_RATIO configuration defined in the openstack_config.yaml file. The range is from 1.0 to 4.0.
VM Hugepage Size	Optional. From the drop-down list, choose 2M or 1G. This configuration overrides the global VM_HUGEPAGE_SIZE value when NFV_HOSTS is enabled.
Disable Hyperthreading	Optional. From the drop-down list, choose True or False. This configuration overrides the global hyper-threading configuration.
Root Drive Type	Optional . From the drop-down list, choose HDD, SSD or M.2_SATA internal SSD. You must choose M.2_SATA if booting off M.2 SATA SSD, however, this option is not valid for M4 platform.
Management IP	It is an optional field but if provided for one server then it is mandatory to provide details for other servers as well.
Storage IP	It is an optional field, but if provided for one server then it is mandatory to provide details for other servers.
Management IPv6	Enter the management IPv6 address.
Vtep IPs	Two input fields for vxlan-tenant and vxlan-ecn ips are available, for any node having compute role, vxlan-tenant and vxlan-ecn in network option.
BGP management addresses	Two input fields for vxlan-tenant and vxlan-ecn ips are available for any node having control role and having vxlan-tenant and vxlan-ecn in network option. IP must be from management subnet, but not from the pool.
trusted_vf	Optional and not reconfigurable. Applicable only for SRIOV node with compute role for C-series pod.
Save	Save the entered information.

ToR Switch Tab

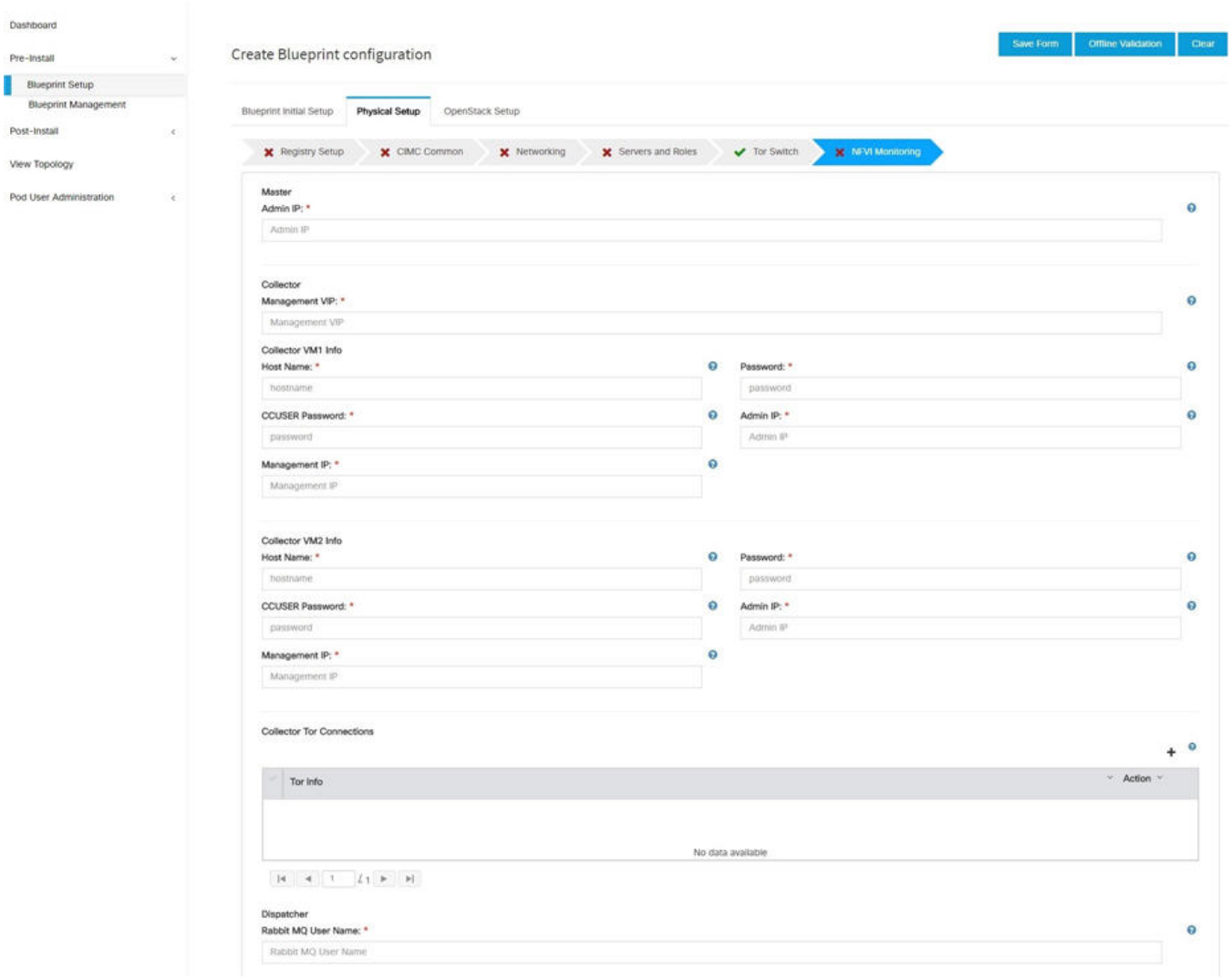
This is an optional section in blueprint setup. Once all the fields are entered, it become a part of the blueprint.



Field	Description
Configure ToR	Changes the configure ToR section from False to True, if enabled.
ToR Switch Information	Click ⊕ to add information for ToR Switch.
Hostname	Denotes the ToR switch hostname.
Username	Denotes the ToR switch username.
Password	Indicates the ToR switch password.
SSH IP	Indicates the ToR switch SSH IP Address.
SSN Num	ToR switch SSN number.
VPC Peer Keepalive	Peer management IP. Must not be defined, if there is no peer.
VPC Domain	Must not be defined, if peer is absent.
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.
Save.	Saves the entered information.
Add ToR Info Connected to Fabric	This field is visible when **Save** is clicked.
Port Channel	Enter the port channel input.
Switch Name	Enter the name of the switch.

NFVI Monitoring Tab

You can unconfigure NFVIMON, once configured.



Fields	Description
Master - Admin IP	IP Address of Control Center VM
Collector - Management VIP	VIP for ceilometer/dispatcher to use, must be unique across VIM Pod
Master 2	Optional, but becomes mandatory if collector 2 is defined. Must contain valid admin IP.
Collector 2	Collector 2 is secondary set of collector. All the properties must be present as collector. Optional, but becomes mandatory if Master 2 is defined. Contains management VIP and collector VM information.
NFVIMON ADMIN	Optional and reconfigurable to add/update user id. Once enabled, you must have only one admin.
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.

Collector ToR Connections	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.
Port Channel	Enter port channel.
Switch - {torSwitch-hostname}	Enter port number, E.g:eth1/15.
Save	Save entered information
Rabbit MQ User Name	Enter Rabbit MQ username.

CVIMMON Tab

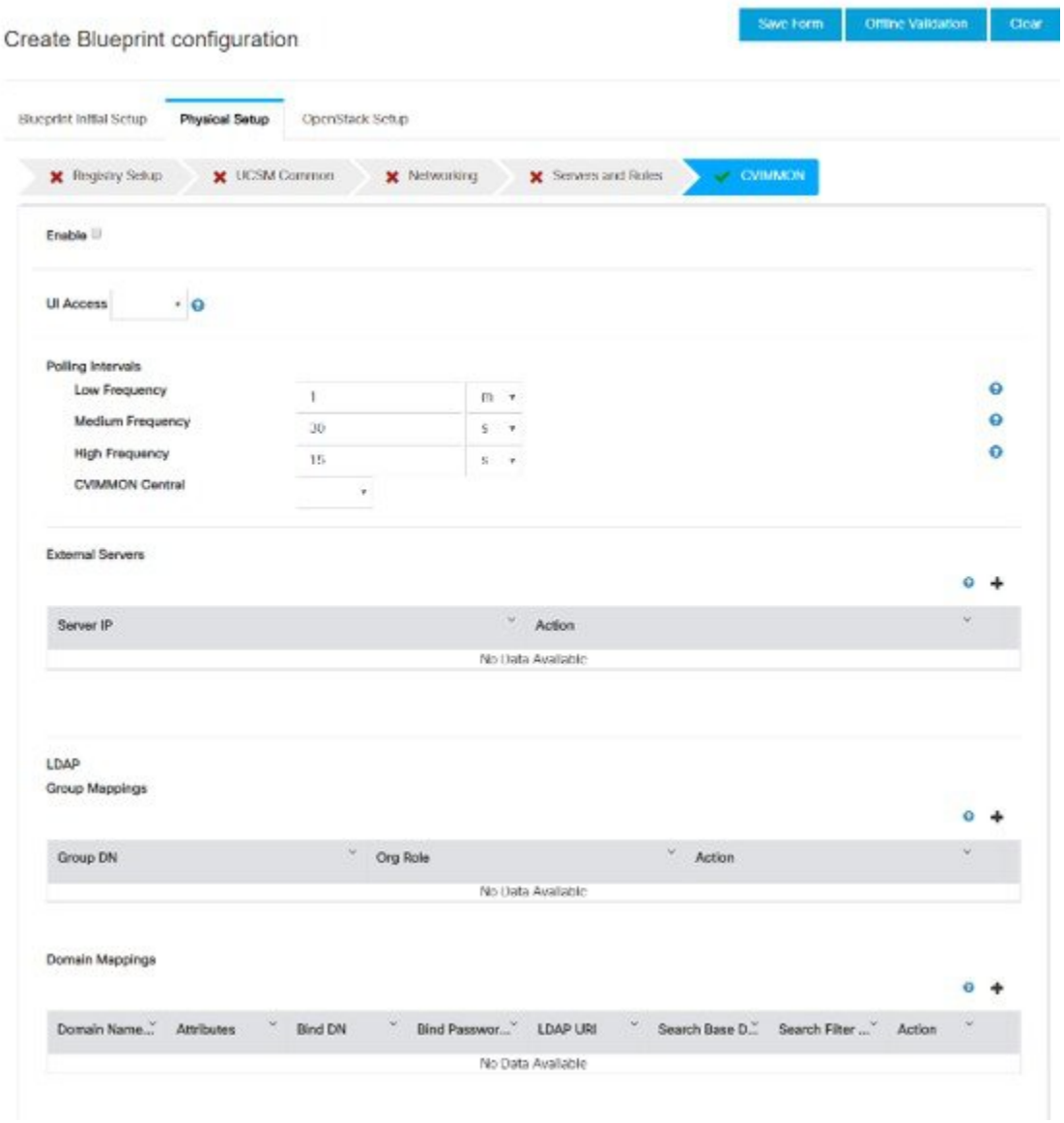
CVIM-MON is a built-in infrastructure monitoring service based on telegraf/prometheus/grafana.
If enabled,

- Telegraf service is deployed on each node on the pod to capture statistics on infrastructure such as CPU, memory, network, containers, and so on.
- Prometheus server is installed on the management node to poll for these statistics and store them in its time series database.

You can view the statistics using the grafana server that is accessible on the management node at port 3000 (password protected).
The three levels of polling intervals used by different telegraf plugins are:

1. Low frequency interval: Used to collect system level metrics like CPU and memory.
2. Medium frequency interval: Used to collect docker metrics.
3. High frequency interval: Used to collect rabbitmq metrics.

Defining polling intervals in setup data is optional. If not defined, the default values are used. PODNAME is required, when CVIM-MON is enabled.



Fields	Description
Enable	By default, it is false. It is case-sensitive and can be True or False.
UI-Access	Optional, and if not defined it is set to True by default. With this option disabled, CVIM_MON with SNMP is available but you cannot access Grafana, Alert-Manager, and Prometheus UIs.
Central	Optional. If not defined, it is set to False by default. With this option enabled, central CVIM-MON is available.
Polling Intervals	Optional. Denotes 's' for seconds, m for minutes, and h for hours.
Low frequency	Minimum of 1 minute (1m) and maximum of 60 mins (1h). If not defined, defaults to 1 minute. It must be more than medium interval.
Medium frequency	Minimum of 30 seconds (30s) and maximum of 60 mins (1h). If not defined, defaults to 30s. It must be more than high interval.
High frequency	Minimum of 10 seconds (10s) and maximum of 60 mins (1h). If not defined, defaults to 15s.
CVIMMON Central	Optional. If not defined, defaults to False. With this option enabled, central CVIM-MON (only telegraf agents running on pod) is available without local Prometheus, AlertManager, or Grafana.
External Servers	Optional. It is the list of external server IPs (v4 or v6) to be monitored by CVIM MON.

CVIMMON LDAP	If defined, the group mappings and domain mappings are mandatory.
group_mappings	Must contain at least one group with the org_role as Admin. Optionally, you can add a second group can with the org_role as Viewer
domain_mappings	Must exactly contain one domain.
domain_name	The domain name must not be empty.
attributes	All subkeys are mandatory.
bind_dn	Describes the user who connects to the LDAP server to check credentials. It can be a read-only user or a group that matches all possible users.
bind_password	The password of the bind_dn user. You must omit this field when the bind_dn is a group.
ldap_uri	URI to connect to the LDAP servers. You must configure at least one. You can configure multiple URIs, separated by a comma.
search_base_dns	Base DNS name to use for all queries.
search_filter	Filter to use for the queries.

If CVIM-MON option is selected in **Blueprint Initial Setup**, an option is provided in the CVIM-MON tab area to enable the SNMP feature. If you enable this SNMP option, **Add a Manager** button is displayed. To add SNMP managers, click **Add a Manager**.

You can add up to three SNMP managers.

Following are various fields related to the SNMP manager:

Fields	**Description**
Address	IPv4 or IPv6 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 of 3 users is allowed.
Name	Username must be unique for the same manager.
auth_key	Requires a minimum of 8 characters.
authentication	Authentication protocol; default: 'SHA'
privacy_key	Encryption password; by default uses the same as the authentication
encryption	Encryption protocol; default: AES128

If CVIM-MON is enabled and platform type is C, an optional feature to get SNMP traps from Cisco CIMC is available in the CVIM-MON tab area. You can enable or disable SERVER_MON and provide host information either as comma separated server information or ALL to include all the servers.

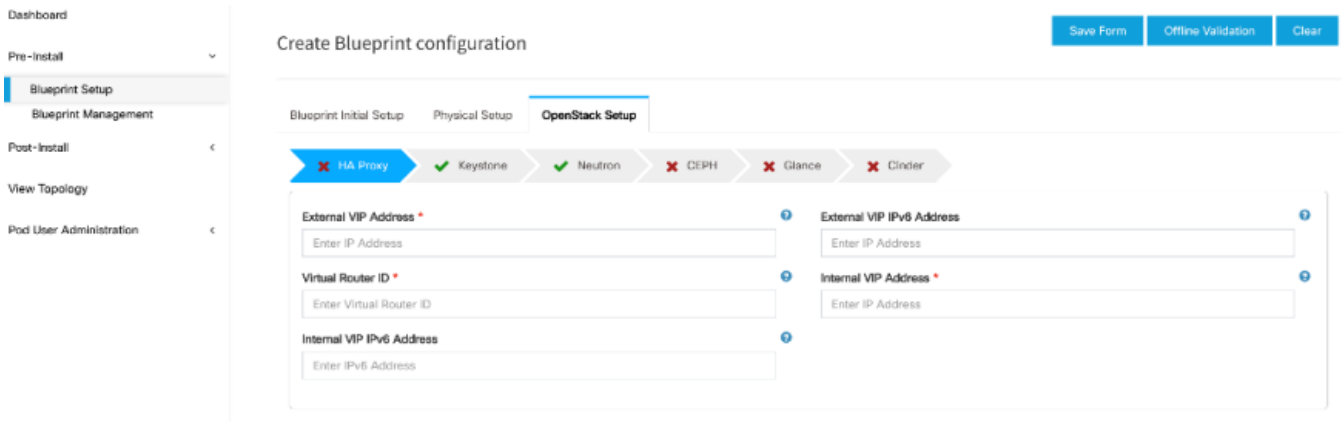
Fields	**Description**
Enable	True/False
Host information	ALL or list of servers.
Remote syslog severity	Optional. Indicates if CIMC is programmed to send rsyslog events with the minimum severity. Possible syslog severity values are: <'emergency' | 'alert' | 'critical' | 'error' | 'warning' | 'notice' | 'informational' | 'debug'>. These are optional and values can be changed.

OpenStack Setup Tab

OpenStack Setup Tab

On the **OpenStack Setup** configuration page of the Cisco VIM Insight wizard, enter the following details:

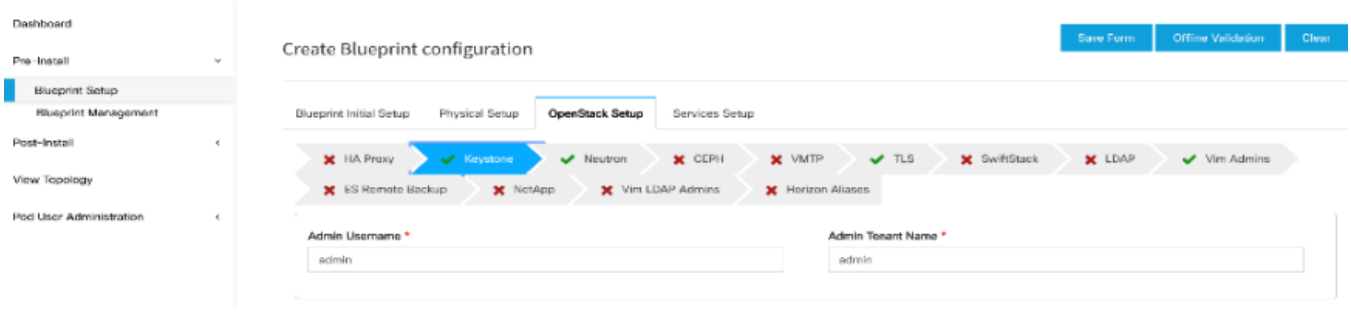
HA Proxy Tab



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

Keystone Tab

Mandatory fields are pre-populated.

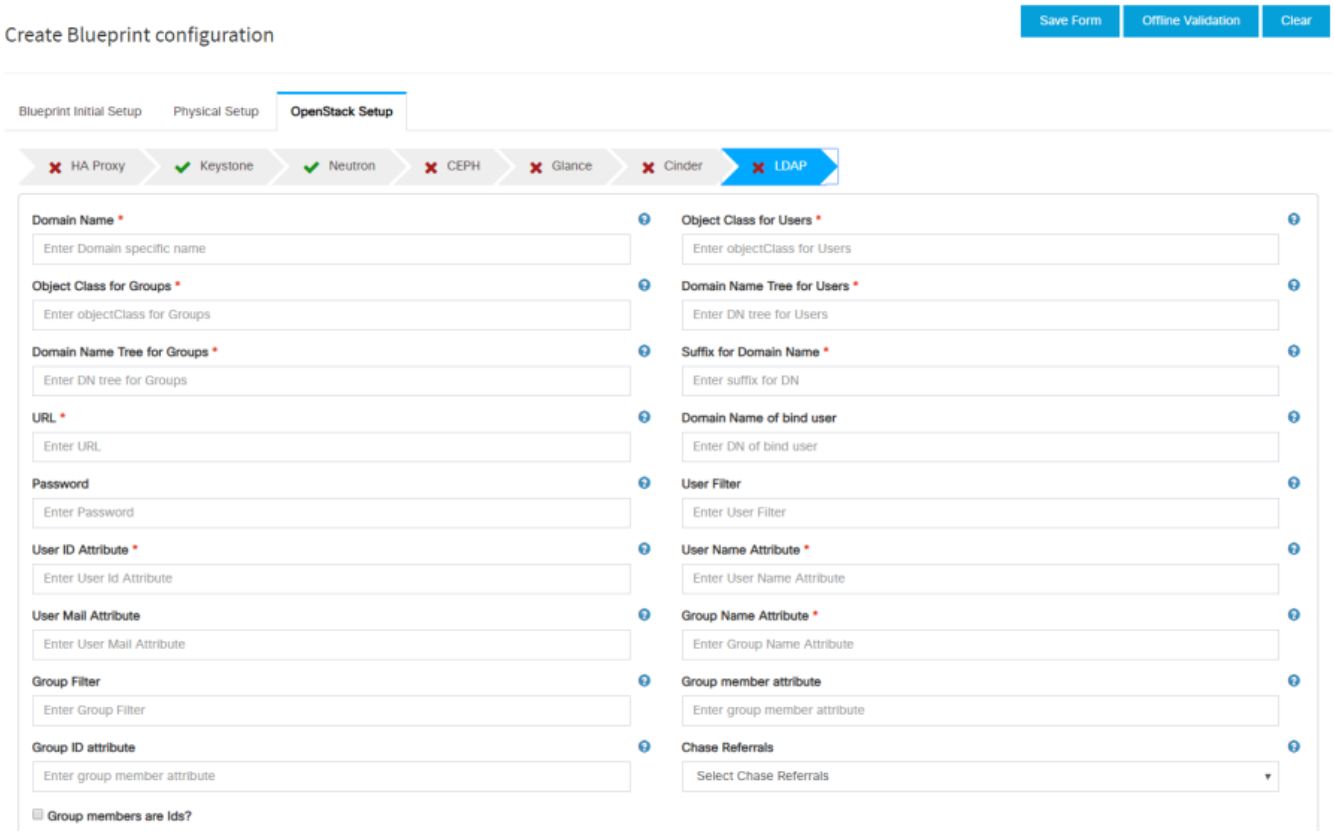


Fields	Description
Admin Username	admin
Admin Tenant Name	admin
LDAP	This option is available only if Keystonev3 is enabled.

LDAP Tab

LDAP enable option is set to False by default.

> This option is only available with Keystone v3. This is available only when LDAP is enabled under **Optional Features and Services** in Blueprint Initial Setup.

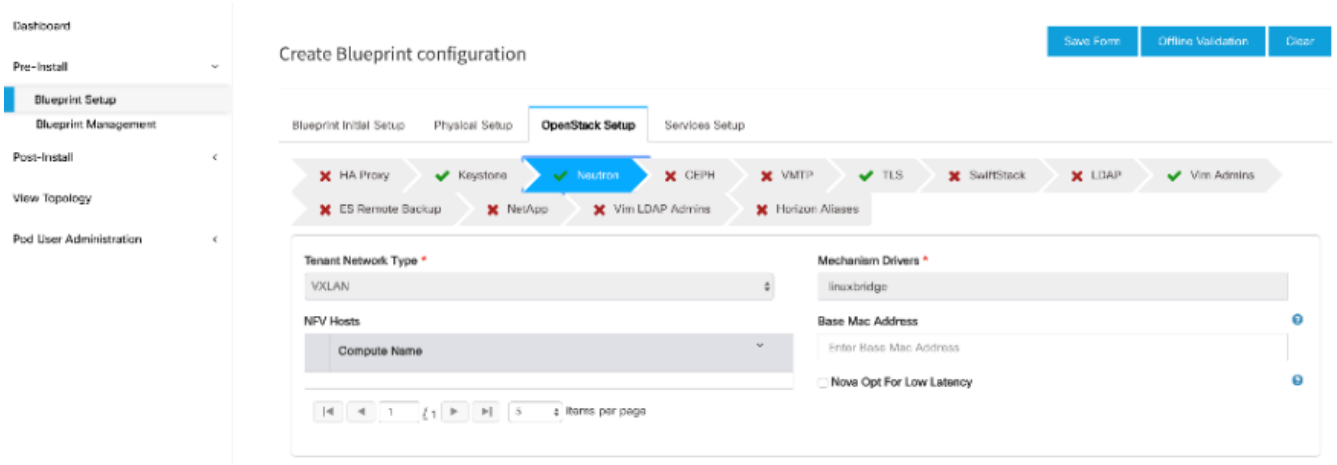


Fields	Description
Domain Name	Enter the domain name.
Object Class for Users	Enter a string as input.
Object Class for Groups	Enter a string.

Domain Name Tree for Users	Enter a string.
Domain Name Tree for Groups	Enter a string.
Suffix for Domain Name	Enter a string.
URL	Enter a URL with ending port number.
Domain Name of bind user	Enter a string.
Password	Enter the password as a string.
User Filter	Enter the filter name as string.
User ID Attribute	Enter the attribute of the user ID as a string.
User Name Attribute	Enter the attribute of the user name as a string.
User Mail Attribute	Enter the attribute of the user's email ID as a string.
Group Name Attribute	Enter the attribute of the group name as a string.
Group_filter	It is optional. Enter the group filter as a string.
Group Member Attribute	It is optional. Enter the attribute of the group member as a string.
Group Id Attribute	It is optional. Enter the attribute of the group ID as a string.
Group Members Are Ids	It is optional. Enter True or False.

Neutron Tab

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:

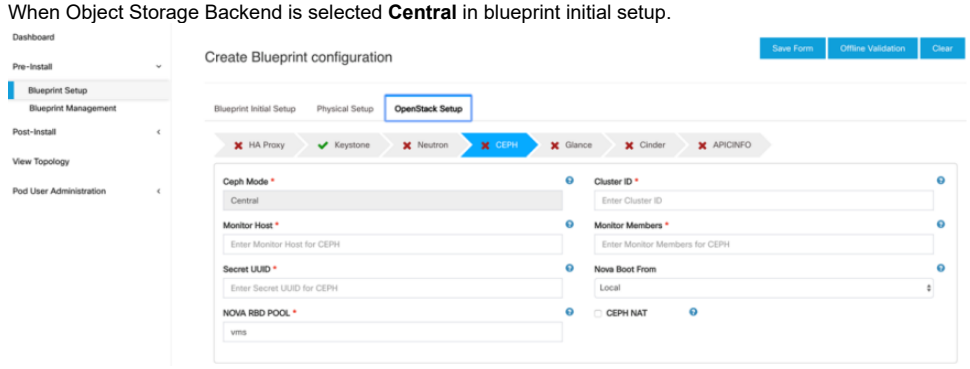


Fields	Description
Tenant Network Type	It is autofilled based on the Tenant Network Type selected in the Blueprint Initial Setup page.
Mechanism Drivers	It is autofilled based on the Tenant Network Type selected in Blueprint Initial Setup page.
NFV Hosts	It is auto-filled with the compute added in Server 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.
ENABLE_CAT	Optional to enable Intel CAT. It is valid only when NFV Host is enabled. By default, it is set to False.
Tenant Network Type	It is autofilled based on the Tenant Network Type selected in the Blueprint Initial Setup page.
Mechanism Drivers	It is autofilled based on the Tenant Network Type selected in Blueprint Initial Setup page.

NFV Hosts	It is autofilled 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.
RESERVED_L3_CACHELINES_PER_SOCKET	Allowed value of reserved cache lines per socket is between 1 and 32. It is valid only when ENABLE_CAT is set to True.
Tenant VLAN Ranges	List of ranges separated by comma form start:end.
Provider VLAN Ranges	List of ranges separated by comma form start:end.
VM Hugh Page Size (available for NFV_HOSTS option)	2M or 1G
Enable Jumbo Frames	Enable the checkbox.
Enable VM Emulator Pin	• Optional, when NFV_HOSTS is enabled. • When a VM is spawned with this parameter enabled, NOVA allocates additional vCPU on top of the vCPU count specified in the flavor, and pin vCPU0 to the pCPU that is reserved in the pool.
VM Emulator PCORES Per Socket	• Optional, if ENABLE_VM_EMULATOR_PIN is enabled. • Enter the number of cores per socket. • Defaults to 1. Can be in the range of 1 to 4.
Base MAC Address	Option for virtual machine MAC addresses. You can configure DHCP reservations for them so that they always get the same IP address regardless of the host hypervisor or operating system that is running. If the MAC address ends with 00:00, • First entry of the first octect must be a Hex • Second entry of the first octect must be 2, 6, a or e For example, [a-f][2,6,a,e]:yz:uv:ws:00:00
Nova Opt for low latency	Optional. You can enable additional real time optimizations in OpenStack NOVA. By default, it is set to False. For Tenant Network Type, Linux Bridge everything remains the same but **Tenant VLAN Ranges** is removed.

CEPH Tab

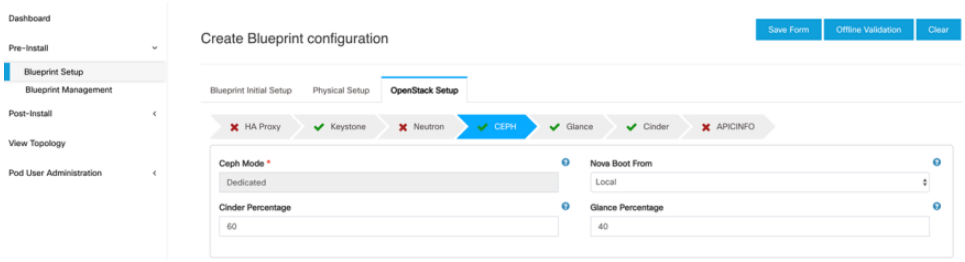
1. When Object Storage Backend is selected **Central** in blueprint initial setup.



Fields	Description
CEPH Mode	By default Ceph Mode is Central.
Cluster ID	Enter the Cluster ID.
Monitor Host	Enter the Monitor Host for CEPH
Monitor Members	Enter the Monitor Members for CEPH
Secret UUID	Enter the Secret UUID for CEPH
NOVA Boot from	You can choose CEPH or local from the drop-down list.
NOVA RBD POOL	Enter the NOVA RBD Pool (default's to vms)

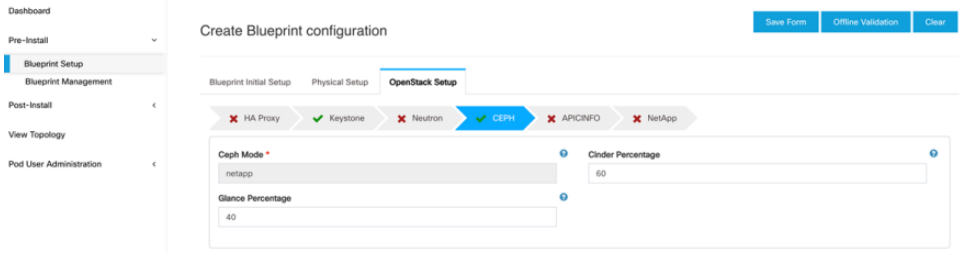
CEPH NAT	CEPH NAT is required for Central Ceph and when mgmt network is not routable.

When Object Storage Backend is selected *Dedicated* in blueprint initial setup for dedicated Ceph.



Fields	Description
CEPH Mode	By default, it is set to *Dedicated*.
Nova Boot From	Can be *Ceph* or *local*.
Cinder Percentage	Must be 60 when **Nova Boot From** is *local*, and must be 40 when **Nova Boot From** is *Ceph*.
Glance Percentage	Available when **Nova Boot From** is *local* or *Ceph*. Must be 40 when **Nova Boot From** is *local*, and must be 30 when **Nova Boot From** is *Ceph*. If Ceilometer is enabled, it must be 35% for **Nova Boot from** *local* and 25% for **Nova Boot From** is *Ceph*.
Nova Percentage	Available when **Nova Boot From** is *Ceph*. Must be 30% otherwise. If **NOVA Boot From** is *local* or *Ceph* the total of **Cinder Percentage** and **Glance Percentage** must be 100.
Gnocchi Percentage	Only applicable when ceilometer is enabled, and must be 5%.
CEPH OSD RESERVED PCORES	Default value is 2. Minimum value is 2 and maximum value is 12 (only for Micropod and hyper-converged pods).

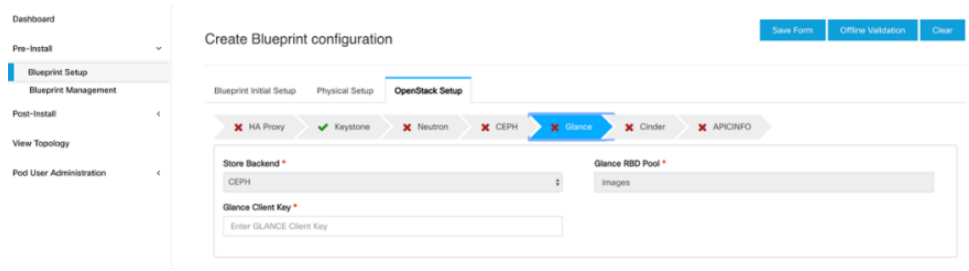
2. When Object Storage Backend is selected *NetApp* in blueprint initial setup.



Fields	Description
CEPH Mode	NetApp is selected by default.
Cinder Percentage	Must be 60%.
Glance Percentage	Must be 40%. Total of **Cinder Percentage** and **Glance Percentage** must be 100.

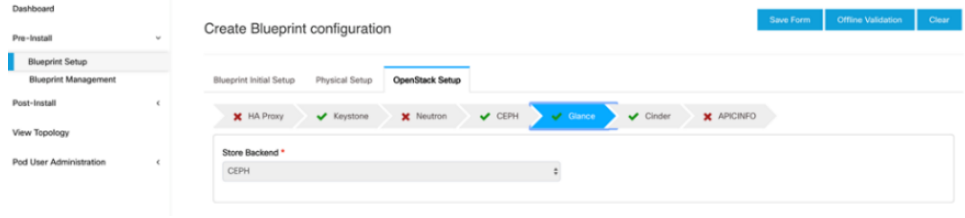
Glance Tab

1. When Object Storage Backend is selected *Central* in blueprint initial setup.



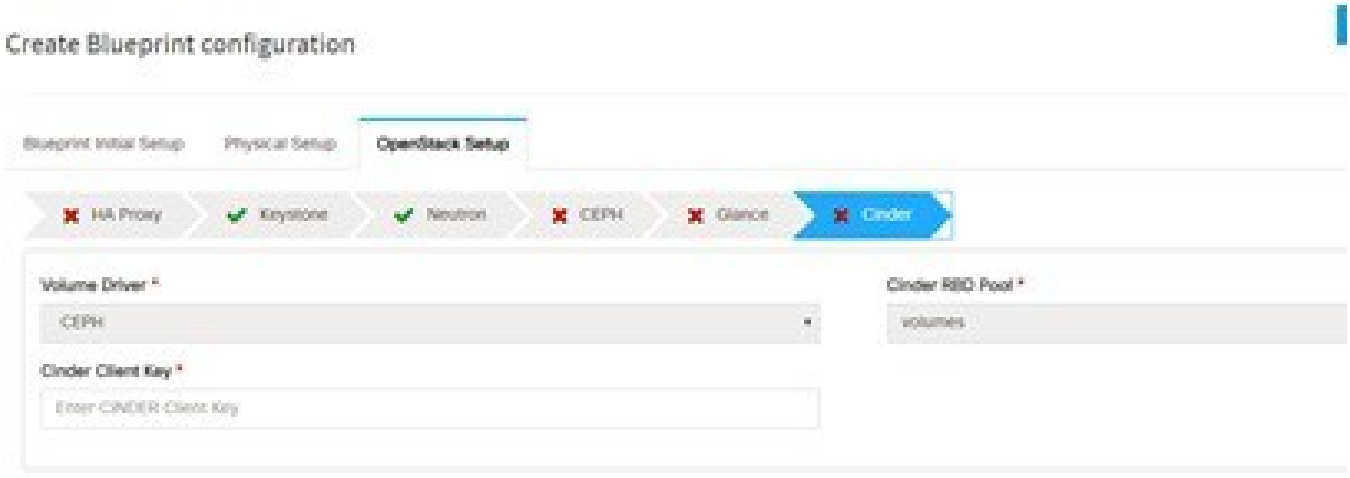
Fields	Description
Store Backend	By default, it is set to CEPH.
Glance RBD Pool	By default, it is set to images.
Glance Client Key	Enter GLANCE Client Key.

2. When Object Storage Backend is selected *Dedicated* in blueprint initial setup.



For CEPH Dedicated, the default value for Store Backend is CEPH.

Cinder Tab



Fields	Description
Volume Driver	By default, it is set to CEPH.
Cinder RBD Pool	By default, it is set to volumes.
Cinder Client Key	Enter the Cinder Client Key

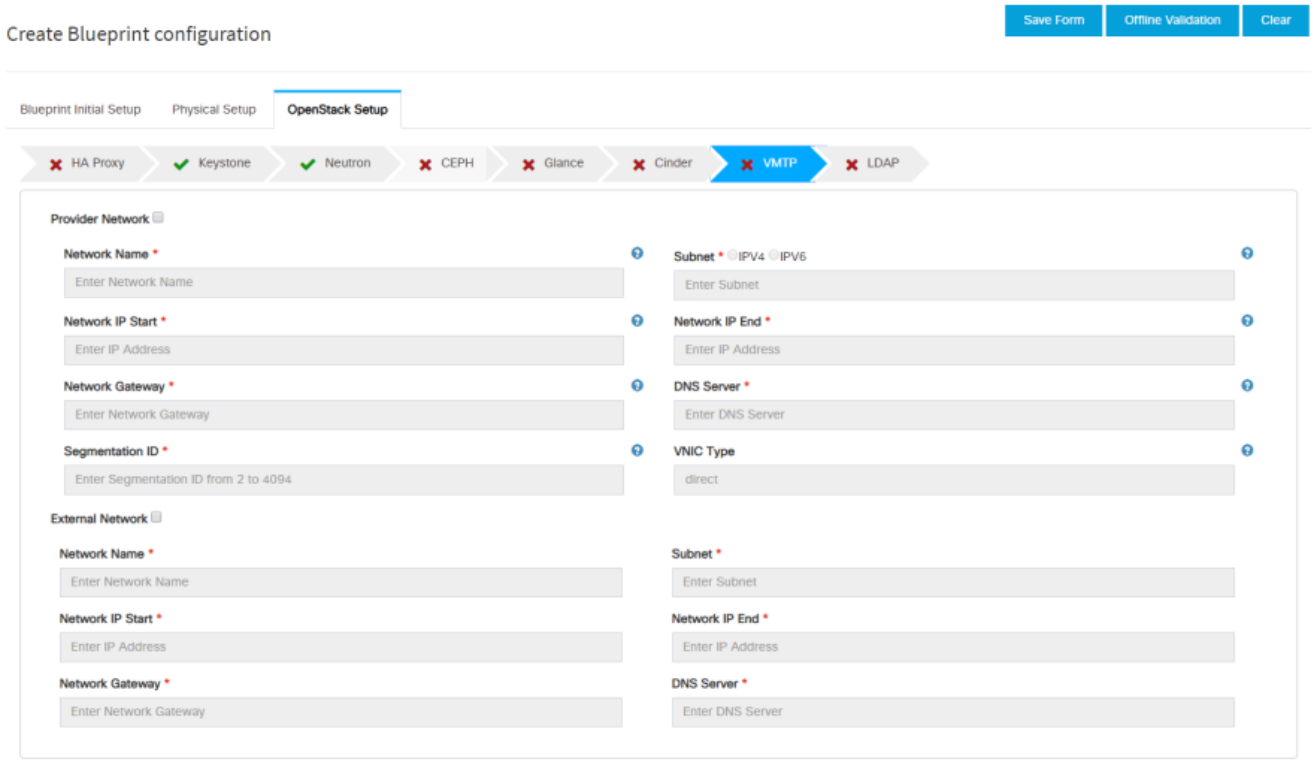
VMTP Tab

VMTP optional section is visible only if VMTP is selected in Blueprint Initial Setup. For VTS tenant type, provider network is only supported.

Check one of the check boxes to specify a VMTP network:

- Provider Network
- External Network

For **Provider Network**, complete the following:



Fields	Description
Provider Network	Select this option to enable provider network.
Network Name	Enter the name of the provider network.
IPv4 Or IPv6	Select either IPv4 or IPv6.
Subnet	Enter the Subnet for provider network.
Network IP Start	Enter the start of the floating IPv4/IPv6 address.
Network IP End	Enter the end of the floating IPv4/IPv6 address.
Network Gateway	Enter the IPv4/IPv6 address for the gateway.
DNS Server	Enter the DNS server IPv4/IPV6 address.
Segmentation ID	Enter the segmentation ID.
IPv6 Mode	Enter the IPv6 address along with the prefix, if IPv6 option is selected.
VNIC Type	For B-series, *Direct* is default value. For C –series, it is either *Default* or *Normal*
PHYSNET NAME	For B-series, the value is phys_prov_fia or phys_prov_fib. For C-series, value like phys_sriov_n is found, where n is number of ports.
External Network	Select this option to enable external network.
Network Name	For external Network, fill in the following details: Enter the name for the external network.
Subnet	Enter the Subnet for the external Network.
Network IP Start	Enter the start of the floating IPv4 address.
Network IP End	Enter the endof the floating IPv4 address.
Network Gateway	Enter the IPv4 address for the Gateway.
DNS Server	Enter the DNS server IPv4 address.

TLS Tab

TLS optional section is visible only if TLS is selected in the **Blueprint Initial Setup** tab.

TLS has two options:

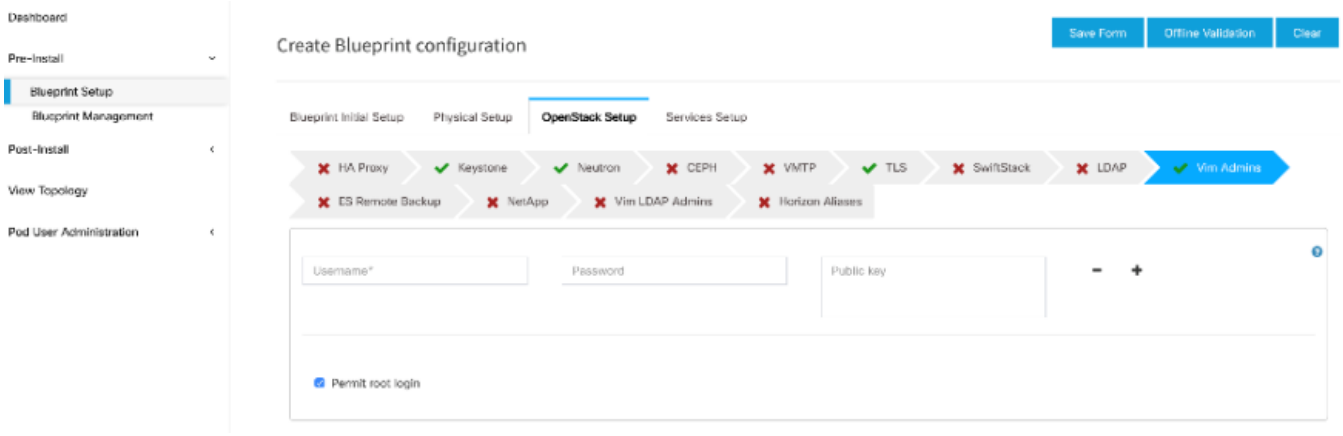
Fields	Description
External LB VIP FQDN	Text Field.
External LB VIP TLS	True/False. By default this option is false.

Vim Admin Tab

Under the OpenStack setup tab, Vim_admins tab is visible only when Vim_admins is selected in the **Optional Features & Services** under the **Blueprint Initial Setup** tab.

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.



Fields	Description
User Name	Enter username for Vim Admin.
Password	Password field. Admin hash password should always start with $6.
Public Key	Public key for vim admin should always start with 'ssh-rsa AAAA….'

SwiftStack Tab

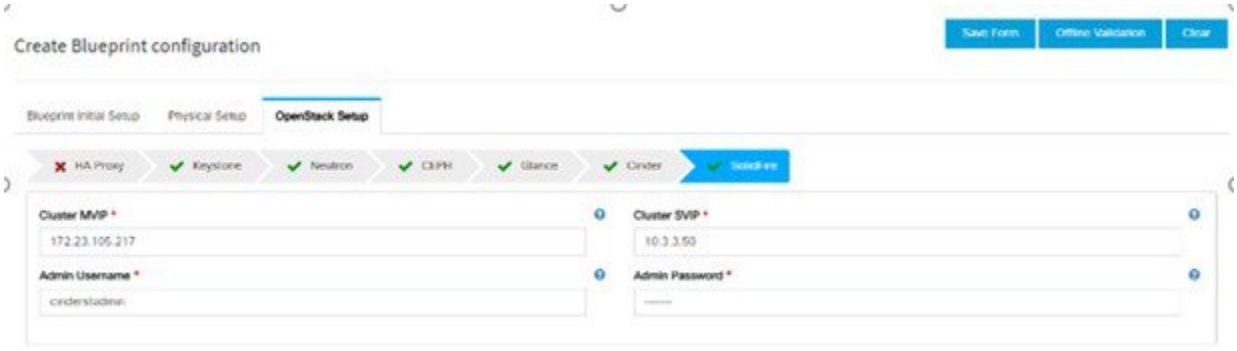
SwiftStack is optional and visible only if SwiftStack is selected in the **Blueprint Initial Setup** tab. SwiftStack is only supported with *KeyStonev2*. If you select *Keystonev3,* you cannot configure SwiftStack.

Following are the options to be filled for SwiftStack:

Fields	Description
Cluster End Point	IP address of PAC (Proxy-Account-Container) endpoint.
Admin User	Admin user for swift to authenticate in keystone.
Admin Tenant	The service tenant corresponding to the Account-Container used by the Swiftstack.
Reseller Prefix	Reseller_prefix as configured for Keysone Auth,AuthToken support in Swiftstack. Example: KEY_
Admin Password	swiftstack_admin_password
Protocol	http or https

SolidFire Tab

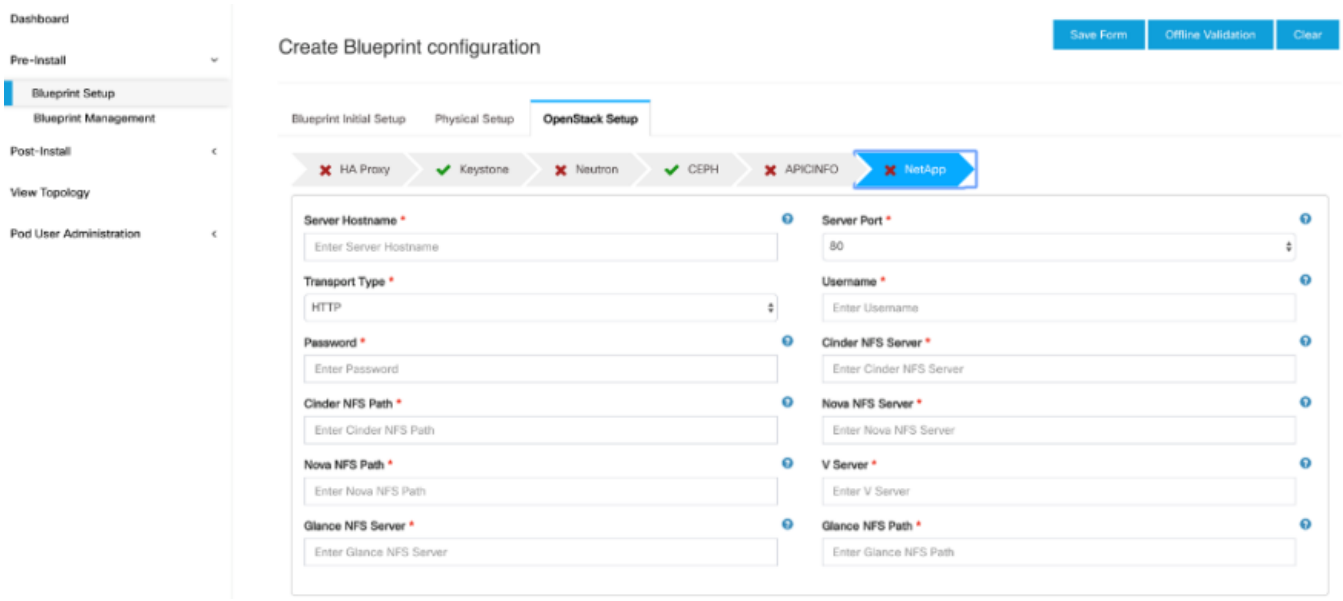
SolidFire is visible for configuration on Day 0. SolidFire is not allowed as a Day 2 deployment option. SolidFire is always available with CEPH.



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

NetApp Tab

It is an optional configuration. No dedicated Ceph is allowed.



Fields	Description
Server Hostname:	It is the IPv4/IPv6/Hostname/FQDN of NetApp management/API server.
Server Port	It is the port of NetApp management/API server. 80 for HTTP 443 for HTTPS.
Transport Type	It is HTTP or HTTPS. Server port depends on Transport type.
Username	It is the username of Netapp API Server.
Password	It is the password of NetApp API Server.
Cinder NFS Server	It is the data path IP of NFS Server. Provide the IPv4/IPv6/Hostname/FQDN
Cinder NFS Path	It is the path of NFS Server.

Nova NFS Server	It is the data path IP of NOVA NFS server. Provide the IPv4/IPv6/Hostname/FQDN.
Nova NFS Path	It is the path of NOVA NFS
V Server	SVM for Cinder NFS volume. Provide the IPv4/IPv6/Hostname/FQDN.
Glance NFS Server	It is the data path of glance NFS server. Provide the IPv4/IPv6/Hostname/FQDN
Glance NFS Path	It is the path of glance NFS server.

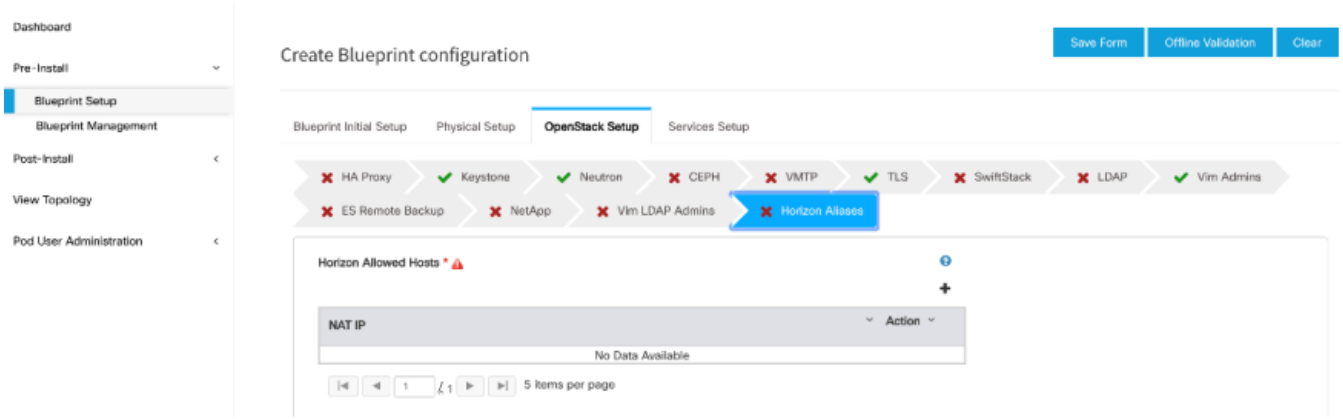
Cloud Settings Tab

This tab is visible only if it is selected in **Blueprint Initial Setup**.

Name	Description
keystone_lockout_failure_attempts	Number of incorrect password attempts before the user is locked out. A default value of 0 indicates no lockout. The minimum value is 0 and maximum is 10.
keystone_lockout_duration	Number of seconds a user is locked out. The default value is 1800 or 30 minutes. The minimum value is 300 or 5 minutes and maximum value is 86400 or 24 hours.
keystone_unique_last_password_count	Enforces the users to change their password to a value not used before. A default value of 0 prevents any check. The minimum value is 0 and maximum is 10.
keystone_minimum_password_age	Enforces the users to change their password after the configured number of days. A default value of 0 removes this restriction. The minimum value is 0 and maximum value is 2.
horizon_session_timeout	Number of seconds of inactivity before the Horizon dashboard logs out. The default value is 1800 or 30 minutes. The minimum value is 300 or 5 minutes and maximum value is 86400 or 24 hours.

Horizon Aliases Tab

If the external_lb_vip is behind a NAT router or with a DNS alias, provide a list of those addresses.

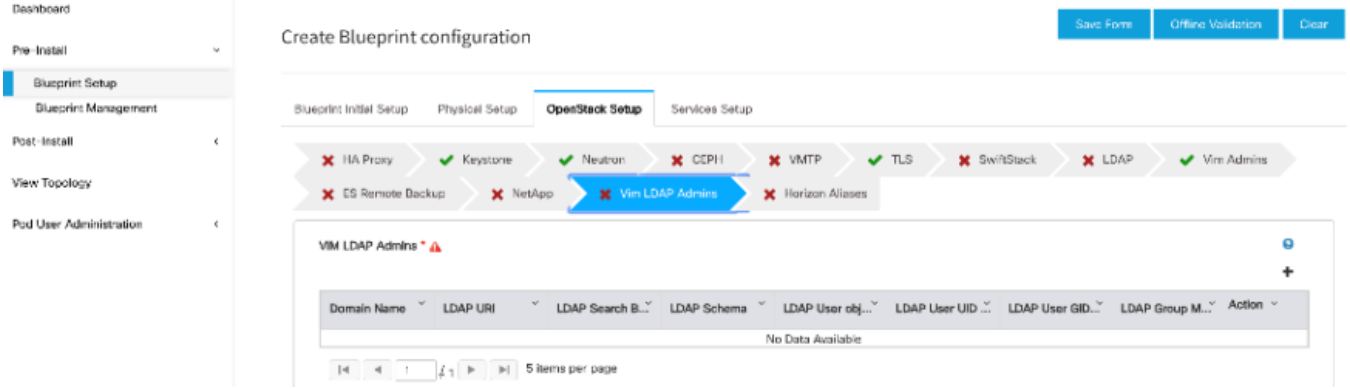


Fields	Description
Horizon Allowed hosts– NAT IP	Uses comma separated list of IP addresses and/or DNS names

Vim LDAP Admins Tab

Optional entry to support LDAP for admin access to management node. For this feature, TLS must be enabled for the external api (i.e. external_lb_vip_tls: True).

Following are the values to be filled to add vim LDAP admins:



Fields	Description
domain_name	Mandatory field. Indicates the domain name to define vim LDAP admins.
ldap_uri	Mandatory. Ensure that ldap_uri is secured over ldaps.
ldap_search_base	Mandatory. Enter search base.
ldap_schema	Optional. Enter the schema.
ldap_user_object_class	Optional. Indicates the posix account.
ldap_user_uid_number	Optional. Indicates the user ID.
ldap_user_gid_number	Optional. Indicates the group ID.
ldap_group_member	Optional. It is the group member ID.
ldap_default_bind_dn	Optional. Enter the default distinguished name
ldap_default_authtok	Optional. Default authentication token
ldap_default_authtok_type	Optional. Default authentication token type.
ldap_group_search_base	Optional. Enter the group search base.
ldap_user_search_base	Optional. Enter the user search base.
access_provider	Optional.
simple_allow_groups	Optional
ldap_id_use_start_tls	Optional. Can be true or false.
ldap_tls_reqcert	Optional. Can be never/allow/try/demand.
chpass_provider	Optional. Can be ldap/krb5/ad/none.

Service Setup Tab

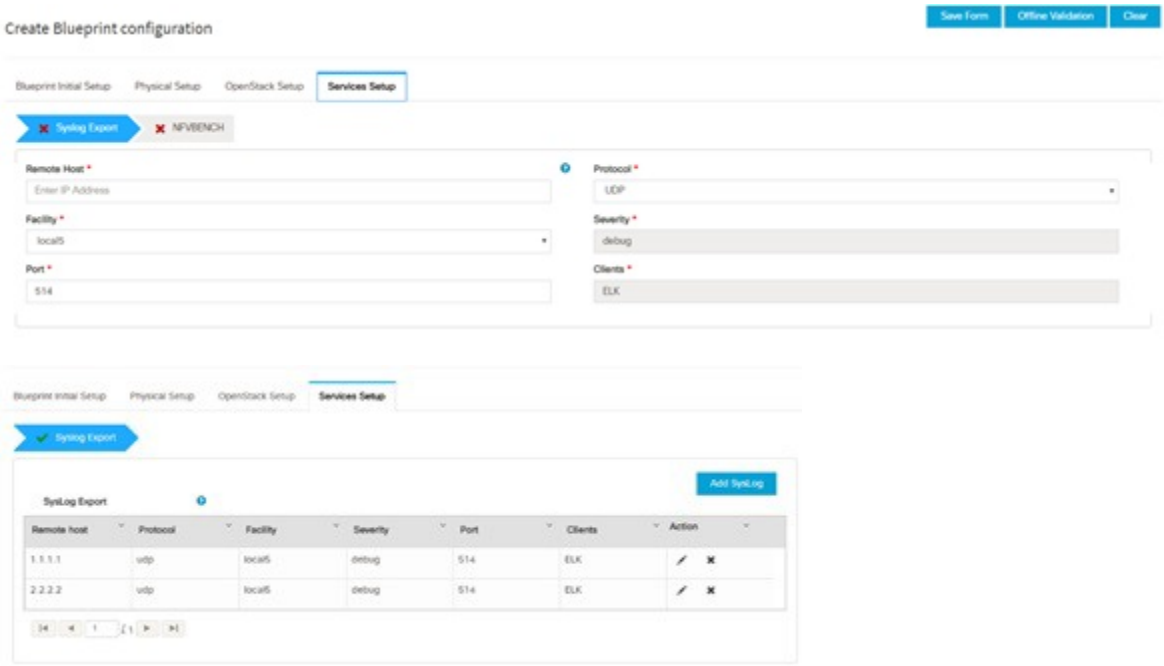
Services Setup Tab

The **Services Setup** page is visible only if **Syslog Export** or **NFVBENCH** is selected in **Blueprint Initial Setup** Page.

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

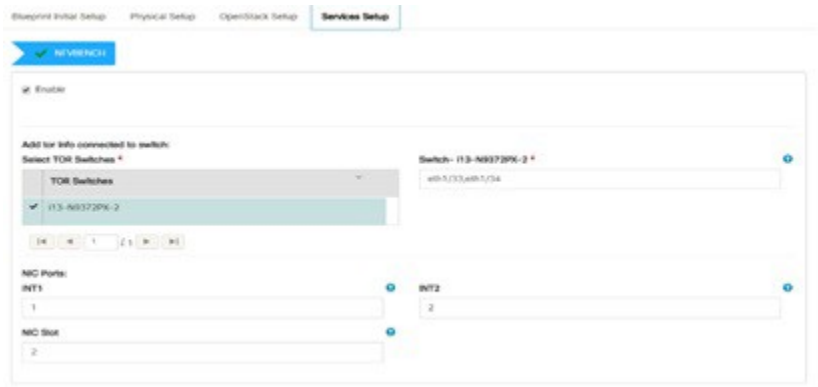
Syslog Export Tab

To view the Syslog settings, click **Syslog Export** tab.



Fields	Description
Remote Host	Enter Syslog IP address.
Protocol	Only UDP is supported.
Facility	Defaults to local5.
Severity	Defaults to debug.
Clients	Defaults to ELK.
Port	Defaults to 514, but can be modified.

NFVBENCH Tab



Fields	Description
Enable	By default, it is set to False. Select this option to enable NFVBench.
Tor Switch	Enter the Switch name, port number and VLANs (VLAN1 and VLAN2). For example: eth1/5 . VTEP VLANS (mandatory and needed only for VTS/VXLAN).
ENABLE_ESC_ PRIV	Enable this option to set it as True. By default, it is False.
NIC Ports	INT1 and INT2 are optional. Enter the 2 port numbers of the 4-port 10G Intel NIC at the management node used for NFVbench.
VTEP IP	For mechanism driver VPP, this is optional if network option is present.
VNI	For mechanism driver VPP, this is optional if network option is present. It is mandatory for NFVbench with VXLAN, and must be comma separated vnid_id pairs.
VTEP Ips	For mechanism driver VTS: Mandatory only for VTS/VXLAN. Comma separated IP pair belongs to tenant network segment, but not in tenant network pool.

C-Series Blueprint Creation

C-Series Blueprint Creation

Creating Blueprint for C-Series

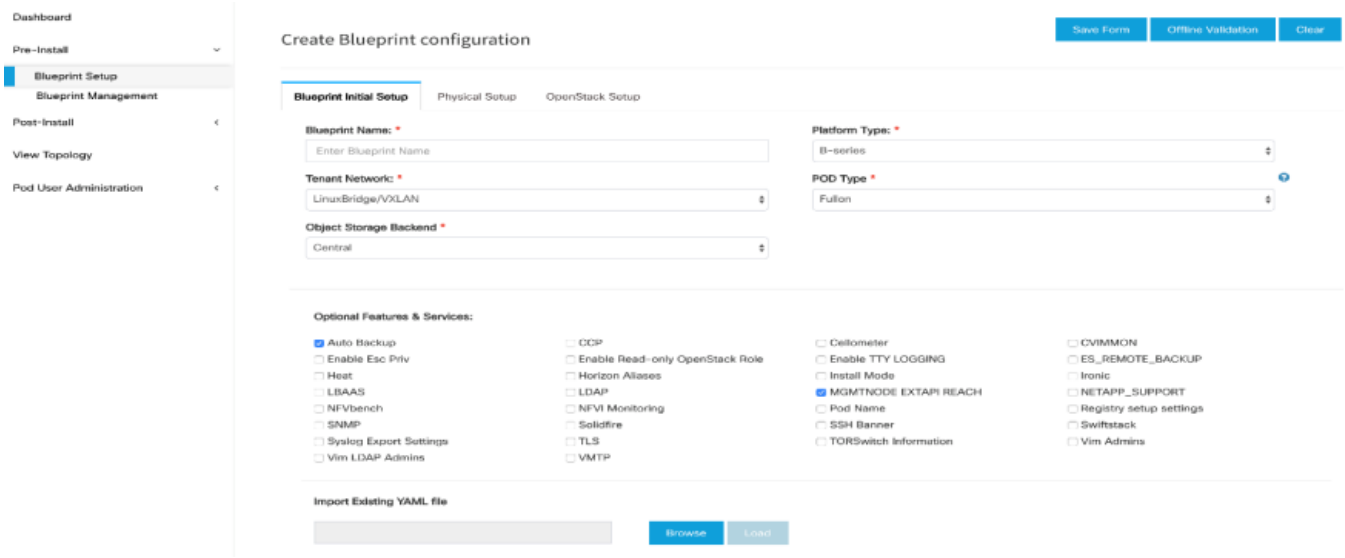
Creating Blueprint for C-Series

1. Log into **Cisco VIM Unified Management** or **Insight**.
2. In the navigation pane, choose **Pre-Install** > **Blueprint Setup**. For blueprint setup, click Blueprint Initial Setup Tab
3. For operations related to physical setup, click Physical Setup Tab
4. For operations related to OpenStack setup, click OpenStack Setup Tab
5. For operations on service setup, click Service Setup Tab.

Blueprint Initial Setup Pane

Blueprint Initial Setup Pane

On the **Blueprint Initial Setup** pane of the Cisco VIM Unified Management or insight, complete the following fields:



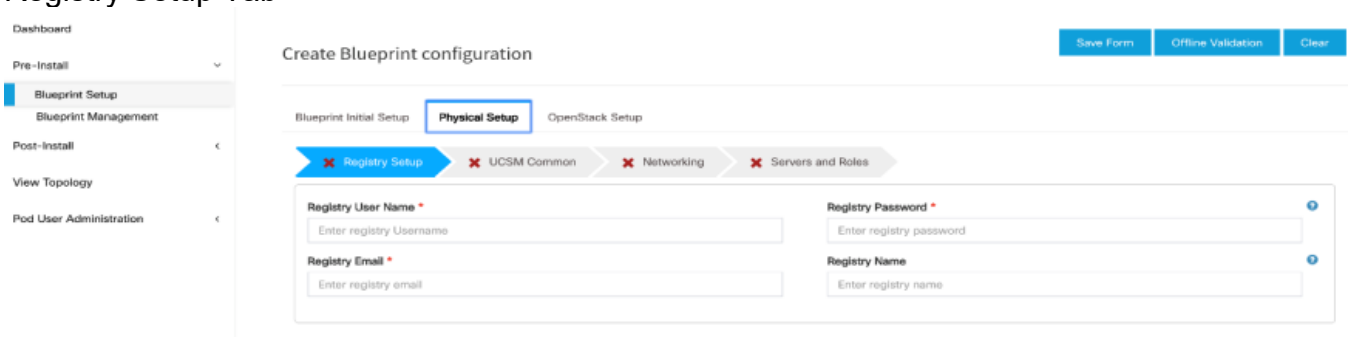
Fields	Description
Blueprint Name	Enter the name for the blueprint configuration.
Platform Type	Choose one of the following platform types: • B-Series (By default) • C-Series (Select C-Series)
Tenant Network	Choose one of the following tenant network types: • Linux Bridge/VXLAN • OVS/VLAN • VTS/VLAN • VPP/VLAN ⚠ If VTS/VLAN is selected, the respective tabs are available on Blueprint setup. If mechanism driver OVS is selected and NFV_HOSTS is enabled, VM_HUGEPAGE_PERCENTAGE field is enabled for all standalone compute nodes.
Pod Type	Choose one of the following pod type : • Fullon(By Default) • Micro • UMHC • NGENAHC ⚠ • 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 and VPP/VLAN.
Ceph Mode	Choose one of the following Ceph types: • Dedicated (By default). • Central. It is not supported in Production.

Optional and Services Features	LDAP, Syslog Export Settings, Install Mode, TorSwitch Information, TLS, NFVMON, Pod Name, VMTP, NFVbench, Autbackup, Heat, Keystone v3, and 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 automatically populates the fields and highlights any missed mandatory in the respective section.
SSH Banner	Optional parameter ssh_banner is available in the setup_data, to accept a string or message that is to be displayed before the login prompt. This message indicates a warning in consistent with company's IT policies.

Physical Setup Pane

Physical Setup Pane

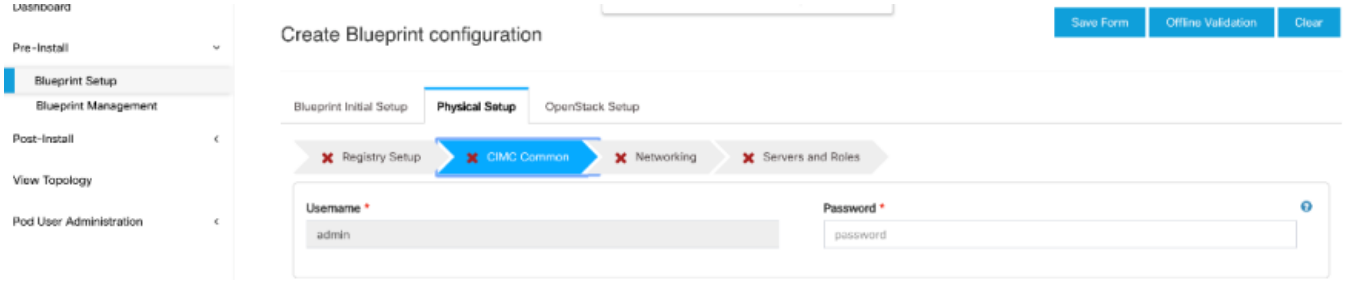
Registry Setup Tab



Fields	Description
Registry User Name	It is a mandatory field. Denotes the User Name for registry.
Registry Password	It is a mandatory field. Denotes the password for registry.
Registry Email	It is a mandatory field. Indicates the email ID for registry.

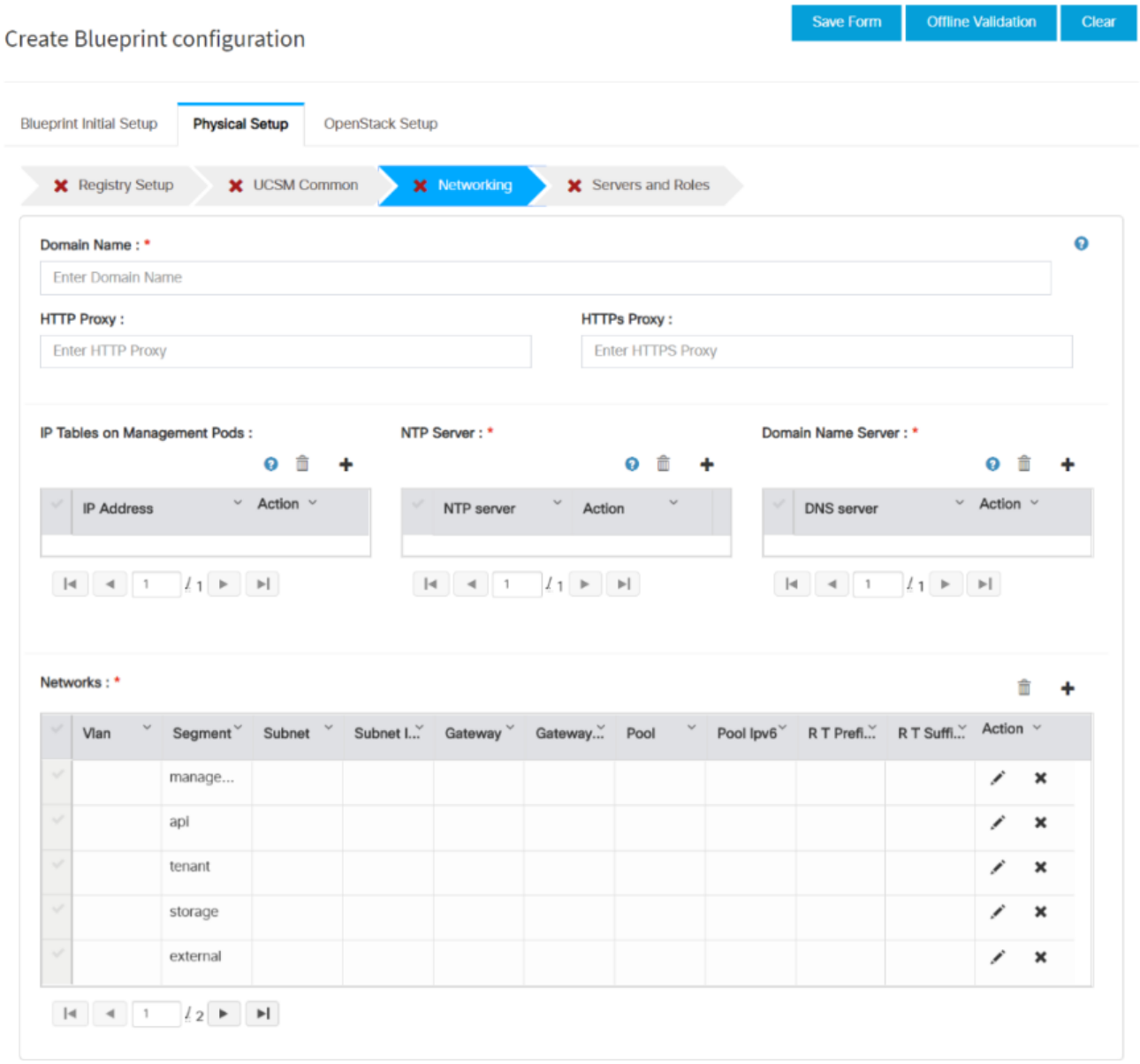
Once all the mandatory fields are filled, the **Validation Check Registry Page** is changed to a Green Tick.

CIMC Common Tab



Fields	Description
User Name	By default, the value is Admin and is disabled.
Password	It is a mandatory field. Enter the password for UCSM Common.

Networking Tab

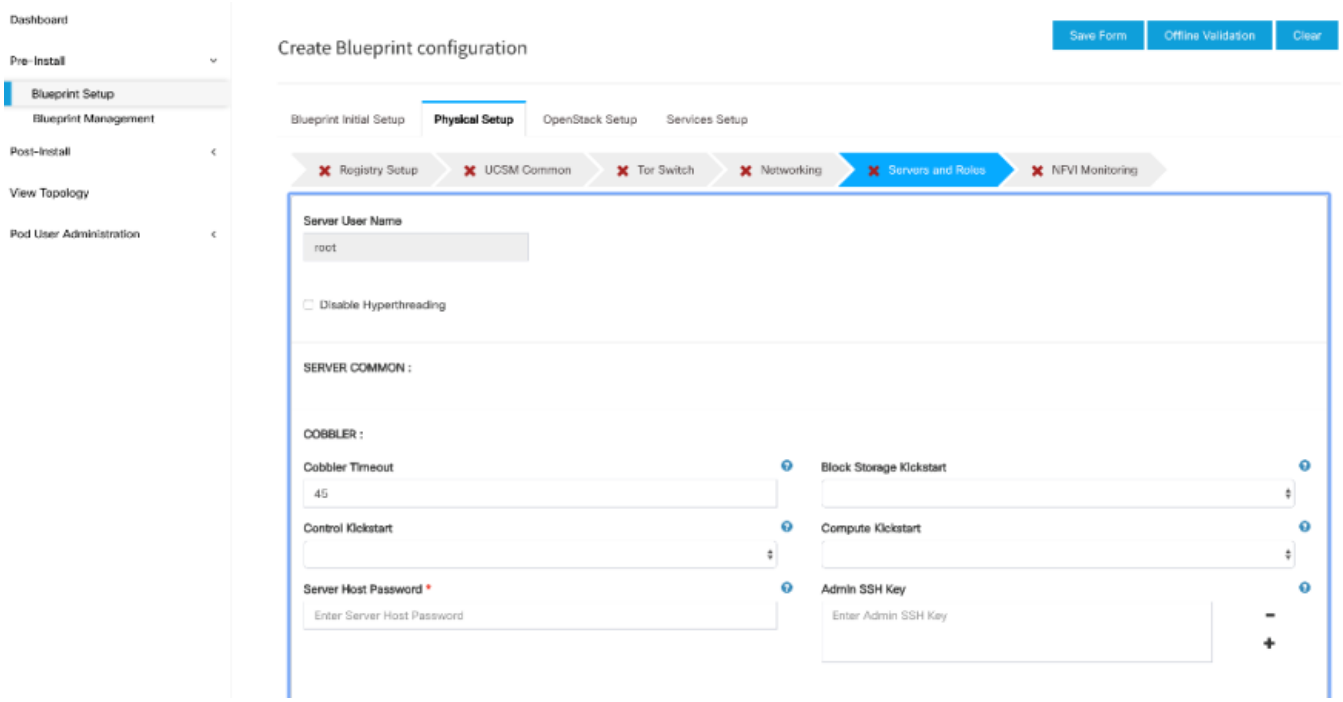


Fields	Description
Domain Name	It is a mandatory field. Enter the domain name.
HTTP Proxy Server	If your configuration uses an HTTP proxy server, enter the IP address of the server.
HTTPS Proxy Server	If your configuration uses an HTTPS proxy server, enter the IP address of the server.
IP Tables on Management Pods	Specifies the list of IP addresses with a mask.
NTP Servers	Enter a maximum of four and a minimum of one IPv4 and/or IPv6 addresses in the table.
Domain Name Servers	Enter a maximum of three and a minimum of one IPv4 and/or IPV6 addresses.
Networks table	Network table is pre-populated with segments. You can either clear all the tables with **Delete all** or click **edit** for each segment and enter the details. You can add, edit, or delete network information in the table. To add new entries (networks) to the table, click **Add** ⊕.
VLAN	Enter the VLAN ID. For Segment - Provider, the VLAN ID value is *none*.

Segment	When you add/edit a new segment, then the following segments types are available in the form of a drop-down list. You can select only one. • API • Management/provision • Tenant • Storage • External • Provider
Subnet	Enter the IPv4 address for the subnet.
IPv6 Subnet	Enter IPv6 address. This field is available only for management provision and API
Gateway	Enter the IPv4 address for the gateway.
Gateway IPv6	Enter the IPv6 address for the gateway. Provides support for API and management provision.
Pool	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 Management/Provision, Storage, and Tenant segments.
IPv6 Pool	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 Allowed only when ToR is NCS-5500. Can only be defined for management/provision, storage, and tenant segments
Save	Saves the entered information

Servers and Roles Tab

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



If you choose OVS as mechanism driver, VM_HUGEPAGE_PERCENTAGE field is available for compute nodes. You can choose values from 0 to 100%, when NFV_HOSTS: ALL is chosen. Also, the option of NIC level redundancy appears only when Intel NIC Support is set to True. This is applicable only for M5 based pods.

Fields	Description
Server User Name	Enter the username of the Server
	By default, it is set to False. You can set it as True or False.

Disable Hyperthreading	
Cobbler	Enter the Cobbler details in the following fields.
Cobbler Timeout	The default value is 45 minutes. This is an optional parameter. Timeout is displayed in minutes, and its value ranges from 30 to 120.
Block Storage Kickstart	Kickstart file for storage node.
Admin Password Hash	Enter the Admin Password. The password must be alphanumeric. The password must contain a minimum of 8 characters and a maximum of 32 characters.
Cobbler Username	Enter the cobbler username to access the cobbler server.
Control Kickstart	Kickstart file for control node.
Compute Kickstart	Kickstart file for compute node.
Cobbler Admin Username	Enter the admin username of the Cobbler.

Add Entry to Servers and Roles	Click **Edit** or **+** to add a new server and role to the table.
	If mechanism driver is OVS, an additional optional field VM_HUGEPAGE_PERCENTAGE is shown when compute role is chosen; This option is valid only when NFV_HOSTS is set to ALL.
	
	If no value is entered, the global value of VM_HUGEPAGE_PERCENTAGE is used.
	
	⚠ If pod-type micro is selected, all the three servers are 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
	
	⚠ If pod type UMHC is selected, the auto-ToR configuration is not supported and the entry of ToR information at server and role level is not allowed.

Server Name	It denotes the name of the server.
Rack ID	Denotes the rack ID for the server.
VIC Slot	Enter a VIC Slot.
CIMC IP	Enter an IP address. Both IPv4 and IPv6 supported.
CIMC Username	Enter a Username.
CIMC Password	Enter a password for CIMC.
Role	Select the **Role** from the dropdown list. Choose Control, Compute, or Block Storage from the dropdown list. If Podtype is *fullon* and selected role type is Block storage, an additional field Osd_disk_type is displayed where you can choose either HDD or SSD.

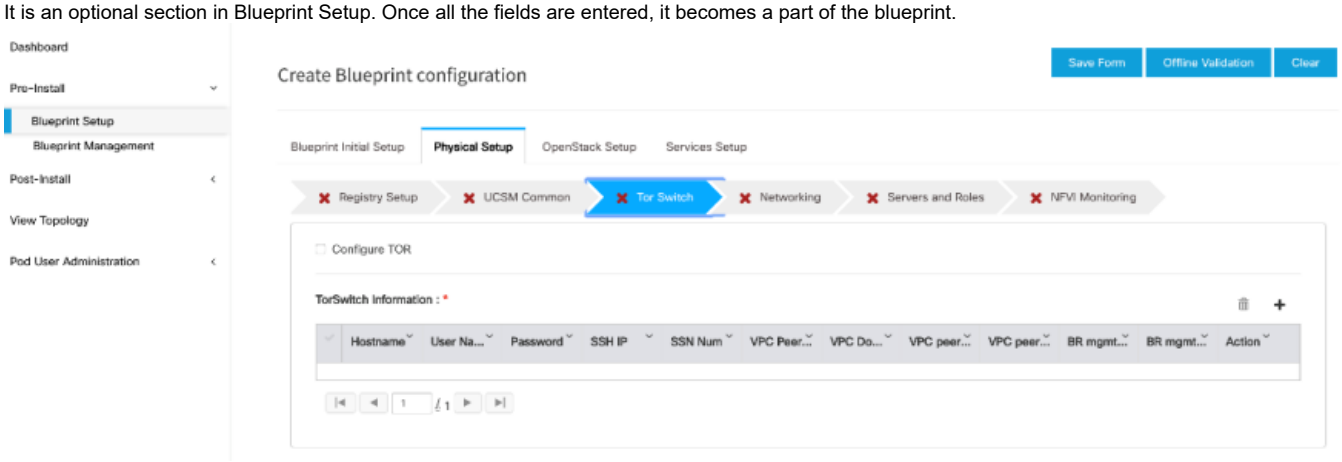
VIC Admin FEC mode	Applicable only for Cisco VIC that supports to change the admin FEC mode. It can be auto/off/cl74/cl91.
Root Drive Type	Optional. From the drop-down list, choose HDD, SSD or M.2_SATA internal SSD. You must choose M.2_SATA if booting off M.2 SATA SSD, however, this option is valid only for C series and not valid for M4 platform.
VIC Port Channel Enable	Optional. Default, it is set to True. It can be either True or False.
Secure Computing mode	Optional. By default, it is set to 1. If not defined, it can be 0 or 1.
Nova CPU Allocation Ratio	Optional, overrides the NOVA_CPU_ALLOCATION_RATIO defined in openstack_config.yaml. Values are in the range of 0.958 to 16.0.
Nova RAM Allocation Ratio	Optional, overrides the NOVA_RAM_ALLOCATION_RATIO defined in openstack_config.yaml. Values are in the range of 1.0 to 4.0
VM Hugepage Size	Optional, 2M or 1G. Overrides the global VM_HUGEPAGE_SIZE value, if NFV_HOSTS is enabled.
Disable Hyperthreading	True or False. Optional, overrides the global hyper-threading configuration.
Root Drive Type	Optional, HDD or SSD in front or rear drive bay. M.2_SATA internal SSD. It is a mandatory configuration if booting off M.2 SATA SSD, and not valid for M4 platform.
Management IP	It is an optional field but if provided for one server then it is mandatory to provide for other servers.
Storage IP	Optional, but if provided for one server then it is mandatory to provide details for other servers.
Vendor	Allow static override value for platform vendor instead of dynamic discovery at runtime. Can be CISCO - Cisco Systems Inc/ QCT - Quanta Cloud Technology Inc/ HPE - Hewlett Packard Enterprise.
Management IPv6	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.
BGP speaker addressees	Optional, only when NETWORK_OPTIONS is vxlan network. For the controller node, IP belongs to the vxlan-tenant network but not part of the pool.
INTEL_SRIOV_VFS	The value range is 1 to 32. It can be defined globally and overridden at per compute level via add/remove or fresh installation, if Intel N3000 card is installed for pod type edge.
NUM GPU CARDS	Optional. Applicable for a server with GPU. Enter a value from 0 to 6.
INTEL_FPGA_VFS	The value range is 1 to 8. It can be defined globally and overridden at per compute level via add/remove or fresh installation if Intel N3000 card is installed for pod type edge.
INTEL_VC_SRIOV_VFS	The value range is 1 to 32. It can be defined globally and overridden at per compute level via add/remove or fresh installation if Intel N3000 card is installed for pod type edge.
Save or Add	On clicking **Save or Add** all information related to Servers and Roles gets saved.
Configure ToR	If **Configure ToR** option is True with at-least one switch detail, these fields are displayed for each server and this is similar to DP ToR: **Port Channel and Switch Name.** Mandatory if **Configure ToR** is set to True.
Port Channel	Enter the port-channel input.
Switch Name	Enter the switch name.
Switch Port Info	Enter the switch port information.
DP ToR	Applicable only for control and compute nodes. Mandatory if Intel NIC support and Configure ToR are True.
Port Channel	Enter the port-channel input.
	Enter the switch name.

Switch Name	
Switch Port Info	Enter the switch port information.
SRIOV TOR INFO	Applicable only for compute nodes. It is mandatory in server and roles, if Intel NIC support and Configure ToR are True with ToR type Nexus. For ToR type NCS-5500, these fields are optional. This field appears only when Intel NIC support is true, as the auto ToR configuration is not supported in VIC_NIC combination.
Switch Name	Enter the switch name. Mandatory if Configure ToR is True.
Switch Port Info	Enter the switch port information.
Intel SRIOV VFS	Valid for Intel NIC testbeds and can be an integer. For SRIOV support for Intel NIC. By Default, SRIOV support is disabled. To enable, define a value in the range # * 1-32 when INTEL_NIC_SUPPORT is set True (X710 Max VFs = 32) # * 1-63 when CISCO_VIC_INTEL_SRIOV is set True (X520 Max VFs = 63)
INTEL_SRIOV_PHYS_PORTS	Valid for Intel NIC test beds and can be of value 2 or 4. By default, it is 2. In some cases, the number of physical SRIOV port needed is 4. To meet that requirement, define the following: # this is optional. If nothing is defined, code assumes it to be 2. The only two 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.
Save or Add	If all mandatory fields are entered, 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.
Save	Saves the entered information.

- Maximum of two ToR information must be configured for each connection type on each node (control, compute and block_storage node).
- If pod-type UMHC is selected, CISCO_VIC_INTEL_SRIOV is set to True.
- CISCO_VIC_INTEL_SRIOV is also supported on Micropod with expanded computes.
- For Tenant type network, port-channel for each ToR port is not available in servers and roles, as APIC automatically assigns the port-channel numbers.

ToR Switch Tab

It is an optional section in Blueprint Setup. Once all the fields are entered, it becomes a part of the blueprint.



Field	Description
Configure ToR	Optional. If enabled, configure ToR section is changed from False to True. - If **UMHC** is selected as podtype, configure ToR is disabled. - If Configure ToR is True, ToR switch information is mapped on servers.

ToR Switch Information	Mandatory. If you want to enter ToR information, click ⊕ to add information for ToR Switch.
Name	Indicates the ToR switch name.
Username	Indicates the ToR switch username.
Password	Indicates the ToR switch password.
SSH IP	Denotes the ToR switch SSH IP.
SSN Num	Specifies the ToR switch ssn num.
VPC Peer Keepalive	Peer Management IP. You cannot define if there is no peer.
VPC Domain	Cannot be defined if no peer is found.
VPC Peer Port Info	Interface for vpc peer ports.
VPC Peer VLAN Info	Optional. VLAN ids for vpc peer ports.
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.
Save	Saves the entered information

⚠ If tenant type ACI/VLAN is selected, the ToR switch information table differs and is mandatory.

Fields	Description
Configure ToR	Is not checked, as by default ACI configures the ToRs.
Host Name	Provide ToR switch name.
User Name	Provide ToR switch user name.
SSH IP	ToR switch SSH IP.
SSN Num	ToR switch SSN num.
VPC Peer keep alive	Entered peer must exist in pairs.
VPC Domain	Enter an integer.
BR Management Port Info	Enter BR management port information, for example, Eth1/19, at least one pair must exist.
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).
Enter Node ID	Entered integer must be unique.

⚠ If ToR_type is NCS-5500, the ToR switch information table differs and is mandatory.

Fields	Description
Configure ToR	Optional. Set to True if enabled.

	⚠ • If Configure ToR is true, ToR switch information is mapped on servers. • If NSC-5500 is selected as ToR type, configure ToR is set as mandatory. • If you want to enter NCS details, enter the **NCS-5500 Information** table. To add information for NCS-500 Switch, click ⊕
HostName	Enter the NCS-5500 hostname.
Username	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.
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).
VPC Peer Port Info	Interface for vpc peer ports.
VPC Peer Port Address	Address for ISIS exchange.
ISIS Loopback Interface address	ISIS loopback IP Address.
ISIS net entity title	Enter a string.
ISIS prefix SID	Integer range is 16000 to 1048575. Optional, if ToR type is NCS-5500. Entry not allowed, if ESI_PREFIX is defined.

When ToR type is NCS-5500 and two NCS-5500 are configured, it is mandatory to configure MULTI_SEGMENT_ROUTING_INFO.

Fields	**Description**
BGP AS Number	Integer range is 1 to 65535.
ISIS Area Tagfield	Must be a valid string.
Loopback Interface name	Loopback Interface name.
API bundle ID	Integer range is 1 to 65535.
API bridge domain	Optional. Required when br_api of mgmt node is also going through NCS-5500. This item and api_bundle_id are mutually exclusive.
EXT bridge domain	A valid string (user pre-provisions physical, bundle interface, sub-interface and external BD for external uplink and provides external BD info setup_data).

When ToR-type is NCS-5500, you can optionally define ESI_PREFIX.

Fields	**Description**
ESI_PREFIX	Ethernet-segment identifier type Example: 91.<Pod_number>.<pod_region_number>.00.00.00.00.

NFVI Monitoring Tab

NFVIMON can be un-configured once configured.

Create Blueprint configuration

Save Form | Offline Validation | Clear

Blueprint Initial Setup | **Physical Setup** | OpenStack Setup

✖ Registry Setup | ✖ CIMC Common | ✔ Tor Switch | ✖ Networking | ✖ Servers and Roles | ✖ NFVI Monitoring

Master ⚠

Admin IP: *

Admin IP

Collector

Management VIP: *

Management VIP

Collector VM Info *

Host Name	Password	Ccuser Password	Admin IP	Management IP	Action
No data available					

1 / 1

Collector Tor Connections

Tor Info	Action
No data available	

1 / 1

Dispatcher

Rabbit MQ User Name: *

Rabbit MQ User Name

NFVIMON Admin:

Admin Name

Zenoss secondary NFVI-MON MASTER/COLLECTOR info

Master 2

Clear All

Admin IP:

Admin IP

Collector 2

Management VIP:

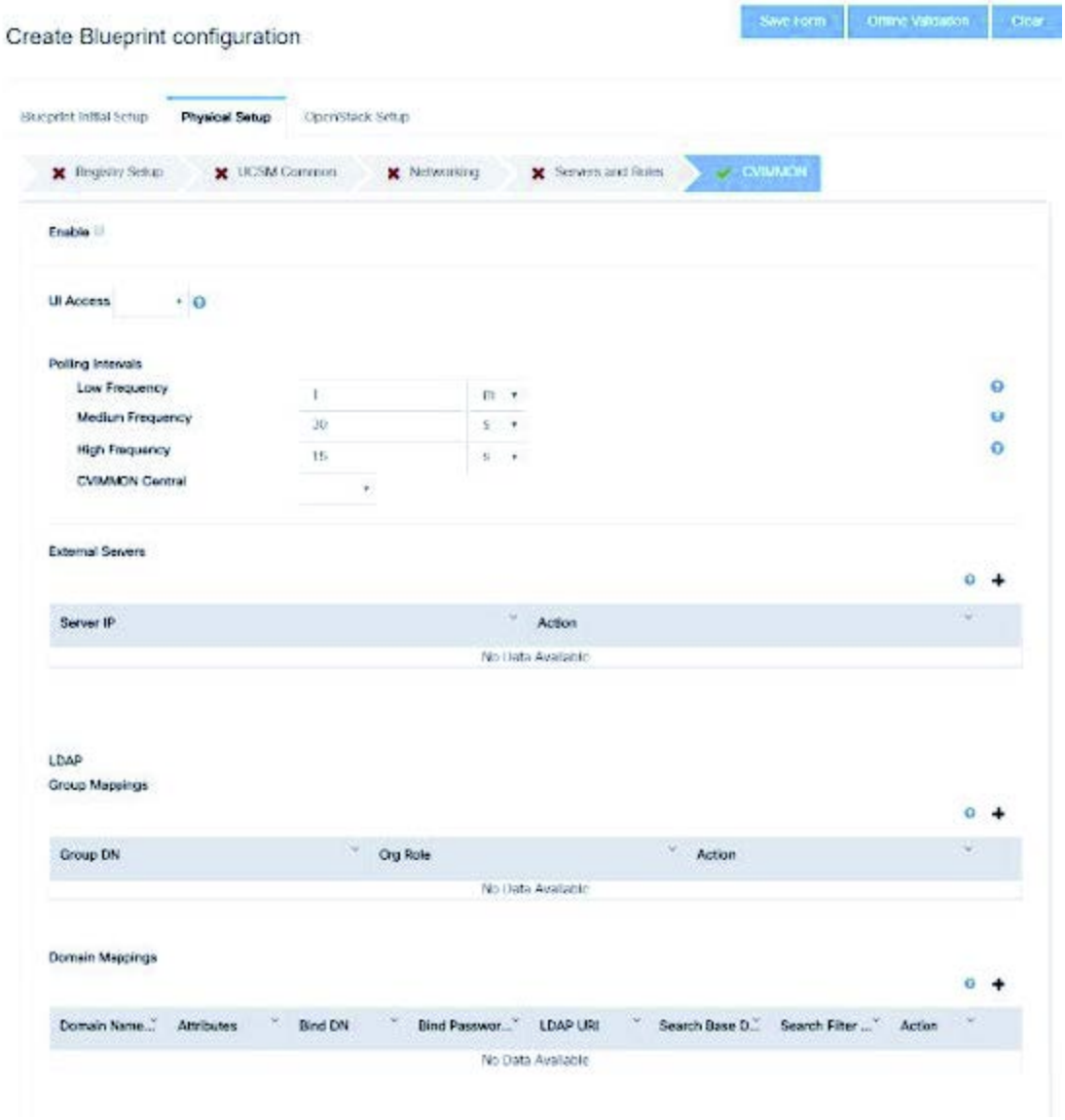
Management VIP

Collector VM Info

Host Name	Password	Ccuser Password	Admin IP	Management IP	Action

Fields	Description
Master - Admin IP	IP Address of Control Center VM
Collector - 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
Master 2	Optional, but becomes mandatory if collector 2 is defined. Must contain a valid Admin IP.
Collector 2	Optional, but becomes mandatory if Master 2 is defined. Contains Management VIP and Collector VM information. Collector 2 is secondary set to collector, with all the properties of Collector.
NFVIMON ADMIN	Optional and reconfigurable to add/update user id. Once enabled, you must have only one admin.
Collector ToR Connections	It is optional and available for ToR type NCS-5500. To add Collector ToR Connections, click on + icon and select the ToR switches from list. Supports adding only one Collector ToR Connection.
Port Channel	Enter port channel.
Switch - {torSwitch-hostname}	Enter port number. For example, eth1/15.
Save	Saves the entered information
Rabbit MQ User Name	Enter the Rabbit MQ username.

CVIMMON Tab



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

- Telegraf service is deployed on each node on the pod to capture infrastructure level statistics of CPU, memory, network, containers, and so on.
- Prometheus server is installed on the management node to poll for these statistics and store them in the time series database.

To view the statistics, use the grafana server that is accessible on the management node at port 3000 (password protected).
The three levels of polling intervals used by different telegraf plugins are:

1. Low frequency interval: Used to collect system level metrics like CPU and memory.
2. Medium frequency interval: Used to collect docker metrics.
3. High frequency interval: Used to collect rabbitmq metrics.

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

Prior to Cisco VIM 3.4.1, CVIM-MON is mutually exclusive to NFVIMON, From release 3.4.1 or later, both can run simultaneously on the same pod. This makes the transitioning from NFVIMON to CVIMMON easier.
PODNAME is required, when CVIM-MON is enabled.

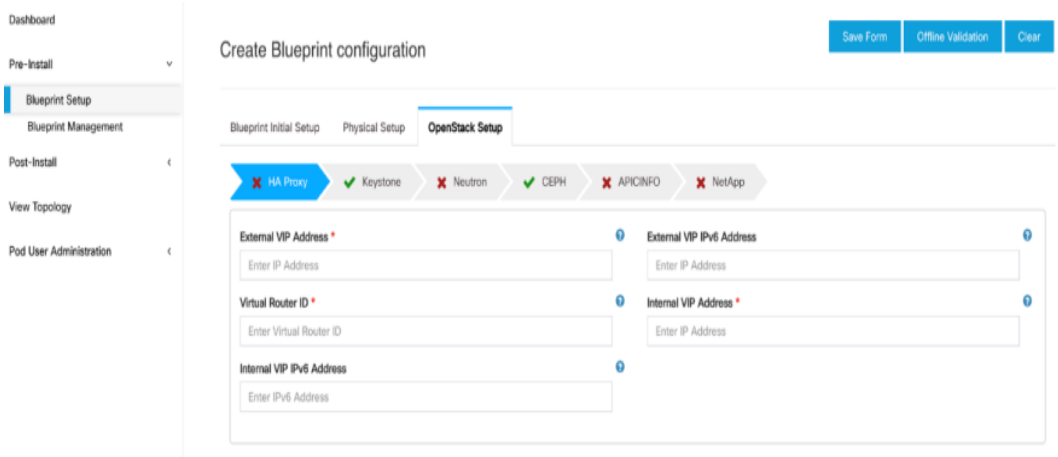
Fields	Description
Enable	Default is False
UI Access	Optional. If not defined, it is set to True by default. With this option disabled, CVIM_MON with SNMP is available, but you cannot access Grafana, Alert-Manager, and Prometheus UIs.
Polling Intervals:	

Low frequency	Minimum of 1 minute (1m) and a maximum of 60 mins (1h). If not defined, defaults to 1 minute. It must be more than a medium interval.
Medium frequency	Minimum of 30 seconds (30s) and a maximum of 60 mins (1h). If not defined, defaults to 30s. It must be more than a high interval.
High frequency	Minimum of 10 seconds (10s) and a maximum of 60 mins (1h). If not defined, defaults to 15s.
CVIMMON Central	Optional, if not defined, defaults to False. With this option enabled, you will get central CVIM-MON (only telegraf agents running on the pod), without local Prometheus, AlertManager, or Grafana
External Servers	Optional, list of external server IPs (v4 or v6) to be monitored by CVIM MON.
CVIMMON LDAP	If defined, the group mappings and domain mappings are mandatory.
group_mappings	Must contain at least one group with org_role Admin Optionally, you can add a second group with org_role Viewer.
domain_mappings	Must contain one domain exactly.
domain_name	Any non-empty name is acceptable.
attributes	All subkeys are mandatory.
bind_dn	Describes the user that can connect to the LDAP server to check credentials. It can be a read-only user or refer to a group that matches all possible users.
bind_password	This is the password of the bind_dn user. When the bind_dn is a group, this field must be omitted.
ldap_uri	The URI used to connect to the LDAP servers One or multiple URIs are configurable and separated by a comma.
search_base_dns	The base DNS name used for all queries.
search_filter	Filter used for the queries.

OpenStack Setup Pane

OpenStack Setup Tab

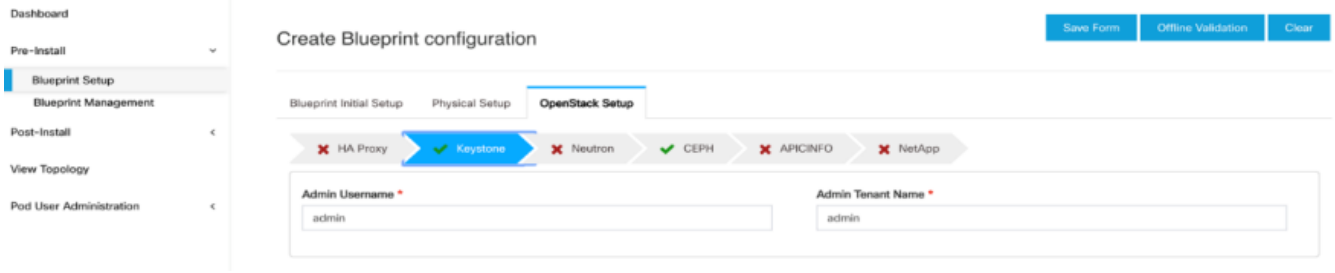
HA Proxy Tab



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

Keystone Tab

Mandatory fields are pre-populated.

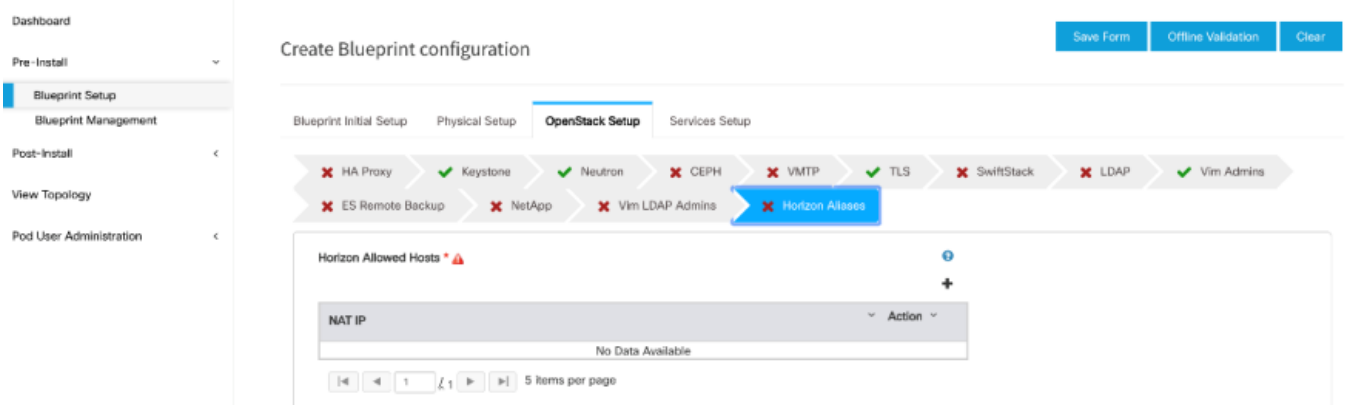


Fields	Description

Admin User Name	Specifies the user name of the admin.
Admin Tenant Name	Specifies the tenant name of the admin.

Horizon Aliases Tab

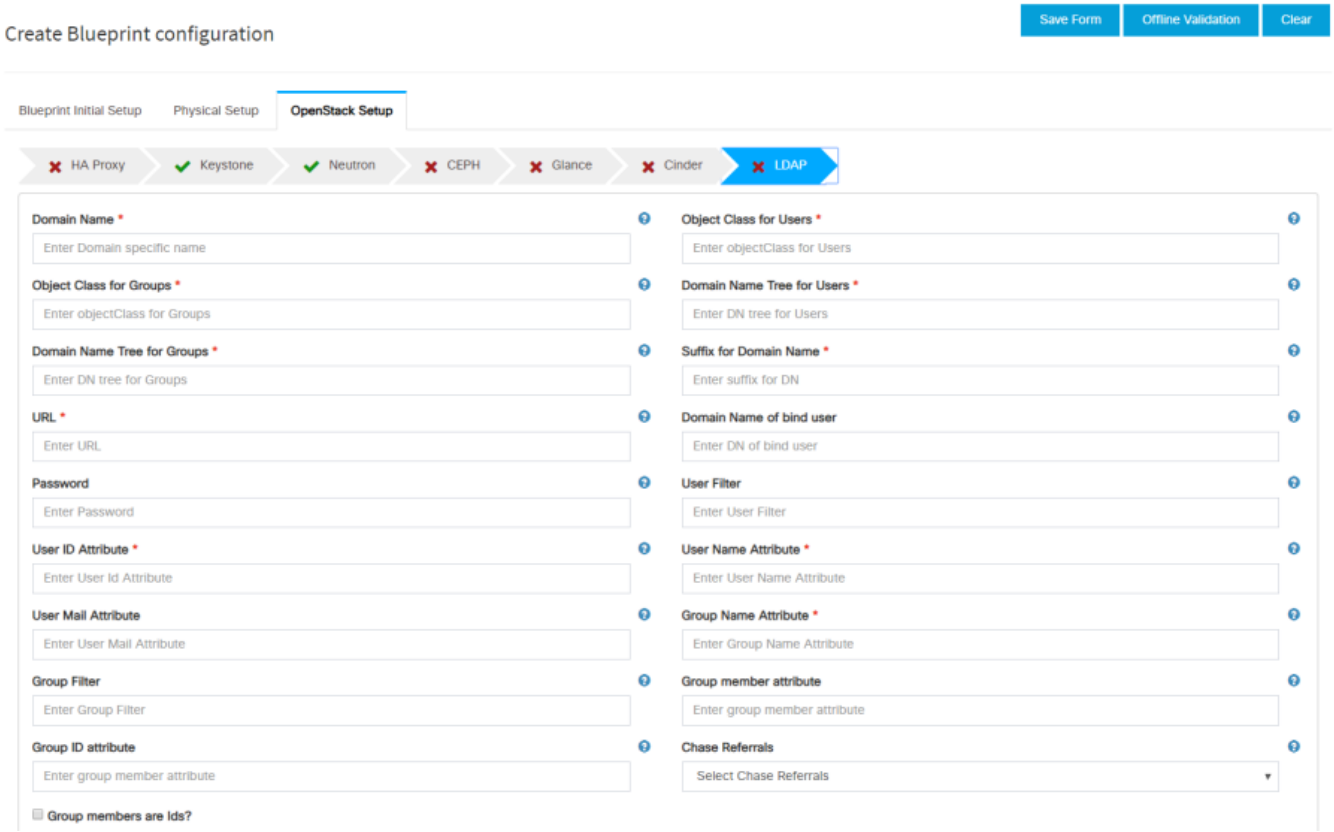
If the external_lb_vip is behind a NAT router or with a DNS alias, provide a list of those addresses.



Fields	Description
Horizon Allowed hosts– NAT IP	Uses comma separated list of IP addresses and/or DNS names

LDAP Tab

LDAP enable option is False by default. LDAP is enabled on keystone.

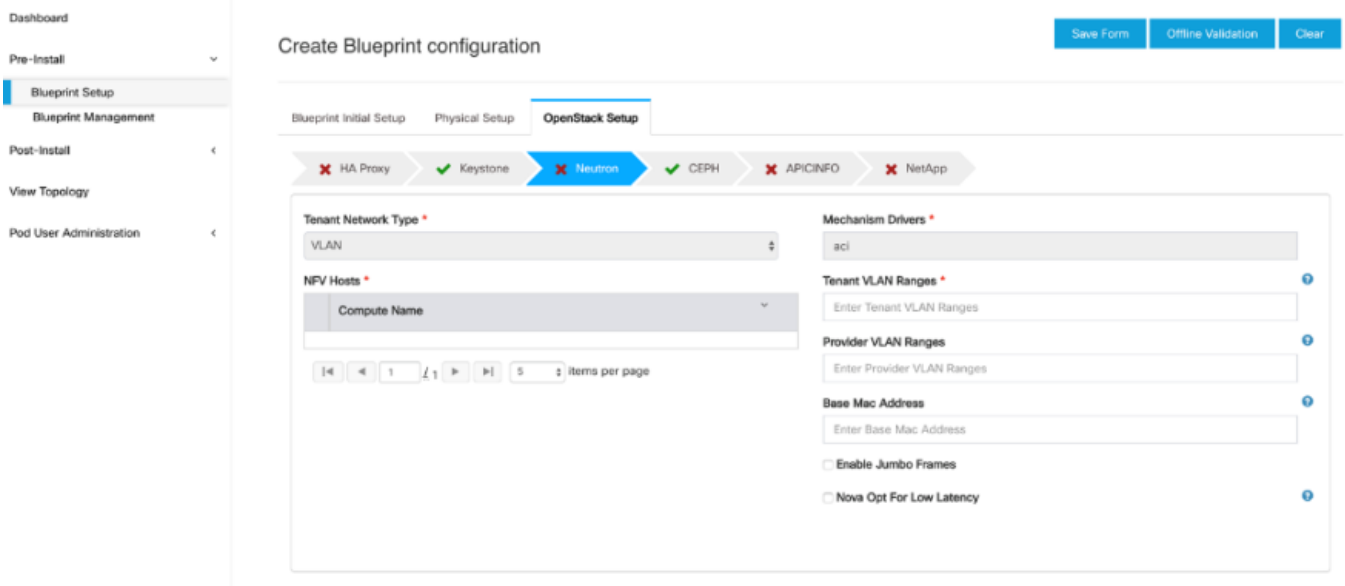


Fields	Description
Domain Name	Enter name for domain name.
Object Class for Users	Enter a string as input for user object class.

Object Class for Groups	Enter a string for group object class.
Domain Name Tree for Users	Enter a string for user domain name tree.
Domain Name Tree for Groups	Enter a string for group domain name tree.
Suffix for Domain Name	Enter a string for domain name suffix.
URL	Enter a URL with ending port number.
Domain Name of Bind User	Enter a string for binding domain name.
Password	Enter the password.
User Filter	Enter filter name in string format.
User ID Attribute	Enter a string for user ID attribute.
User Name Attribute	Enter the attribute of the user name.
User Mail Attribute	Enterthe attribute of the user's email as a string.
Group Name Attribute	Enter the attribute of the group name as a string.

Neutron Tab

Neutron fields change based on the **Tenant Network Type** selected under **Blueprint Initial Setup.**

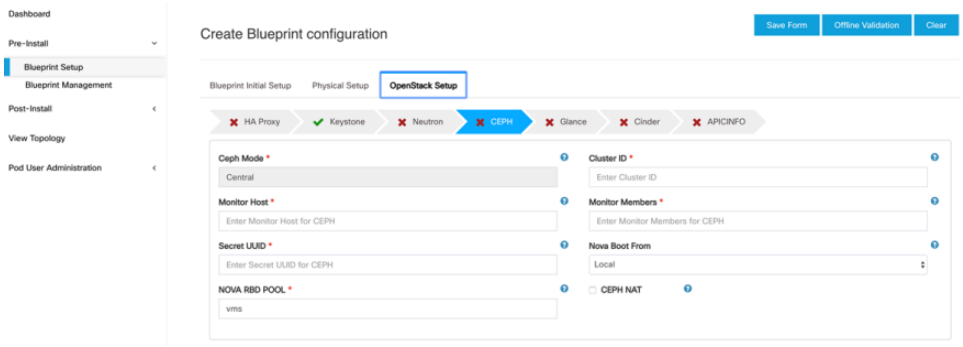


Fields	**Description**
Tenant Network Type	Autofilled based on the Tenant Network Type selected in the Blueprint Initial Setup page.
Mechanism Drivers	Autofilled based on the Tenant Network Type selected in Blueprint Initial Setup page.
NFV Hosts	Autofilled with the compute that is added in Server and Roles. If you select *All*, NFV_HOSTS: ALL is added to the blueprint. You can select one particular compute. For example, NFV_HOSTS: compute-server-1, compute-server-2.
Tenant VLAN Ranges	List of ranges separated by comma form start:end.
Provider VLAN Ranges	List of ranges separated by comma form start:end.
VM Hugh Page Size	Available for NFV_HOSTS option. 2M or 1G (optional, defaults to 2M)
VM_HUGHPAGE_PERCENTAGE	Optional, defaults to 100%. Range is 0 to 100.
ENABLE_CAT	Optional to enable Intel CAT. It is valid only when NFV Host is enabled. By default, it is set to False.
RESERVED_L3_CACHELINES_PER_SOCKET	Allowed value of reserved cache lines per socket is between 1 and 32. It is valid only when ENABLE_CAT is set to True.

VSWITCH_WORKER_PROFILE	Allowed only for VPP. Available options are: • numa_zero: The reserved cores always reside in NUMA node 0. • Even : The reserved cores are evenly distributed across all NUMA.
NR_RESERVED_VSWITCH_PCORES	Allowed only for VPP. Number of cores associated to VPP, defaults to 2. Value is in the range of 2 to 6.
Enable Jumbo Frames	Enable the checkbox.
Enable VM Emulator Pin	• Optional, when NFV_HOSTS is enabled. When a VM is spawned with this parameter enabled, Nova allocates additional vCPU on top of the vCPU count specified in the flavor, and pins vCPU0 to the pCPU that is reserved in the pool.
VM Emulator PCORES Per Socket	• Optional, when ENABLE_VM_EMULATOR_PIN is enabled. • Enter the number of cores per socket. Defaults to 1. Values range from 1 to 4.
Nova Opt For Low Latency	• Optional. Used to enable additional real-time optimizations in OpenStack NOVA. Defaults to False.
Tenant VLAN Ranges	For Tenant Network Type Linux Bridge, everything remains the same but **Tenant VLAN Ranges** is removed.

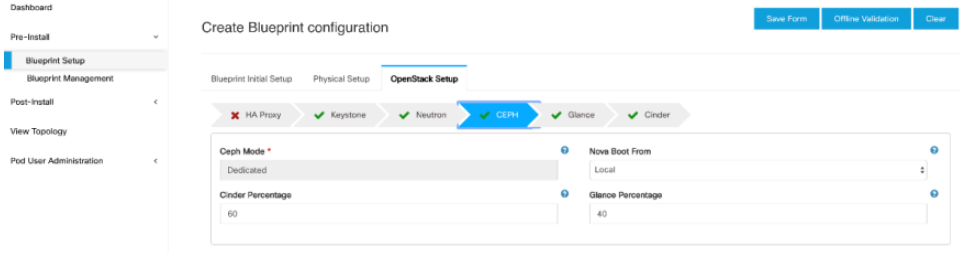
CEPH Tab

1. When Object Storage Backend is selected *Central* in **Blueprint Initial Setup**.



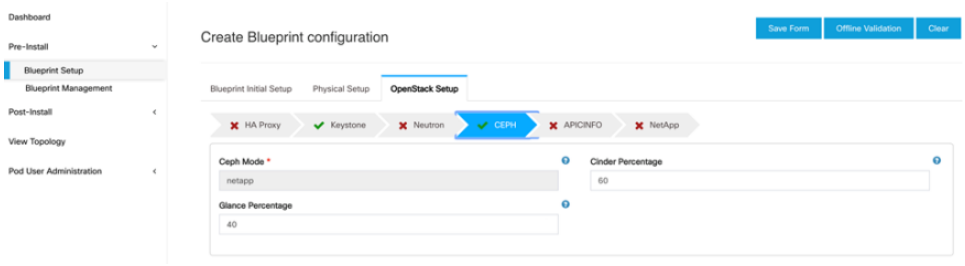
Fields	Description
Ceph Mode	By default, it is Central.
Cluster ID	Enter Cluster ID.
Monitor Host	Enter Monitor Host for CEPH
Monitor Members	Enter Monitor Members for CEPH
Secret UUID	Enter Secret UUID for CEPH
NOVA Boot from	Drop down selection. You can choose CEPH or local.
NOVA RBD POOL	Enter NOVA RBD Pool (default's to vms)
CEPH NAT	Optional, needed for Central Ceph and when mgmt network is not routable

2. When Object Storage Backend is selected *Dedicated* in **Blueprint Initial Setup**.



Fields	Description
CEPH Mode	By default, it is set to Dedicated.
NOVA Boot	You can choose CEPH or local.
Cinder Percentage	Must be 60 when Nova Boot From is local, and must be 40 when Nova Boot is Ceph
Nova Percentage	Only applicable when Nova Boot From is Ceph and must be 30%.
Glance Percentage	Must be 40 when Nova Boot From is local, and must be 30 when NOVA Boot From is Ceph. If Ceilometer is enabled, it must be 35% for Nova Boot from local and 25% for NOVA Boot From is Ceph.
Gnocchi Percentage	Only applicable when ceilometer is enabled, and must be 5%.

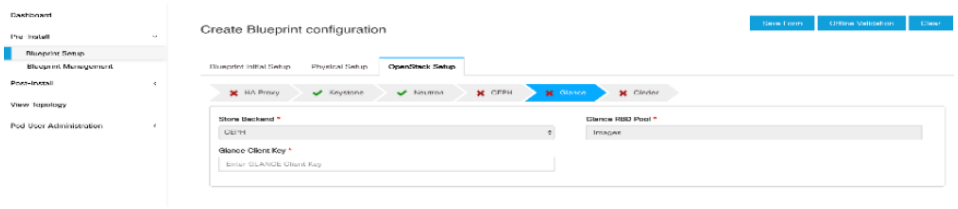
3. When Object Storage Backend is selected *NetApp* in **Blueprint Initial Setup.**



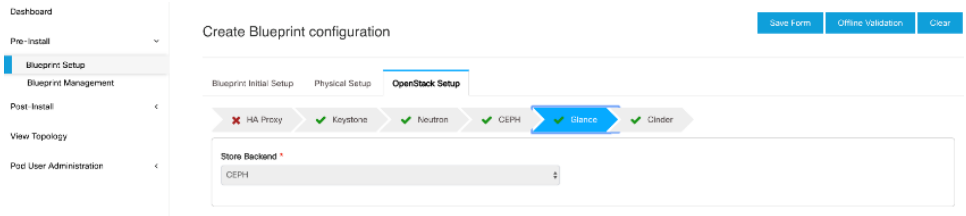
Fields	Description
Ceph mode	By default, it is NetApp.
Cinder Percenatge	Must be 60%
Glance Percenatge	Must be 40%

Glance Tab

1. When Object Storage Backend is selected *Central* in Blueprint Initial Setup.



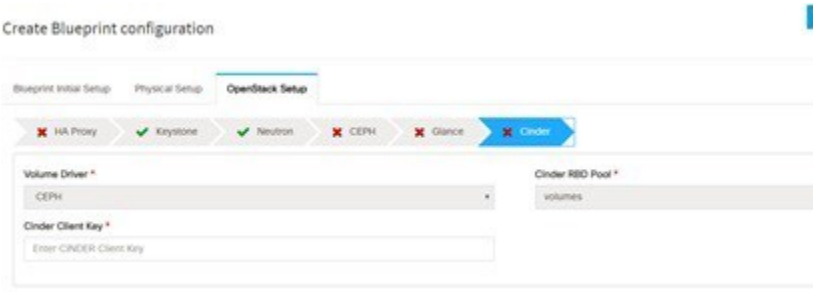
2. When Object Storage Backend is selected *Dedicated* in blueprint initial setup.



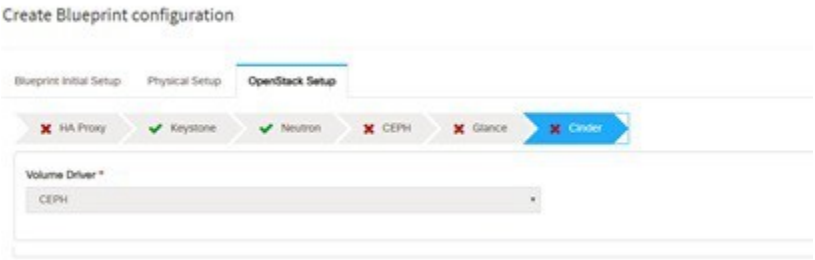
> ⚠ For CEPH Dedicated, Store Backend value is CEPH by default.

Cinder Tab

For CEPH Dedicated, Volume Driver value is *CEPH* by default.



When Object Storage Backend is selected *Dedicated* in **Blueprint Initial Setup**.

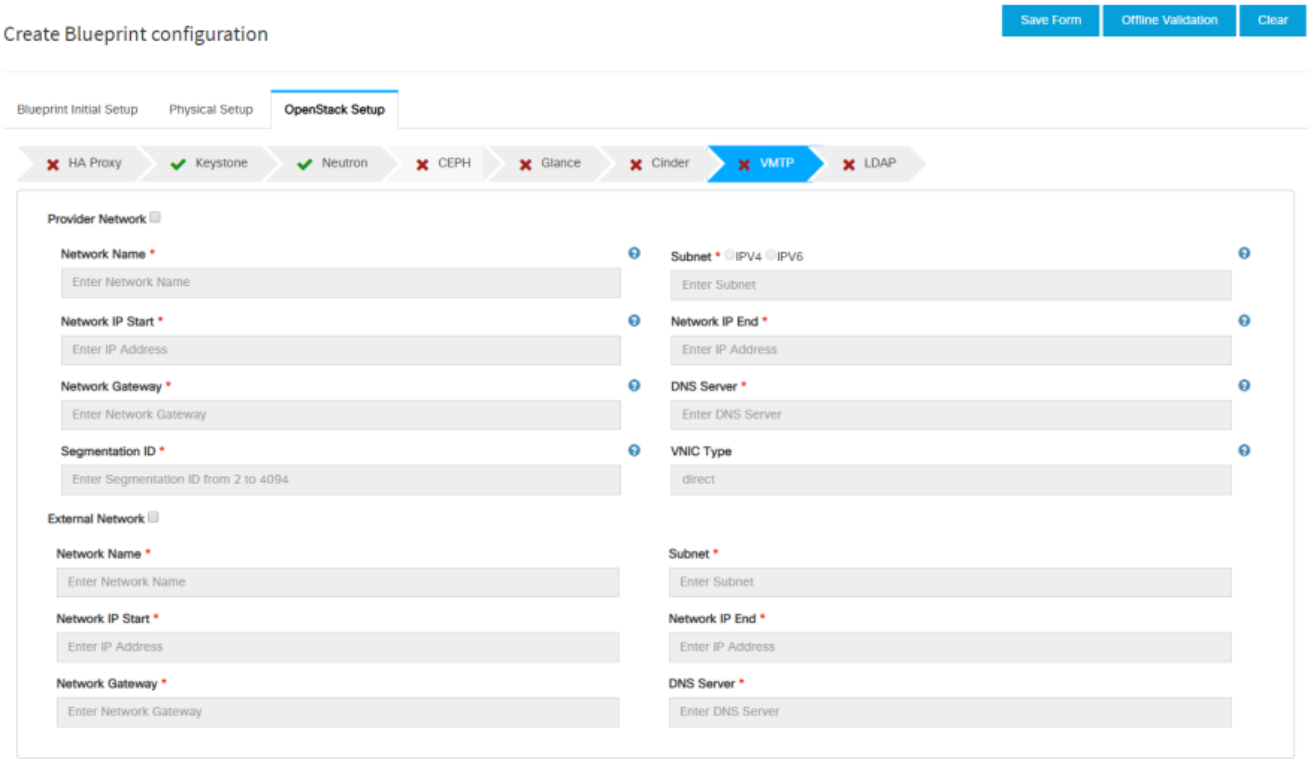


VMTP Tab

VMTP is optional and visible only if VMTP is selected under **Blueprint Initial Setup**. For VTS tenant type, only the Provider network is supported. Select one of the below to specify a VMTP network:

- Provider Network
- External Network

For **Provider Network** and **External Network,** complete the following:



Fields	Description
Network Name	Enter the name for provider network.

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

TLS Tab

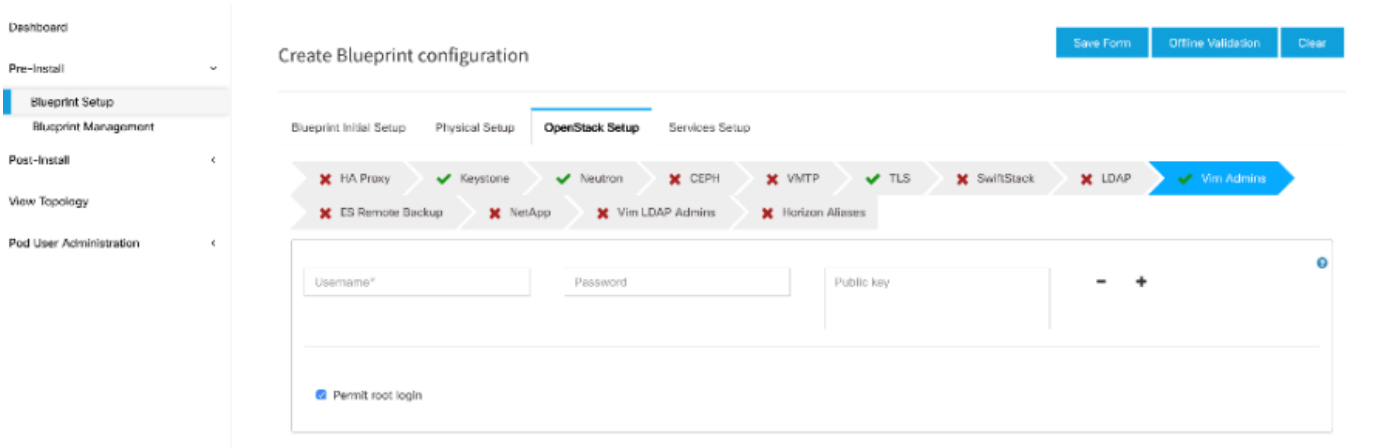
TLS is optional and visible only if TLS is selected under **Blueprint Initial Setup** Page.
TLS has two options:

Fields	Description
External LB VIP FQDN	Enter the string.
External LB VIP TLS	True/False. By default, it is set to False.
Management Node External API FQDN	Enter the string

Vim Admin Tab

This tab is visible only when Vim_admins is selected from the **Optional Features & Services** under the **Blueprint Initial Setup** tab.

- Add Username, Password, and Public key for the non-root login.
- At least one Vim Admin must be configured, when Permit root login is False.



Fields	Description
User Name	Enter username for Vim Admin.
Password	Password field. Admin hash password should always start with $6.
Public Key	Public key for vim admin should always start with 'ssh-rsa AAAA….'

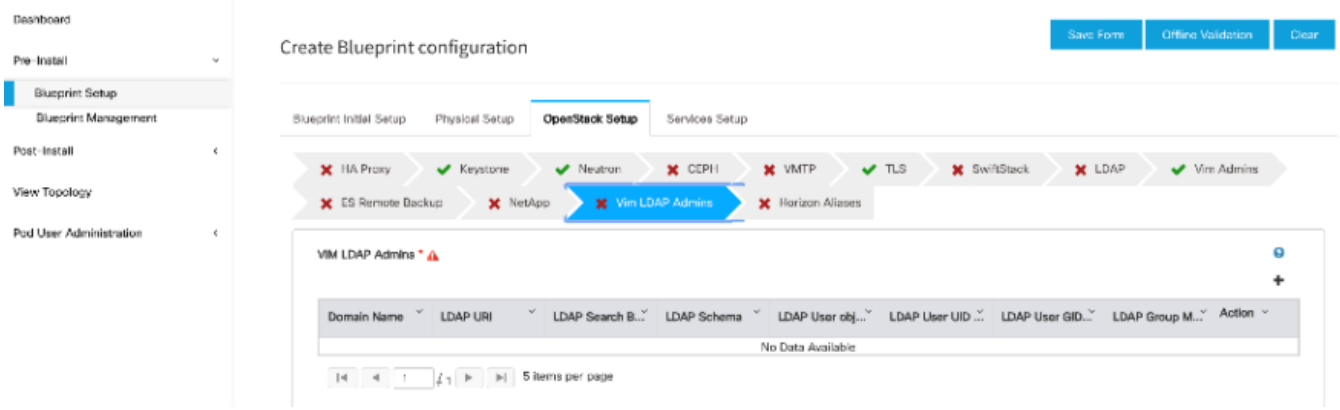
SwiftStack Tab

SwiftStack optional section is visible only if SwiftStack is selected from **Blueprint Initial Setup** Page. It is only supported with **KeyStonev2**. If you select **Keystonev3**, swiftstack is not available for configuration.
Following are the options that needs to be entered for SwiftStack:

Fields	Description
Cluster End Point	IP address of PAC (proxy-account-container) endpoint.
Admin User	Admin user for swift to authenticate in keystone.
Admin Tenant	The service tenant corresponding to the Account-Container used by Swiftstack.
Reseller Prefix	Reseller_prefix as configured for Keysone Auth,AuthToken support in Swiftstack E.g KEY_
Admin Password	swiftstack_admin_password
Protocol	http or https

Vim LDAP Admins Tab

Optional entry to support LDAP for admin access to management node. For this feature, TLS must be enabled for the external api, that is, external_lb_vip_tls: True.
Following are the values to be provided to add vim LDAP admins:



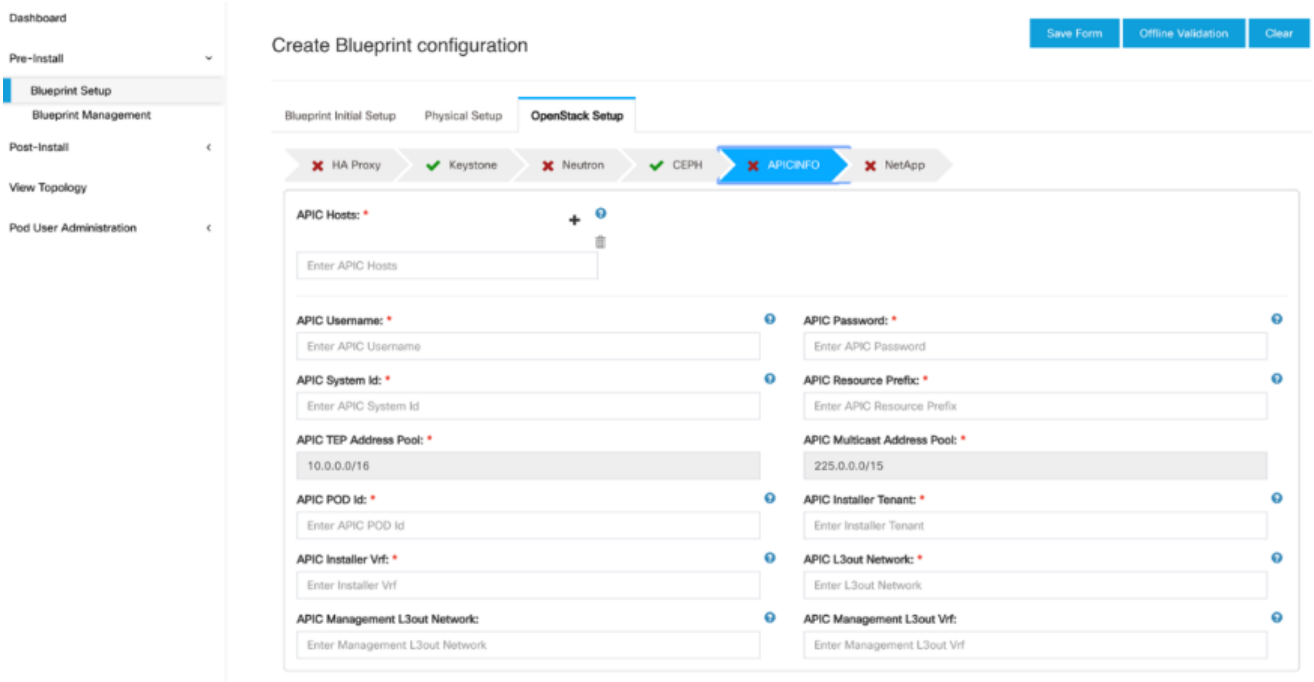
Fields	Description
domain_name	Mandatory field. Indicates the domain name to define vim LDAP admins.
ldap_uri	Mandatory. Ensure that ldap_uri is secured over ldaps.
ldap_search_base	Mandatory. Enter search base.
ldap_schema	Optional. Enter the schema.
ldap_user_object_class	Optional. Indicates the posix account.
ldap_user_uid_number	Optional. Indicates the user ID.
ldap_user_gid_number	Optional. Indicates the group ID.
ldap_group_member	Optional. It is the group member ID.
ldap_default_bind_dn	Optional. Enter default distinguished name
ldap_default_authtok	Optional. Default authentication token
ldap_default_authtok_type	Optional. Default authentication token type.
ldap_group_search_base	Optional. Enter group search base.
Fields	Description
ldap_user_search_base	Optional. Enter user Search Base

access_provider	Optional.
simple_allow_groups	Optional
ldap_id_use_start_tls	Optional .Can be true or false
ldap_tls_reqcert	Optional . Can be never/allow/try/demand.
chpass_provider	Optional. Can be ldap/krb5/ad/none

APICINFO Tab

APICINFO tab is available in Openstack setup, when the Tenant type ACI/VLAN is selected in blueprint initial setup.

> ⚠ If ACI/VLAN is selected, the ToR switch from initial setup is mandatory.



Fields	**Description**
APIC Hosts	Enter host input. Example: <ip1|host1>:[port] . Maximum of 3 and minimum of 1, but not 2.
apic_username	Enter a string format.
apic_password	Enter Password.
apic_system_id	Enter input as string. Max length 8.
apic_resource_prefix	Enter string max length 6.
apic_tep_address_ pool	Allowed only 10.0.0.0/16
multiclass_address_pool	Allowed only 225.0.0.0/15
apic_pod_id	Enter integer in the range of 1 to 65535.
apic_installer_tenant	Enter a string with maximum length of 32.
apic_installer_vrf	Enter a string with a maximum length of 32.
api_l3out_network	Enter a string with a maximum length of 32.

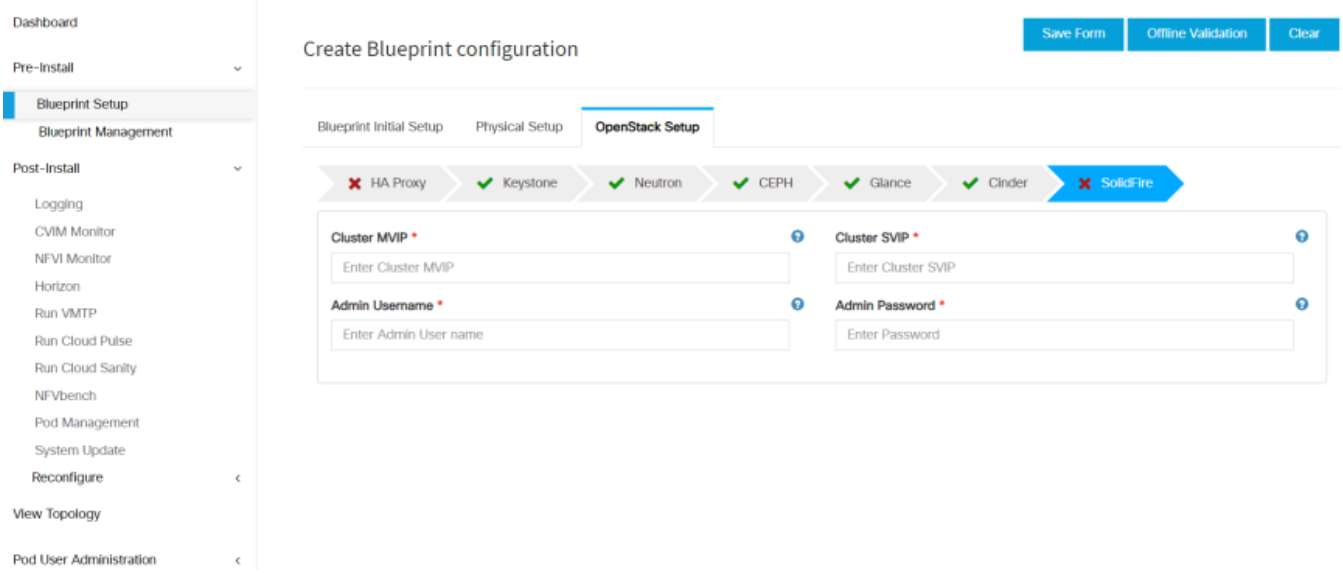
VTS Tab

This tab is available, when Tenant Type is VTS/VLAN selected. If VTS Day 0 is enabled, the SSH username and SSH password are mandatory. If SSH_username is entered, SSH password is mandatory or vice-versa.

Fields	Description
VTS Day 0	True or False. By default, it is False.
VTS User name	Enter a string without special characters.
VTS Password	Enter the password
VTS NCS IP	Enter IP Address format.
VTC SSH Username	Enter the VTC SSH username.
VTC SHH Password	Enter the password.

SolidFire Tab

SolidFire is visible for configuration on Day 0 and is always available with CEPH. It is not allowed as a Day 2 deployment option.



Fields	Description
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.

Service Setup Pane

Services Setup Tab

If **Syslog Export** or **NFVBENCH** is selected in **Blueprint Initial Setup** page, the **Services Setup** page is enabled. Following are the options under **Servic es Setup** Tab:

Syslog Export Tab

1. 

You can add a maximum of three entries.
To add new SysLog information, click **Add SysLog**, provide all the required information listed below and hit **Save**.

Fields	Description
Remote Host	Enter Syslog IP address.
Protocol	Only UDP is supported.
Facility	Defaults to local5.
Severity	Defaults to debug.
Clients	Defaults to ELK.
Port	Defaults to 514, but can be modified.

NFVBENCH Tab

NFVBENCH enable option is set to False, by default.

Fields	Description
Tor Switch	Enter the Switch name and port number. For example: eth1/5 . VTEP VLANS. Mandatory only for VTS/VXLAN. Enter VLAN1 and VLAN2.
ENABLE_ESC_PRIV	Enable the option by setting it as True. By default, it is False.

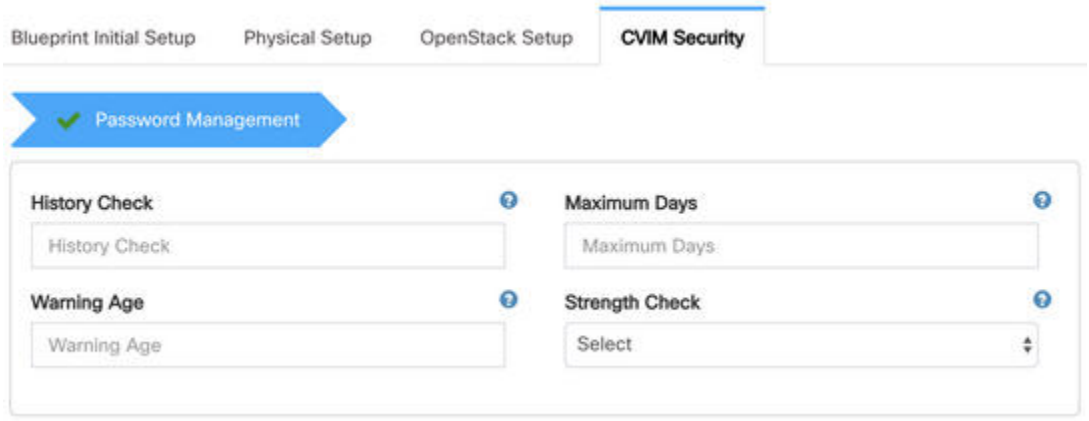
NIC Ports	INT1 and INT2 optional. Enter the two port numbers of the 4-port 10G Intel NIC at the management node used for NFVbench.
NIC Slot	Optional and must be in the range of 1-6. Indicates which NIC to use in case there are multiple NICs. If nic_slot is defined, the nic_port must be defined and vice-versa. ⚠ NIC port and slot need to be together.

CVIM Security Pane

CVIM Security Pane

Password Management Tab

The **CVIM Security** tab is visible, if you select the **Password Management** option under the optional features. Under **CVIM Security** tab, the **Password Management** pane is displayed.



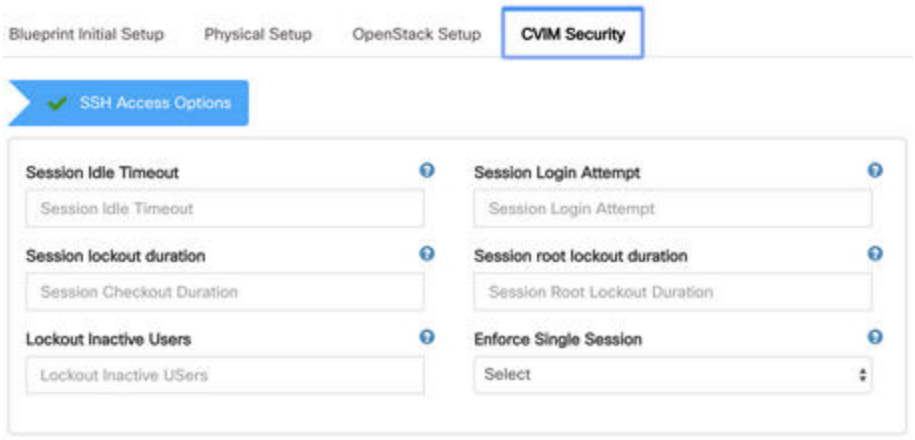
Following are the options available in the **Password Management** pane:

Fields	Description
History Check	Provides the number of last set of used passwords for comparion with new one. Value must be in the range of 2 to 12.
Maximum Days	Indicates the maximum days after which you are forced to change the password. Values must be in the range of 90 to 99999.
Warning Age	Indicates the number of days for expiry of the password. You are notified about the password expiry upon login. Values must be in the range of 1 to 99998, but less than value of **Maximum Days**.
Strength Check	Indicates whether or not to apply Cisco VIM password strength check.

If **Maximum days** is defined, it is mandatory to define **Warning Age**. You may skip both the values. If the entered values is out of the allowed range, then the values are not saved.

SSH Access Options Tab

The **CVIM Security** tab with **SSH Access Options** pane is visible, only if you select **SSH Access Options** option under optional features.



Following are the fields available in SSH Access Options pane:

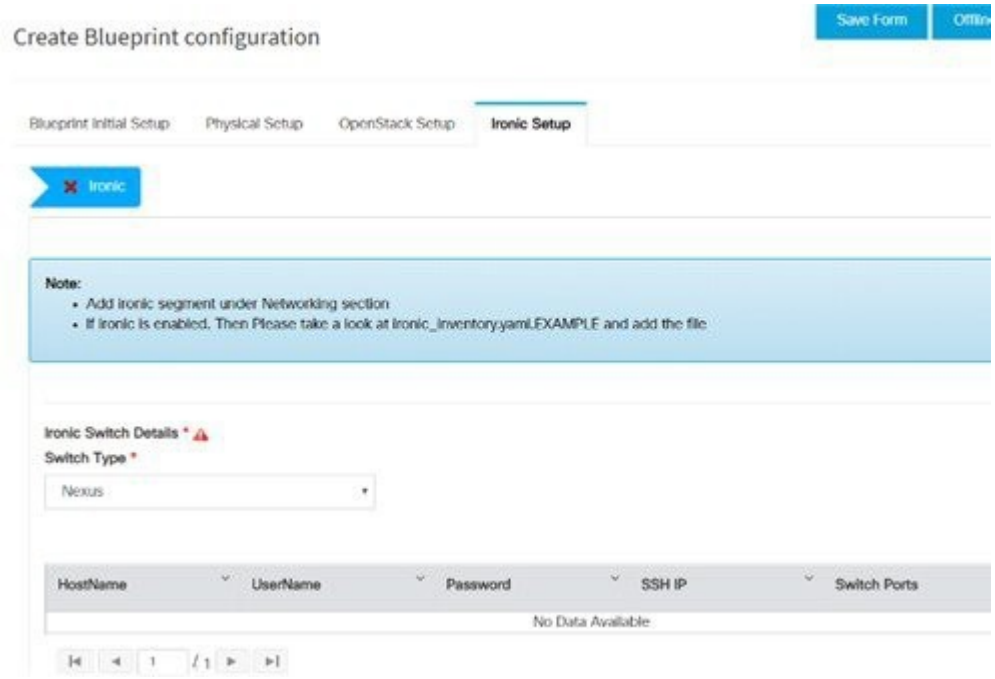
Fields	Description
Session idle timeout	Provides the Idle session timeout in seconds. By default, it is 3600. The minimum value is 300 and maximum value is 3600.
Enforce single session	Enforces you to have only one active session. It is not enabled by default.
Session login attempt	Number of attempts given for login. Minimum is 3 and maximum is 6. It is not enabled by default.
Session lockout duration	Indicates the session lockout duration in seconds for the users whose login attempts are exceeded by the usage of incorrect passwords. By default, it is not enabled. Minimum is 300, and maximum is 86400 seconds.
Session root lockout duration	Indicates the duration in seconds for which the root user is locked out when their session login attempts are exceeded the maximum value. By default, it is not enabled. Minimum is 300, maximum is 1800 seconds
Lockout inactive users	Specifies the days after which inactive users are locked out. By default, it is not enabled. Minimum is 90, and maximum is 99998.

Ironic Setup Pane

Ironic Setup Tab

Following are the options for Ironic :

- Ironic is applicable only for C-series and OVS/VLAN tenant network.
- Ironic is available in optional service list. If ironic is enabled, the ironic segment under Networks Segment and Ironic Switch Details under Ironic are mandatory.



Fields	Description
Switch Type	It can be Nexus, ACI, or BypassNeutron
Hostname	Enter ironic hostname. Required only if **Switch Type** is ACI or BypassNeutron.
Username	Enter ironic username. Required only if **Switch Type** is ACI or BypassNeutron.
Password	Enter the ironic password. Required only if **Switch Type** is ACI or BypassNeutron.
SSH IP	Enter ironic switch SSH IP. Required only if **Switch Type** is ACI or BypassNeutron.
Switch Ports	Optional. Indicates the ports that are in use to slap on inspector VLAN through Auto-ToR. Can be specified if **Switch Type** is ACI or BypassNeutron.

Activating Blueprint in Existing Pod

Activating Blueprint in Existing Pod with OpenStack

Following are the steps to activate blueprint in an existing pod installed with OpenStack:

> **Before you begin**
>
> You must have a pod with OpenStack installation in active state. If the OpenStack installation is in failed state, the UM UI cannot fetch the blueprint.

1. Go to the **Landing page** of the UM Log in.
2. Click **Register Management Node.**
3. Enter the following details:

    a. Management Node IP Address.
    b. Management Node Name (Any friendly Name).
    c. REST API Password (*/opt/cisco/ui_config.json*).
    d. Description about the management Node.
    e. Pod Admin's Email ID.

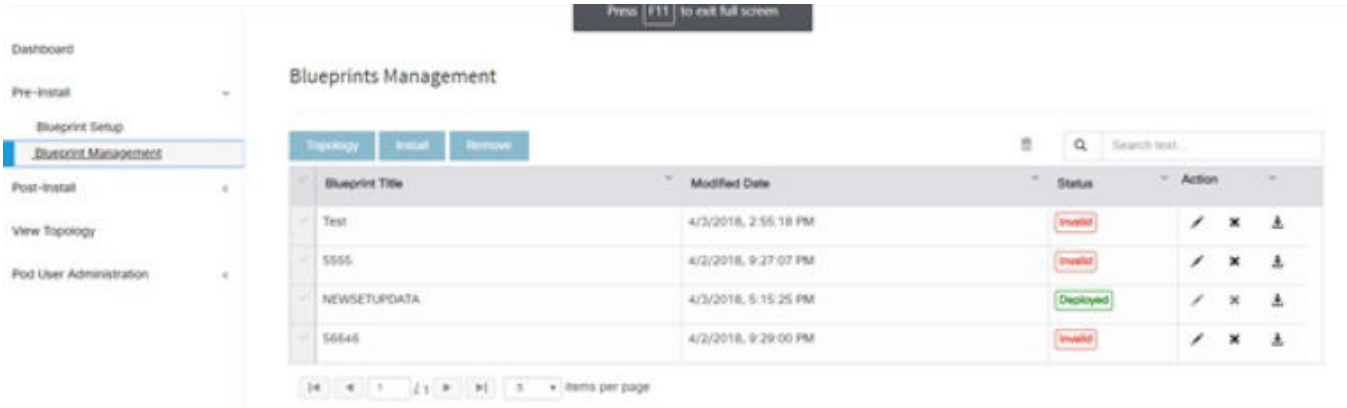
    A notification email is sent to the email id entered during registration.
4. Login using the same email id and password.
5. In the navigation pane, click **Pre-Install** > **Blueprint Management**. Choose the **NEWSETUPDATA** from the **Blueprint Management** pane. This is the same setup data that is used by ciscovimclient to run the installation on the management node.

Blueprint Management

Blueprint Management

Overview

You must have at least one blueprint in *Active, InActive,* or *In-progress* in the **Blueprint Management** pane.



Blueprint Management grid contains the list of all the blueprints that are saved. You can save the blueprint even if it is failed in the blueprint setup, but cannot deploy those blueprints.
The grid displays the following :

- Blueprint Name: It is unique and not editable. It shows the name of the blueprint that is saved after offline validation.
- Modified Date: This shows when the blueprint was last modified.
- Status: Indicates the status of the blueprint. It can take one of the following values:

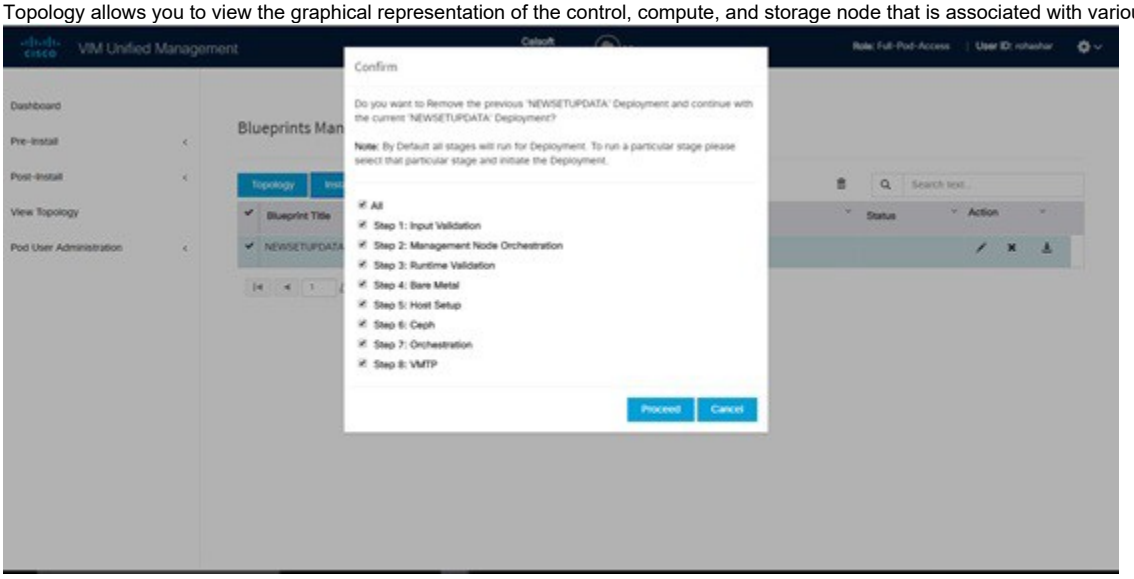
    1. Valid: Indicates that blueprint is saved after successful offline validation.
    2. Invalid: Indicates that blueprint is saved after the failure of offline validation.
    3. In-progress: Indicates that the blueprint is saved without running offline validation.
    4. Deployed: Indicates that the blueprint is used to bring up cloud without failures.
    5. Installing: Indicates that the blueprint is used to initiate the cloud deployment.
    6. Failed: Indicates that the blueprint is used to deploy the cloud which eventually failed.

You can edit, remove, search and download the blueprints.

With every blueprint record, there are some operations associated that you can perform by using the buttons Topology, Install, and Remove.

Topology

Topology allows you to view the graphical representation of the control, compute, and storage node that is associated with various network segments.



Install

To initiate the deployment with the stages you want to run, click **Install**. By default, all stages are selected.

You can also do an incremented installation. For incremented installation, you must choose the stages in the order. For example, if you choose validation stage, the second stage management node orchestration is enabled. You cannot skip stages and run a deployment. Once you click **Proceed**, the cloud deployment is initiated and the progress can be viewed from the Dashboard.

Remove, Edit, and Download Blueprint

To remove a blueprint, choose the blueprint and click **Remove**. A confirmation message is displayed with **Proceed** button. If you click **Proceed**, the blueprint removal operation is initiated.

You can edit or delete a blueprint which is not in *Deployed* state. If you want to take a backup of the blueprint locally, click **Download** icon which generates the preview to download the blueprint.
Following are the ways to deploy a Blueprint:

- If there is no blueprint in *Deployed* state, you can choose any Valid blueprint from the list.
- If there is a blueprint in a *Failed* state, you can choose another Valid blueprint but Unified Management prompts you to remove the previous deployment before proceeding.
- If there is a blueprint in *Deployed* state, you can choose another Valid blueprint but Unified Management prompts you to remove the previous deployment before proceeding.

The deployment of blueprint occurs step by step. If any one step fails for some reason, a **Play** button is displayed. Click on **Play** button to begin the installation for that particular state.

> ⚠ There is always one blueprint in Deployed state. You cannot deploy multiple blueprints in the cloud.

Search Blueprint

Use the **Search** box displayed on top-right of the table to lookup for blueprint by their name or status. Navigate to **Topology** and choose a blueprint which redirects you to the default blueprint, the one which is selected in the Blueprint Management pane.

> ⚠ During various operations across the application, the cloud icon in the center of the header changes its color based on the following table.

Pod Operation	Status	Icon or Color
Management Node Registered, No Active Deployment	Pending	Gray
Cloud Up And Running, No Failure	Active	Green
Cloud Installation/ Any Operation In Progress	In-Progress	Blue

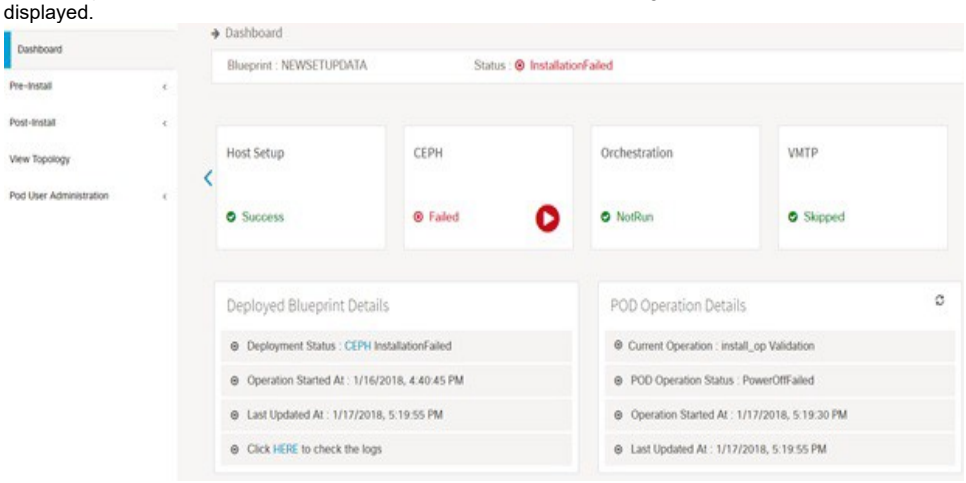
Cloudpulse Failed	Critical Warnings	Red
Pod Operation Failed	Warning	Amber
Software Update (Auto) Rollback Failed	Critical Warnings	Red
Uncommitted Software Update	Warning	Amber
Reconfigure Openstack Password	Critical Warning	Red
Reconfigure CIMC Password	Warning	Amber
Reconfigure Optional Features/ OS	Critical Warning	Red
Power Management Operation Fails	Warning	Amber
Management Not-Reachable	Not-Reachable	Red

Redeploy Multiple Install Stages

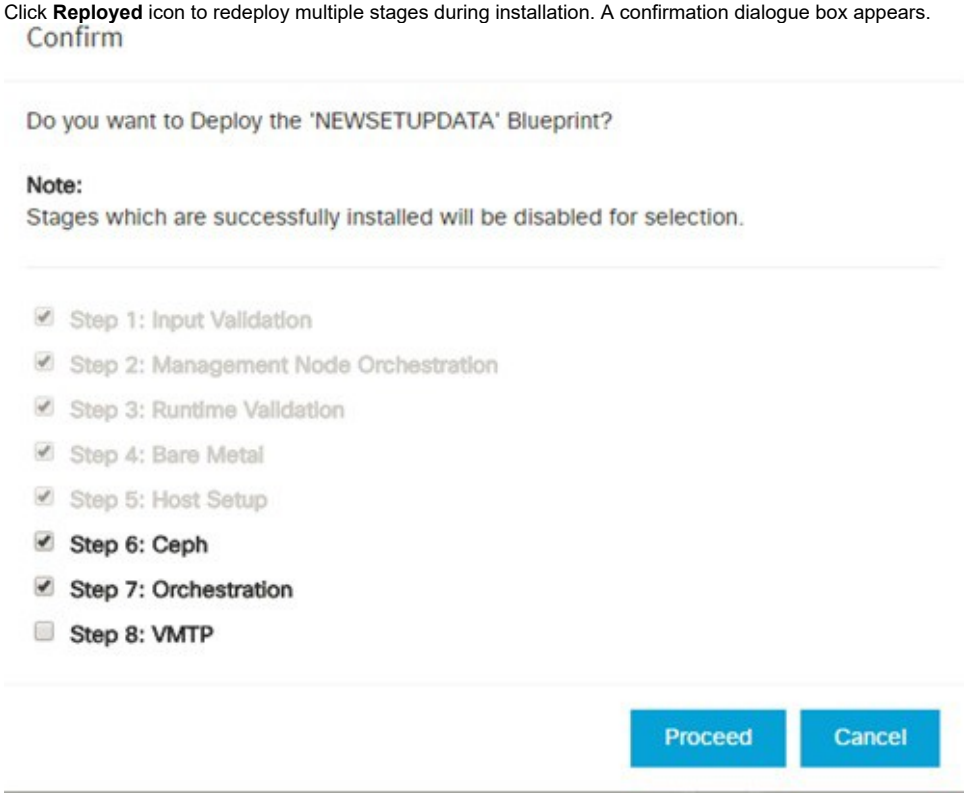
Redeploy Multiple Install Stages Using UM

You can redeploy Cisco VIM in multiple stages during blueprint installation using the Cisco VIM Unified Management dashboard.

1. If the blueprint installation status is *Active/failed/Installation failed* and stage install status is *Failed/NotRun/Skipped*, the redeployed icon is displayed.



2. Click **Reployed** icon to redeploy multiple stages during installation. A confirmation dialogue box appears.



3. Select the stages to be installed.
4. You can select the stages only in sequence. For example, you can select the VMTP stage (current) stage only if the Orchestration (previous) stage is selected for blueprint installation (assuming Orchestration is in Failed/NotRun state).
5. Click **Proceed** to run the installation.

Downloading Blueprint

Downloading Blueprint

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

1. Log in to **CISCO VIM Unified Management**.
2. In the navigation pane, expand the **Pre-Install Section**.
3. Click **Blueprint Management**.
4. Go to **Download** for any blueprint under Action.
5. Click the **Download** icon. A pop-up window is displayed to view the blueprint in the *yaml* format.
6. Click the **Download** button at the bottom left of the pop-up window. The *yaml* is saved locally with the same name of the blueprint.

Validating Blueprint

Validating Blueprint

1. Log in to **CISCO VIM UnifiedManagement**.
2. In the navigation pane, expand the **Pre-InstallSection**.
3. Click **BlueprintCreation**.
4. Upload an existing *yaml* or create a **NewBlueprint**. Enter all the mandatory fields so that all **Red Cross** changes to **Green Tick**.
5. Enter the name of the Blueprint.
6. Click **Offline Validation**.

    a. If the validation is successful, the UM allows you to save the blueprint.
    b. If you see any errors, a hyperlink is created for those errors. Click the link to be navigated to the page where error is encountered.

Using Unified Management

Using Cisco VIM Unified Management (UM)

Naming Conventions

Naming Conventions

The following are the naming conventions used in the Cisco VIM UM

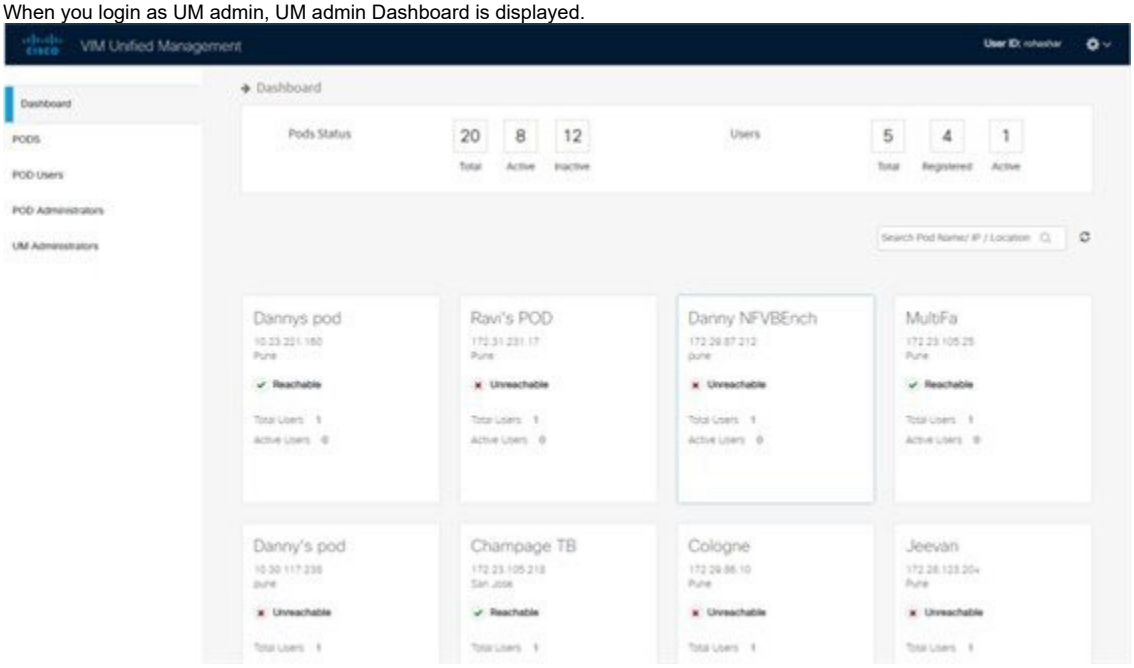
1. Super Administrator (UM Admin): User having access to UM Admin profile.
2. Pod Administrator: User having access to register a pod in the system. Only UM admin can add new Pod Admin in the system.
3. Pod users (Normal users): Denotes all the users associated with the pod. Full-pod-access is the role assigned to user to give full access of a specific pod.

- User who are UM admin or Pod admin but not associated with any pod are not counted in UM admin dashboard user count section.
- Only Pod Admins can register a new pod.
- Every pod must have a user with *Full-pod-Access* role.
- You cannot revoke/delete user if the user is the last user on the pod with *Full-Pod-Access* role.
- You cannot delete a user, if the user is a Pod admin or UM admin.

UM Dashboard

UM Dashboard

When you login as UM admin, UM admin Dashboard is displayed.



The UM dashboard displays information about the currently managed pods:

Pod Status

- Active - Number of pods with health status OK (Example: Management node health of the pod is good).
- Inactive - Number of pods whose health status is not good (Example: Management node health of the pod is not good).
- Total number of Pods - Number of pods registered in the system.

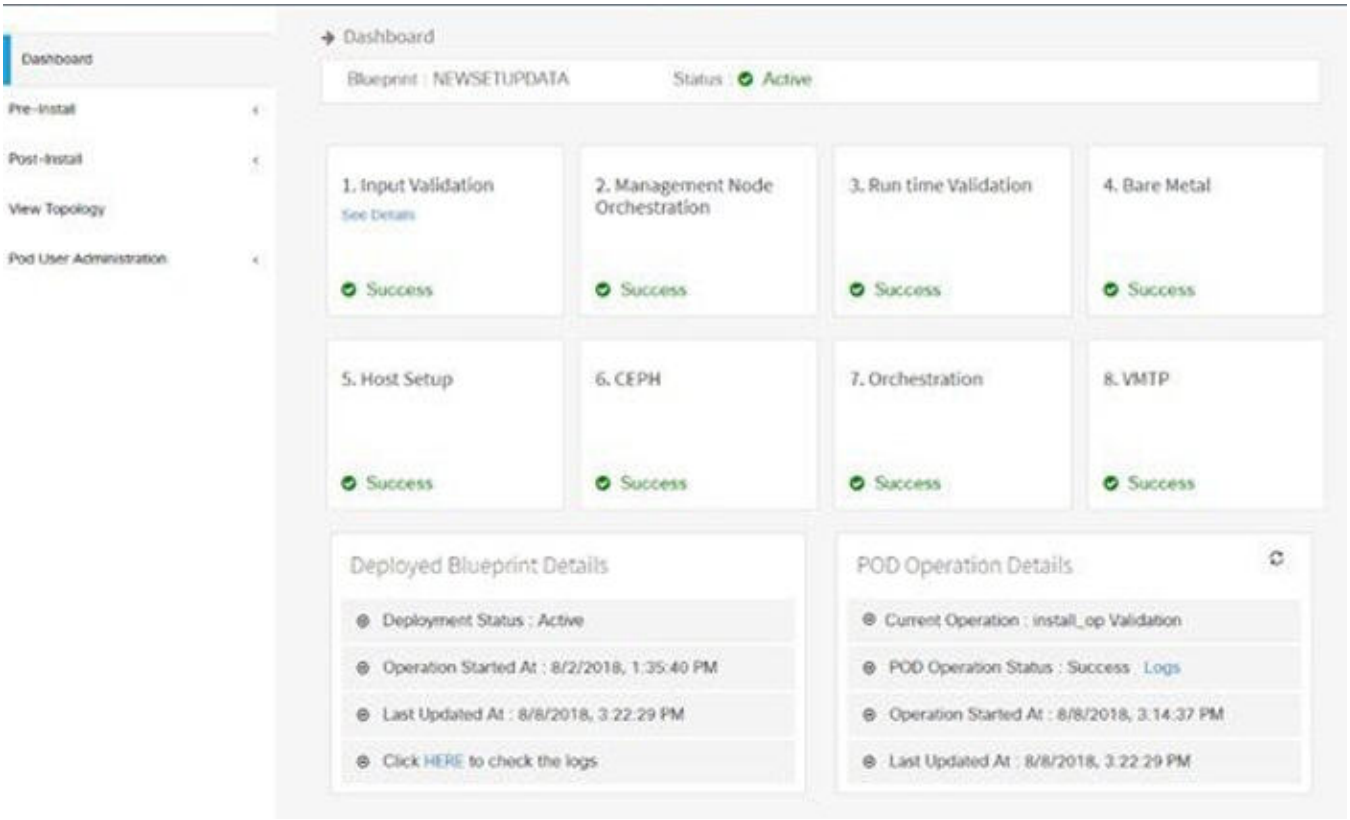
Pod Users

- Total – Total number of registered users 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 pods with its Pod name, description, IP address, location, and 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.

To check the health of the pod, click **Get health of current nodes icon (spin)**.

After selecting a pod, the **Dashboard** of that particular pod is displayed.



Blueprint

Blueprint pane provides the blueprint name and the status of the blueprint and various installation stages. The status is *Success*, *Failed,* or *Not Run*. To navigate between various installation stages, click **Next and Previous**.

Deployed Cloud Status

Following are the different types of cloud status on the pod.

- Active (Green): Indicates that the cloud is deployed without any failures.
- Failed (Red): Indicates the failure of the cloud deployment.
- Not Available (Gray): Indicates that cloud is not deployed on the pod.

Deployed Blueprint Details

Provides information about the deployed blueprint including deployment status, Operation start time, operation update time, and a link to the log of last operation. During cloud installation failure, the name with keyword regarding component failure is visible as **Deployment Status**.

Pod Operation Details

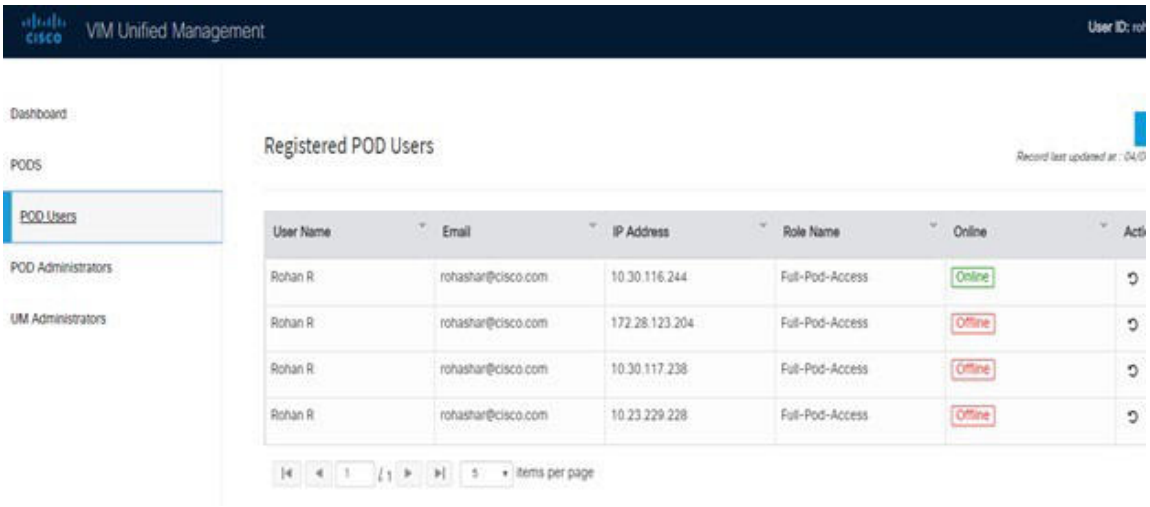
Provides information about the current operation details, pod operation status, and operation start/update time. Refresh icon at the top right corner of **Pod Operation** pane facilitates you to fetch the latest operation status from the pod.

Pods

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.



Privileges and Responsibilities

UM Administrator

The Unified Management UI Admin has the following privileges and responsibilities:

1. UM UI Admin(s) can only add Pod Admin in one of the two ways:
   - Local database.
   - LDAP with registration type as mail, uid, cn or group.
2. UM UI Admin manages all the users in UM from **Manage Pod Users**.
   - UI Admin can revoke permission of users: If UI Admin wants to revoke a user from a Pod, click **Revoke permission** under **Action** column.
   - UI Admin can delete a user: If UI Admin wants to delete a user from the UM, Click **Delete** under **Action** column. If there is only one user associated with a Pod, UI Admin must delete the pod first and then delete or revoke the user permission.
3. UM UI Admin can manage Pod Admin(s) from **Manage Pod Admin**.
   - UI Admin can add a new Pod Admin in UM.
   - UI Admin can revoke permission of a user or LDAP group from being a Pod Admin.
4. UM UI Admin can manage pods from Manage Pods.
   - UI Admin can delete a Pod from Unified Management.
   - UI Admin can also update password for the REST incase there was a system update on the pod and REST password was changed in that process.
5. UM UI Admin can manage other UI Admin(s) from **Manage UI Admin Users**.
   - UM UI Admin can add another UI Admin.
   - UM UI Admin can revoke permission of the user from being an UI Admin.

> ⚠ If there is only one UI Admin for UM, the revoke permission icon is disabled for the user.

Pod UI

As Cisco VIM is Rest API based, you can manage a pod through CLI, Rest API, or UI. You can always bring in a partial or fully functional pod and register with Cisco VIM UM. UM queries the pod status through Rest API and reflects the same.

> ⚠ Cisco recommends the admin to choose only one path to manage the pod.

Managing Pods

Adding a Pod

> ⓘ **Before you begin**
>
> Complete the following prerequisites to add a Cisco VIM pod:
>
> - Bootstrap of Cisco VIM UM must be complete and successful.
> - UI and Pod Admin must be available.

1. Navigate to https://br_api:9000
2. Click **Register Management Node** link.
    a. Enter the endpoint IP (IPv4/IPv6) which is the **br_api** of your pod, or FQDN address.

    > ⚠ Execute a runtime validation to check if the endpoint IP is already registered to UM.

    b. Give a name or tag for the pod that is to be registered.
    c. Enter the REST API password for the pod. You can locate the REST API password on the pod that you are registering. The path to locate REST API password is : */opt/cisco/ui_config.json*.
    d. You can optionally enter a brief description about management node.
    e. Enter the email ID of the Pod Admin and execute the runtime validation to check if the email ID is Pod admin or not.
        - If False, the UM gives an error that the user is not registered as Pod Admin.
        - If True, the User Name is auto-populated and the **Register** button is enabled.
3. Click **Browse** to upload restapi server CA Certificate. This is enabled once the Pod Admin validation is successful.
    - Navigate to */var/www/mercury/mercury-ca.crt* of the management node.
    - Download the certificate to the local machine and upload the certificate using UM.
    - Perform a validation check for file size and extension as part of upload. In case of failure, the certificate is deleted and you need to reupload the valid certificate. If the certificate is uploaded successfully, the **Register** button is enabled. To do a management node health check, click **Register**.
    - If the REST API service is down on the management node, a failure message **Installer REST API service not available** is displayed, but the certificate is not deleted.
    - If the certificate is invalid and there is SSL connection problem with the management node, the certificate is deleted and message is displayed to upload the certificate again.
    - If the certificate is valid, you are redirected to the login page with a message that the management node is registered successfully.
4. Click **Register** to redirect the user to the landing or login page. Pod Admin receives the notification mail that the management node is registered successfully.

    > ⚠ If UM_ADMIN_AS_POD_ADMIN is set to True, all UM-Admins are added as pod-users with **Full-Pod-Access** during pod registration.

5. If you encounter an error stating **Certificate file size is more than allowed limit** during pod registration, use a script to change the default value of the size of your certificate file to 4000 bytes. To change the default value, follow the below procedure:
    a. Navigate to Insight installer directory on the UM node:

    ```
    /root/insight-<tag_if>/tools/
    ```

    b. Execute the script: insight_cert_size_change.sh:

    ```
    /insight_cert_size_change.sh -s <pass the size in bytes>
    ```

    > ⚠ Ensure that you pass the value in bytes as it might decrease the limit from the default value.

c. Once the script is executed, Insight service is restarted automatically with the new file size check.
d. Follow the above steps to register the management node again.

Editing Pod

You can edit the pod by following the below steps:

1. Log in as UM UI Admin.
2. In the navigation pane, click **PODS**.
3. Choose the pod that you want to EDIT in the **Action** column.
4. In the **Edit Pod** popup window, edit the **Node name** and **Description**.
5. Click **Save** to update the pod.

Deleting Pod

When you delete a pod from Cisco VIM UM, you are not deleting the pod from your OpenStack deployment.

Before you begin

- Bootstrap of UM is complete and successful.
- At least one UI and Pod Admin must exists.
- UM manages the targeted Pod.

Following are the steps to delete a pod:

1. Log in as the **UM UI Admin**.
2. In the navigation pane, click **Manage Pods**.
3. Choose the pod that you want to delete in the **Action** column and then click **Delete**.
4. Click **Proceed** to confirm the deletion.

Monitoring Pod Status

Monitoring Pod Status

The Unified Management application manages the pods and displays the pod management action status with a cloud icon.

The following table displays a summary of the pod operation, the corresponding cloud-icon color, and the pod status.

Pod Operation	UM Icon-Color	Pod Status
Active cloud with no failures	Green	Active
Cloud installation or pod management operation is in progress	Blue	In-progress
Software update (auto) rollback is failed	Red	Critical Warnings
Pending commit post software update	Amber	Warning
Reconfigure failed (for any operation)	Red	Critical Warning
Update, commit, or Rollback failed	Red	Critical Warning
Power management operation fails	Amber	Warning
Management not reachable	Red	Not Reachable

Managing Hardware

Managing Hardware

Management of your Cisco VIM pods includes adding, removing, or replacing the nodes.

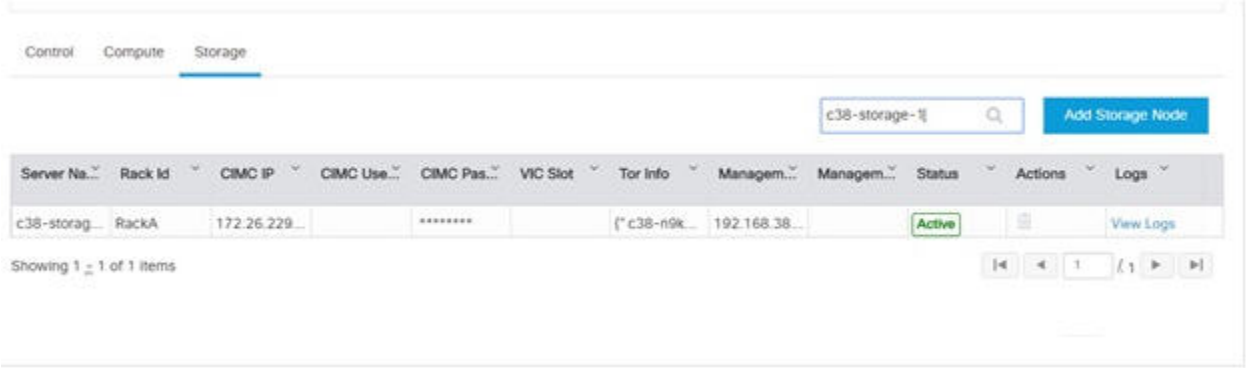
You cannot change multiple nodes at the same time. For example, if you want to replace two control nodes, you must successfully complete the replacement of the first node before you begin to replace the second node. Same restriction applies for addition and removal of storage nodes.

You can add or remove multiple nodes together only in case of compute nodes. However, there must always be one active compute node in a pod at any given point. VNF manager stays active and monitors the compute nodes to move the VNFs in accordance with the compute node management.

- When you change a control, storage, or compute node in a Cisco VIM pod using Unified Management, it automatically updates the server and role in the active blueprint. Thus, the OpenStack deployment changed.
- When a node is removed from Cisco VIM, sensitive data may remain on the drives of the server.
- Administrator recommends you to use Linux tools to wipe the storage server, before using the same server for another purpose. The drives that are used by other application server must be wiped out before adding to Cisco VIM.

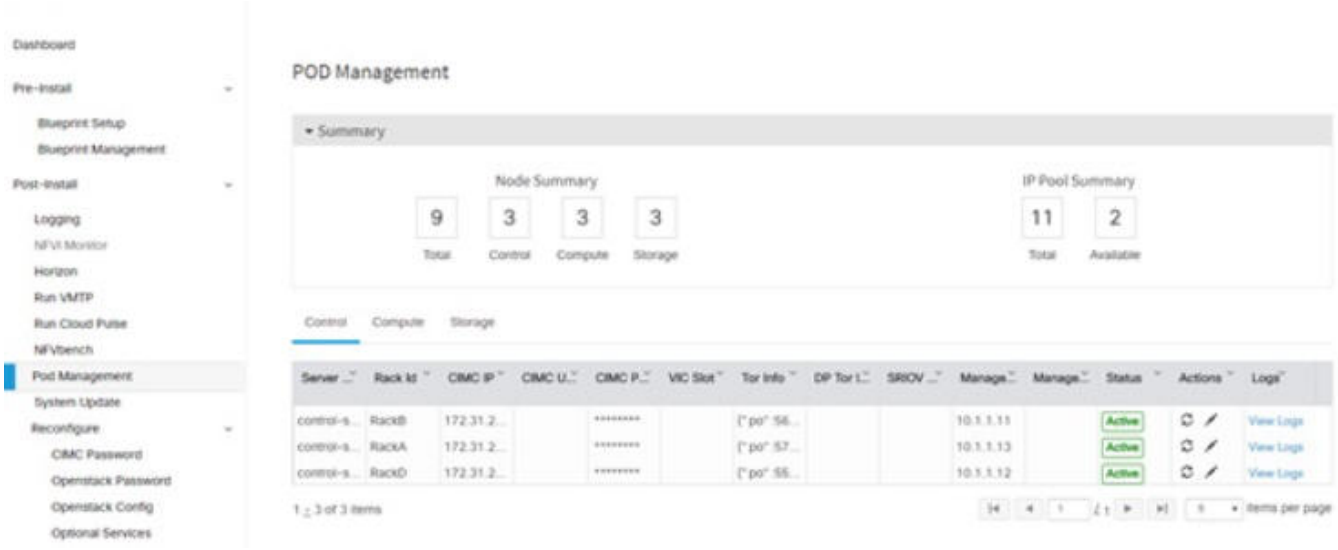
Searching Compute and Storage Nodes

This functionality allows you to search the Compute and Storage nodes by server names only. The search result is generated or shows an empty grid if there are no results.



Pod Management

Cisco VIM allows the admin to perform pod life-cycle management from a hardware and software perspective. Cisco VIM provides the ability to power on /off compute node, add, remove or replace nodes based on the respective roles when the nodes of a given pod corrupts at times.



Pod Management page has two sections–

1. **Node Summary:** This section shows the number of available nodes and the detailed count of Control, Compute and Storage.
2. **IP Pool Summary:** This section shows the total pool summary and the currently available pool count.

The operations performed on the running pod are:

- Replace control nodes: Double fault scenario is not supported. At a time, only one controller can be replaced.

> ⚠ If the ToR type is Cisco NCS 5500, an additional popup is displayed to enable the user to update splitter configuration before replacing the control node

- Add computes/storage nodes: N-computes nodes can be replaced simultaneously. However at any given point, at least one compute node must be active.

> ⚠ If the ToR type is Cisco NCS 5500, an option is available to update the splitter cable configuration.

- Power On/ Off compute nodes: You can power ON or power OFF compute node. At least one compute node must be powered on.
- Remove compute/storage nodes: You can add one node at a time, when Ceph is run as a distributed storage.

> ⚠ If ToR type is Cisco NCS 5500, an additional popup is displayed to enable the user to update the splitter cable configuration, before the removal of compute or storage node.

- Add Pool**:** You can increase pool size at any time.

Managing Storage Nodes

Before you add or remove a storage node, review the following guidelines for Managing Storage Nodes.

- Required Number of Storage Nodes: A Cisco VIM pod must have a minimum of three and a maximum of 20 storage nodes. If your pod has only two storage nodes, you cannot delete a storage node until you add another storage node. If you have fewer than three storage nodes, you can add one node at a time until you get to 20 storage nodes.
- Validation of Nodes: When you add a storage node to a pod, Cisco VIM Unified Management validates that all the nodes in the pod meet the minimum requirements and are in active state. If you have a control or compute node in a faulty state, you must either correct, delete, or replace that node before you can add a storage node.
- Update Blueprint: When you add or delete a storage node, Unified Management updates the blueprint for the Cisco VIM pod.
- Storage Node Logs: You can access the logs for each storage node from the link in the **Log** column on the Storage Nodes t

Adding Storage Node

Complete the following instructions to add a storage node:

> ⚠ You cannot add more than one storage node at a time

Before you Begin

- Remove the non-functional storage node from the pod. You can have maximum 20 storage nodes in a Cisco VIM pod.
- Ensure that the server for the new storage node is in powered state in OpenStack for C Series.

1. In the navigation pane, choose **Post-Install > Pod Management > Storage**.
2. Click **Add Storage node** button on the **Storage** tab. A popup will open where you can provide information about the new Storage node.
3. For C-series, add the following details:

   - **Server Name**: Name for the Storage Server to be added.
   - **Rack ID**: Enter the Rack ID. (Accepts String format).
   - **CIMC IP**: Enter the CIMC IP.
   - **CIMC User Name**: User name for the CIMC.
   - **CIMC Password**: Enter the password for the CIMC
   - **VIC Slot**: Enter the VIC Slot (Optional).
   - **ToR switch info**:Mandatory if ToR is configured as True
   - **Management IPv6**: Enter IPv6 Address.
4. For B-series, add the following details:

   - **Server Name**: Name for the Storage Server to be added.
   - **Rack ID**: Enter the Rack ID. (Accepts String format).
   - **Rack Unit ID**: Enter the Rack Unit ID.
   - **Management IPv6**: Enter IPv6 Address

   Clicking **Cancel** discards the changes and closes the popup.

   If all mandatory fields are filled in correctly, the **Add Storage** is enabled.
5. Click **Initiate Add Storage**. Add node initialized message will be displayed.
6. To view logs, click **View logs** under Logs column. The status of the POD will change to *Active*.
7. Two kinds of failure may occur:

   a. **Add Node Pre-Failed**: When addition of node failed before the bare-metal stage (step 4), the Active Blueprint is modified but the Node is not yet added in the Cloud. If you press X Icon, then Unified Management will delete the node information form the Blueprint and the state would be restored.
   b. **Add Node Post-Failed**: When addition of node failed after the bare-metal stage (step 4), the Active Blueprint is modified and the node is registered in the cloud. If you press X Icon, thn Unified Management will first delete the node from the Blueprint and then node removal from cloud would be initiated.

   You can view the logs for this operation under **Logs** column.

Deleting Storage Node

You cannot remove more than one storage node at a time.

Following are the steps to remove a storage node:

1. From the navigation pane, choose **Post-Install > POD Management > Storage**.
2. Click **X** adjacent to the storage node you want to remove. **Node Removal Initiated successfully** message is displayed when removed. You can delete a storage node with *force* option for hyper-converged pod. The *force* option is useful when VM's are running on the node.
3. To view logs, click **View logs** under logs column.

   - If the storage node is removed successfully, the storage node is removed from the list under **Add/Remove storage Node**.
   - If removal of storage node fails, the **Clear Failed Nodes** button appears.
4. Click **Clear Failed Nodes** to remove the node from cloud and blueprint.

Managing Compute Nodes

Before you add or remove a compute node, review the following guidelines:

- Required number of compute nodes: Cisco VIM pod must have a minimum of one compute node and a maximum of 128 nodes. Out of 128 nodes, three nodes are control nodes and the remaining 125 nodes are between compute and ceph nodes with a maximum of 25 ceph nodes. If your pod has only one compute node, you cannot delete that node until you add another compute node.

- Update blueprint: When you add or remove a compute node, Unified Management updates the blueprint for the Cisco VIM pod.
- Compute node logs: You can access the Logs for each compute node from the link in the Log column on the Compute Nodes table.

Adding Compute Node

Add IP Pool

If all the existing pool size is already used, you need to increase the pool size. On the **Add compute** or **Add storage** popup, click **Expand Management IP Pool** to add a new Pool.

Follow the below steps to add a compute node:

> **Before you begin**
>
> Ensure that the server for the new compute node is in powered state in OpenStack. You can add more than one compute node at a time.

1. In the navigation pane, click **Post-Install > Pod Management > Compute**.
2. Click **Add Compute Node** on the **Compute** tab a popup opens. Add the required information in the popup. To add another node, click **Add Another Node** if you planned to add another compute node OR hit **Initiate Add Compute** if you do not plan to add any more compute node. If you click **Add Another Node** button, the existing form will be emptied. You need to fill the information for the new compute node and then repeat step 1. You may use **Previous** and **Next** button to navigate among different added node information.
3. For C-series, add the following details:

    - **Server Name**: Name for the Compute Server.
    - **Rack ID**: Enter the Rack ID. (Accepts String format).
    - **CIMC IP**: Enter the CIMC IP.
    - **CIMC User Name**: User name for the CIMC.
    - **CIMC Password**: Enter the password for the CIMC.
    - **VIC Slot**: Enter the VIC Slot (Optional).
    - **ToR switch info**: Mandatory if configured ToR is true.
    - **DP ToR switch info**: Enter input as string format.
    - **SRIVO ToR info** : Enter input as string format.
    - **Management IPv6** : Enter IPv6 address.
    - **Trusted_vf**: Optional and not reconfigurable. Applicable only for SRIOV node with compute role for C-series pod.
    - **Vtep IPs**: IP address from vxlan-tenant and vxlan-tenant.
    - **INTEL_SRIOV_VFS** :Value range is 1 to 32.
    - **INTEL_FPGA_VFS**: Value range is 1 to 8.
    - **INTEL_VC_SRIOV_VFS**: Value range is 1 to 32.
    - **Vendor**: Optional. It can be CISCO - Cisco Systems Inc or QCT - Quanta Cloud Technology Inc or HPE - Hewlett Packard Enterprise.
    - **VM Hugepage Size**: Optional. It can be 2M or 1G. Only applicable with NFV HOSTS.
    - **RX TX Queue Size**: Optional. It can be 256, 512, or 1024.
    - **SECCOMP_SANDBOX** : Optional. If not defined, set to 1.
    - **NOVA_CPU_ALLOCATION_RATIO**: Optional, overrides the NOVA_CPU_ALLOCATION_RATIO defined in openstack_config.yaml. Values lie in the range of 0.958 to 16.0
    - **NOVA_RAM_ALLOCATION_RATIO:** Optional, overrides the NOVA_RAM_ALLOCATION_RATIO defined in openstack_config.yaml. Values lie in the range of 1.0 to 4.0
    - **NUM GPU CARDS**: Optional, for server with GPU. Value lies in the range from 0 to 6
    - **root_drive_type: <HDD or SSD or M.2_SATA, NUM_GPU_CARDS**: 0 to 6
    - **VIC Port Channel Enable**: Optional. It can be True or False. By default, it is set to True.
    - **VIC Admin FEC mode**: Optional. It can be auto, off, cl74, or cl91.
4. For B series, add the following details:

    - **Server Name**: Name for the Storage Server to be added.
    - **Rack ID**: Enter the Rack ID. (Accepts String format).
    - **Rack Unit ID**: Enter the Rack Unit ID.
    - **Chassis ID**: Enter the Chassis ID. Range for Chassis ID is 1-24.
    - **Blade ID**: Enter the Blade ID. Range for Blade ID is 1-8.
    - **CIMC Password**: Enter the CIMC Password.
    - **VM Hugepage Size**: Optional. It can be 2M or 1G. Only applicable for NFV HOSTS.
    - **RX TX Queue Size**: Optional. It can be 256, 512, or 1024.
    - **SECCOMP_SANDBOX** : Optional. If not defined, set to 1.
    - **NOVA_CPU_ALLOCATION_RATIO**: Optional, overrides the NOVA_CPU_ALLOCATION_RATIO defined in openstack_config.yaml. Values lie in the range of 0.958 to 16.0
    - **NOVA_RAM_ALLOCATION_RATIO:** Optional, overrides the NOVA_RAM_ALLOCATION_RATIO defined in *openstack_config.yaml.* Values lie in the range of 1.0 to 4.0

- **Management IPv6**: Enter IPv6 address.

  If all mandatory fields are filled in correctly, click **Save**

  > ⚠
  > - Add compute process can initiate multiple addition of compute nodes. Fill in the mandatory fields to save new compute node or press cancel to exit.
  > - Fields of pod management will remain mandatory for user input based on setup-data.

5. You may perform one among these steps mentioned below:

   - Clicking **Cancel** displays the compute node information listed in the table and **Add Compute Node** button is enabled.
   - If you feel you have filled in a wrong entry for the compute node information, click **Delete**. This will delete the entry from the table as this information is not added in the Blueprint.
   - Click **Initiate Add Compute**, displays Add node initialized message.
6. To view logs, click **View logs** under Logs column. The status of the pod will change to *Active*.
7. Two kinds of failure may occur:

   - **Add Node Pre-Failed**: When addition of node failed before the bare-metal stage (step 4), the Active Blueprint is modified but the node is not yet added in the cloud. If you press X icon, the Unified Management deletes the node information from the Blueprint and the state is restored.
   - **Add Node Post-Failed**: When addition of node failed after the bare-metal stage (step 4), the Active Blueprint is modified and the node is registered in the cloud. If you press X icon, the Unified Management first deletes the node from the Blueprint and then initiates the node removal from cloud.

   You can view the logs for this operation under **Logs** column.

Deleting Compute Node

You can remove a single or multiple compute nodes simultaneously in case of a hardware failure.

> ⚠ If your pod contains only one compute node, you cannot remove that node until you add another compute node.

1. From the navigation pane, choose **Post-Install** > **POD Management** > **Compute.**
2. Click **X** for the compute node to be removed. To remove multiple compute nodes, choose the target compute nodes which is on the extreme left column, then click **Trash** to remove multiple computes. You can remove a compute node with *Force* option which is useful when VM's are running on the node. **Node removal initiated successfully** message is displayed.
3. To view the Logs, click **View logs** under Logs column.

   - If compute nodes are removed successfully, you cannot view the compute node in the list under **Add or Remove Compute Node**.
   - If the removal of compute node fails, the **Clear Failed Nodes** button is displayed.
4. Click **Clear Failed Nodes** to remove the node from cloud and blueprint.

Managing Control Nodes

Before you replace a control node, review the following guidelines:

- Required Number of Control Nodes: A Cisco VIM pod must have three control nodes and you can only replace one node at a time.
- Validation of Nodes: When you replace a control node, Cisco VIM Unified Management validates if all the other nodes in the pod meet the minimum requirements and are in active state. If you have a storage or a compute node in a faulty state, you must correct the faulty state or delete or replace that node before you can replace the control node.
- Update Blueprint: When you replace a control node, Unified Management updates the Active blueprint for the Cisco VIM pod.
- Control Node Logs: You can access the logs for each control node from the link in the **Logs** column of Control Nodes table.

Replacing Control Node

You can replace only one control node at a time.

a. In the navigation pane, click **Post-Install > Pod Management > Control.**
b. Click (**Spin**) icon and a confirmation pop-up is shown. Click **Proceed** to continue.

   You can replace a control node with Force option for Micropod. The Force option is useful when VM's are running on the node.
c. If you want to edit a specific control node before replace, click **Edit** to update the changes.
d. On success, **Replace Node Initiated** successfully message is displayed.
e. You can view the logs in the **Logs** column on the **Control Nodes** table.
f. If the replacement of the control node fails, do the following:

   - Click the link in the **Logs** column.
   - Check the logs to determine the cause of the failure.
   - Correct the issue and attempt to replace the control node again.

> ⚠
> - For replace controller, you can change only a subset of the server information.

- For C-series, you can change the server information such as CIMC IP, CIMC Username, CIMC password, rack_id, and tor_info.
- For B-series, you can change the rack_id, chassis_id, and blade_id, but not the server hostname and management IP during the operation of replace controller.

For remove-compute, remove-storage, and replace-controller operations, Cisco VIM attempts to change the host OS boot mode to single user and power-off those server(s) to avoid the creation of duplicate IP address on the management and storage networks, and to prevent the remove/replace server from connecting back to the deployment.

If the remove/replace server is powered-off before triggering Cisco VIM remove/replace operation, then the server must not be brought back on the network as it may create duplicate IP address when connected to deployment with valid credentials.

To power up those removed/replaced server(s):
- isolate the server on the network (shutdown of corresponding ToR switchports or unplug the network cables)
- power up the server
- delete the virtual drive from CIMC
- power-cycle the server
- bring the server on the network (no shutdown of corresponding ToR switchports or plug back the network cables)

Managing Power

Managing Power

Powering of Multiple Compute Nodes

Compute node can be powered ON or OFF from the **Compute** Tab in **Pod Management** section. There is a power button associated with each compute with information provided as tooltip when you hover on that icon.

Following are the steps to power ON/OFF multiple compute nodes:

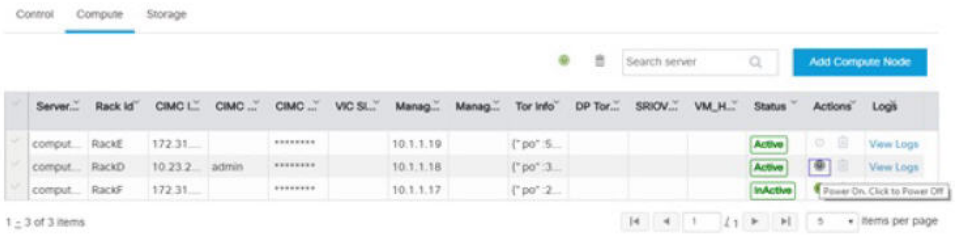
1. Click **Power** button located to the left of **Delete** button.
2. Select the compute node so that the corresponding **Power** button is enabled.

Powering ON a Compute Node

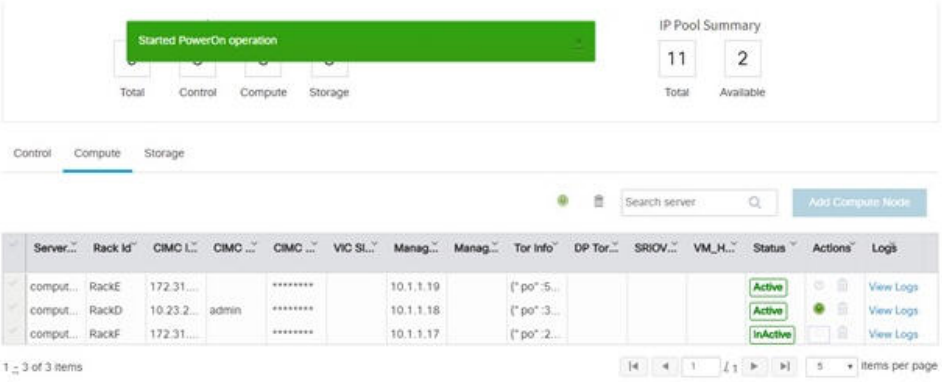
Following are the steps to power on the compute node:

1. Click the **Compute** tab.
2. In the **Pod Management** area, select the compute node that you want to power on.

> The **Power** button of a compute node is enabled only after you select the compute node.



3. Under the **Actions** column, click **Power** button of the compute node. It may take a few minutes for the compute node to power ON. The tooltip of the **Power** button displays the status of the compute node. Once the compute node is powered ON, the **Power** stops blinking and its color changes to green.



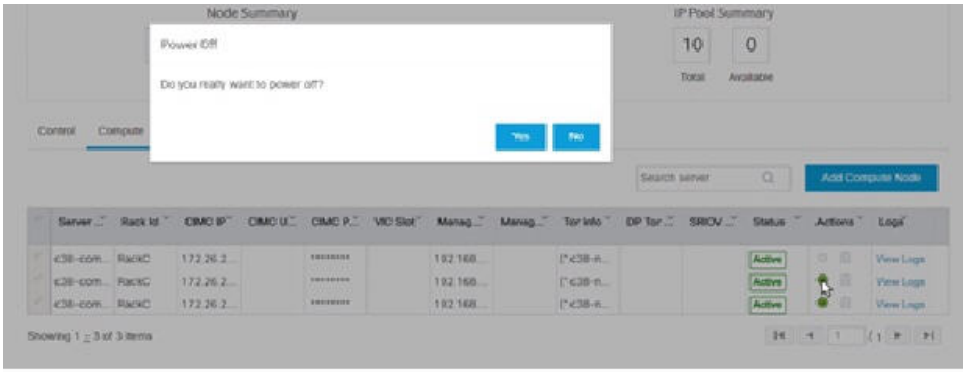
You can add a compute node only when the power ON task is complete.

Powering OFF a Compute Node

> ⚠ You cannot power off all the compute nodes. There must be at least one compute node in ON state.

Follow these steps to power OFF a compute node:

1. Click the **Compute** tab.
2. In the **Pod Management** pane, under the **Actions** column, click the **Power** button of the compute node that you want to power off.



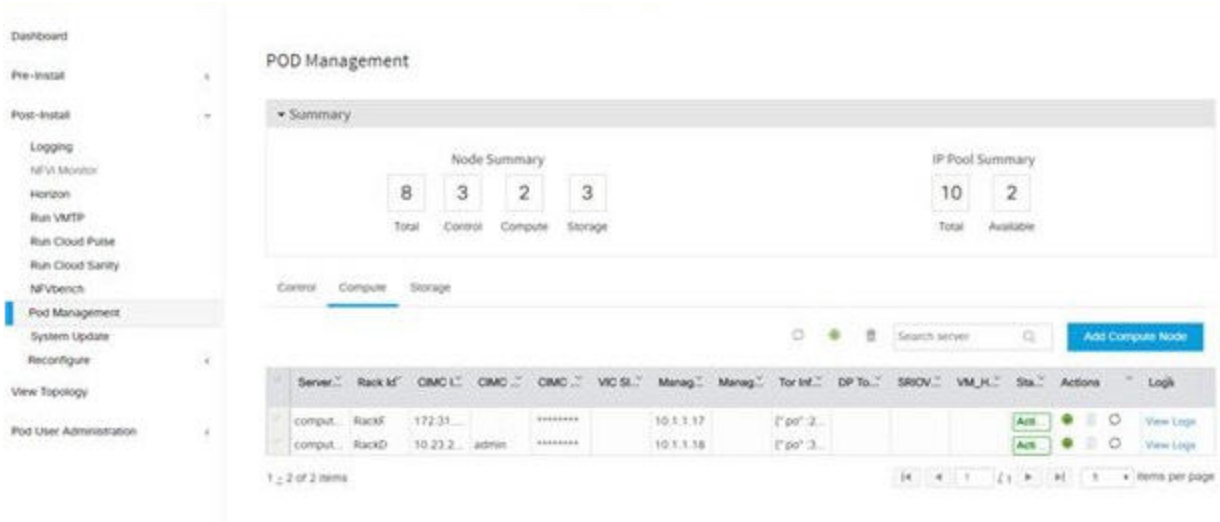
3. Click **Yes** in the confirmation dialog box.

   It may take a few minutes for the compute node to power OFF. The tooltip of the power button displays the status of the compute node. Once the compute node is powered OFF, the **Power** button stops blinking and its color changes to grey.

> ⚠ If there is only one compute node in the grid, and you try to power OFF it, a message **Last compute node can't be powered off** is displayed. Also, when you power off the last available compute node in the list of nodes, the message **At least one compute node should be powered on** is displayed.

Powering/ Delete/ Reboot Operation for Multiple Computes

You can perform power, delete, and reboot operation on multiple compute nodes using the global buttons located at the top of grid. To enable this operation, select at least one compute node.



Rebooting Compute Node

To reboot the compute node, follow the below steps:

1. Click on **Compute** tab.
2. In the Pod **Management** pane, under the **Actions** column, click **Reboot** of the compute node that you want to reboot.
3. Click **Yes** in the confirmation dialog box, to perform reboot. You can reboot a compute node with *Force* option which is useful when VM's are running on the node.

Powering/ Delete/ Reboot Operation for Multiple Computes

You can perform power, delete, and reboot operation on multiple compute nodes using the global buttons located at the top of grid. To enable this operation, select at least one compute node

The following figure explains the pod management operation:

Searching Compute and Storage Nodes

This functionality allows you to search the compute and storage nodes by server names only. The search result is generated or shows an empty grid if there are no results. The following figure shows the storage node search results.

Control Compute Storage

c38-storage-1 Add Storage Node

Server Na...	Rack Id	CIMC IP	CIMC Use...	CIMC Pas...	VIC Slot	Tor Info	Managem...	Managem...	Status	Actions	Logs
c38-storag...	RackA	172.26.229...		********		{" c38-n9k...	192.168.38...		Active		View Logs

Showing 1 - 1 of 1 items

1 / 1

Pod Users

Pod Users

The Pod Users page gives you the details associated with the pod, status (Online or Offline) and their roles.
UM admin manages all the 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. You cannot revoke the user's permission, if the user is the only user with a *Full-Pod-Access* role for that particular pod. In this case, you can grant another user with a *Full-Pod-Access* role for that pod and then revoke permission of the old user.

> ⚠ If the user is revoked from the last associated pod, then the user is deleted from the system.

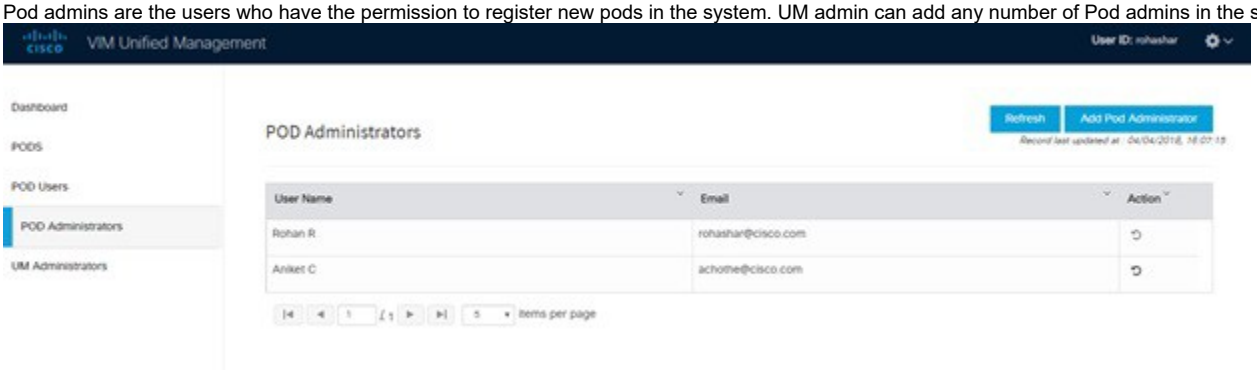
Deleting Users

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 this case, you can grant another user 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 Administrator

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



Adding Pod Admin

1. Log in as **UI Admin** and navigate to POD Administrator page.
2. Click **Add Pod Administrato**r.
3. Select User auth for the new user. This option is enabled only if LDAP mode is true.
4. Enter the Email ID/LDAP user id (if LDAP user attribute is set to uid) of the user.
    - If the email is already registered, the **Username** gets populated automatically.
    - If the 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.
5. Navigate to https://br_api :9000.
6. Enter the **Email ID** and **Password** of the Pod Admin
7. Click **Login as Pod User**. It redirects to the landing page where 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.

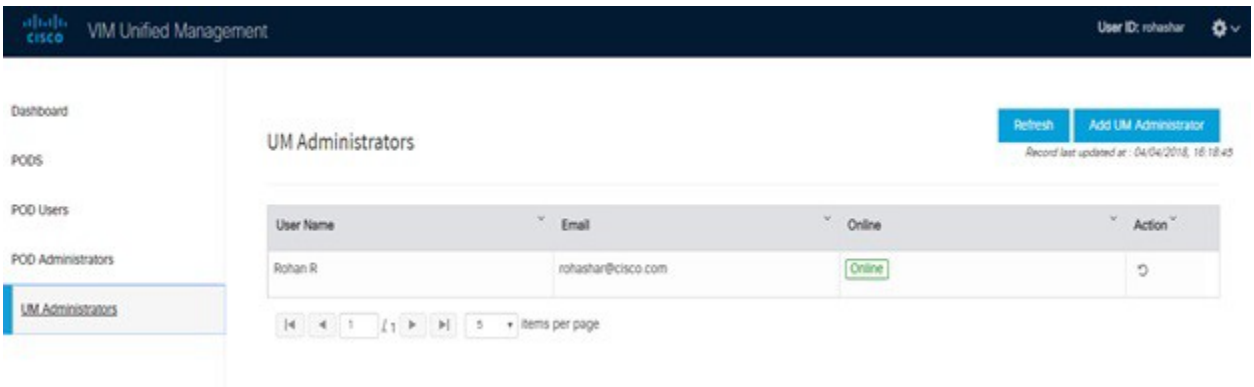
> ⚠ You cannot revoke self permission.

UM Administrator

UM Administrator

UM admins have access to the UM profile. Only an UM admin can add another UM admin in the system.

> ⚠ Ensure that there must be at least one UM admin in the system.



Adding UM Admin

To add a UM admin perform the following steps:

1. Log in as **UI Admin** and navigate to UM Administrator page.
2. Click **Add UM Administrator**.
3. Select User auth for the new user. This option is enabled only if LDAP mode is true.
4. Enter the Email ID/ LDAP user id (if LDAP user attribute is set to uid) of the user.
    - If email is already registered, the **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.
5. Navigate to https://br_api: 9000.
6. Enter the Email ID and Password of the UM Admin**.**
7. Click **Log in as UM admin** to view the 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.

> ⚠ You cannot revoke the permission for yourself. You can revoke user permission, if the user is not associated with any pod. After revoking, the user is deleted from the system.

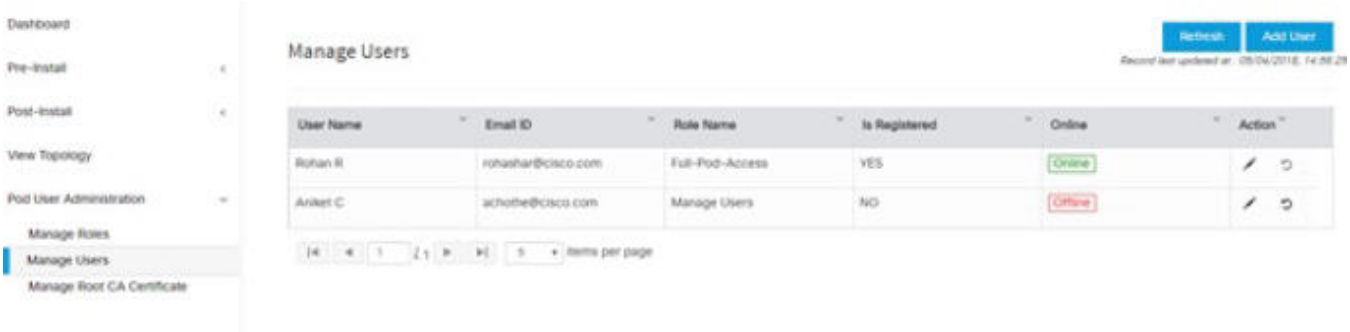
Pod User Administration

Pod User Administration

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

Managing Users

Allows you to add the users. It shows all the users associated with the pod. You can check the online status of all the user. Click **Refresh** on upper right corner to check the status.



Adding Users

To add a new user, follow the below steps:

1. Click **Login as PODUser**.
2. Navigate to **POD UserAdministration**.
3. Click **ManageUsers**.
4. Click **Add Users** to add a new user.
5. Complete the following fields in the **Add Users** page of the Cisco VIM Insight/UM:

Field Name	Field Description
User auth	Select the User auth for the new user. This option is enabled only if LDAP mode is True.
Select User	While adding new pod-user, a list of users having pod-user permissions is displayed in the user-registration form. This list is available only, when DISPLAY_ALL_POD_USERS is set to True.
Registration Type	Registration type can be User/Group, only when User Auth is LDAP. Following fields are available when the Registration Type is *Group*: • Group Dn – Enter the distinguished name of the LDAP group. • Group Name – Enter the name of the LDAP group
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.

6. Click **Save**.

Editing Users

A user with Full-Pod-Access or Manage Users permission can edit other user's permission for that specific pod.

To edit user's permission:

1. Click **Edit** icon.

2. Update the permission.
3. Click **Save**. The grid gets refreshed automatically.

Revoking Users

User with Full-Pod-Access or Manage Users permission can revoke other users from the specific Pod.

To revoke users:

1. Click **Undo** icon. A confirmation pop up appears.
2. Click **Proceed** to continue.

> ⚠ Self revoke is not permitted. After revoking the user, if the user is not associated with any other pod, then the revoked user is auto-deleted from the system.

Managing Roles

To create a new role, follow the below steps:

1. Click **Log in as POD User**.
2. Navigate to **Pod User Administration** and click **Manage Roles**. By default, you will see a full-pod-access role in the table.
3. Click **Add Role** to create a new role.
4. Complete the following fields on the **Add Roles** page in Cisco VIM Insight:

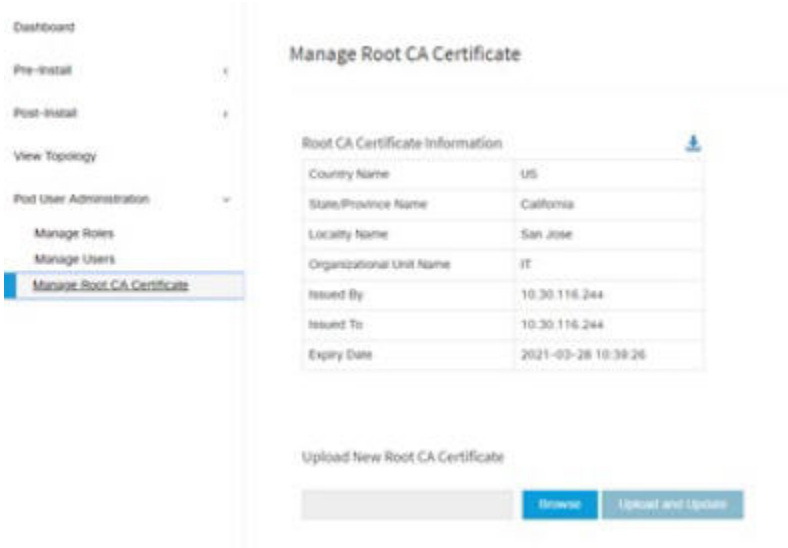
Field Name	Field Description
Role	Enter the name of the role.
Description	Enter the description of the role.
Permission	Check the **Permission** check box to select the permission.

5. Click **Save**. Once the Blueprint is in an active state, all the permissions are the same for both C-series and B-series pods other than Reconfigure CIMC Password which is missing for B-series pod.

> ⚠ Permissions are divided into 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 pod registration. 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, follow the below steps:

1. Click **Login as POD User**
2. Navigate to **POD User Administration >Manage Root CA certificate**.
3. Click **Browse** and select the certificate that you want to upload.
4. Click **Upload.**

- If the certificate is invalid and does not match with the certificate on the management node located at (**var/www/mercury/mercury-ca.crt**), Insight/UM reverts the certificate which is used previously.
- If the certificate is valid, Insight/UM performs a management node health check and then updates the certificate with the latest one.

The CA certificate that you upload must be same as the one which is in the management node.

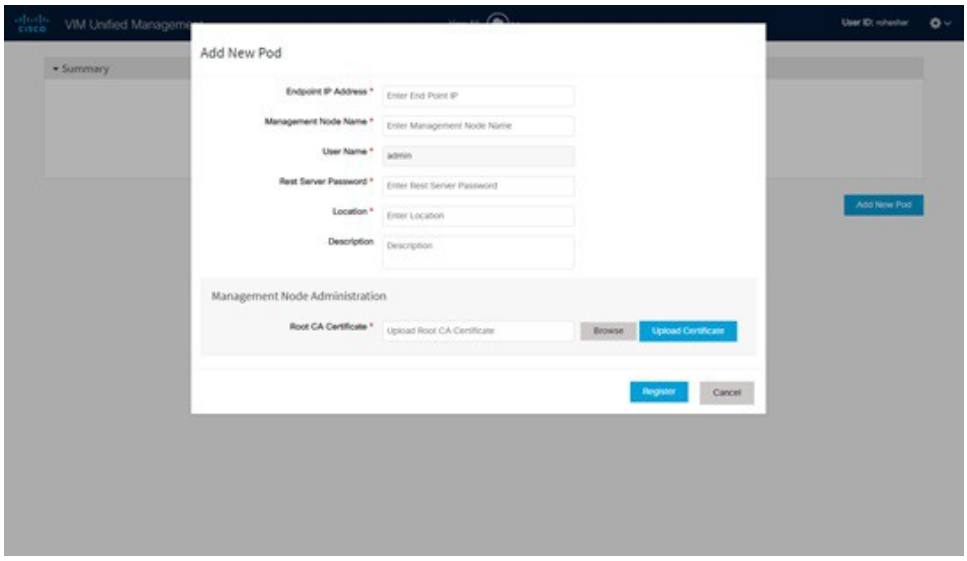
Registering New Pod to Insight

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 must register a Pod Admin to allow them to access a pod.

1. Log in as **UM Administrator**.
2. Navigate to Pod Administrator and click **Add Pod Admin**.
3. Enter the Email ID and the Password of the Pod Admin and click **Login as Pod User**. Then, you will be redirected to the landing page.
4. Click **Add New Pod** to register a Pod. The **Add New Pod** popup window appears on the screen.



5. Enter the br_api of the pod management node as the **Endpoint IP Address** and **Rest Server Password** from the file **/opt/cisco/ui_config.json.**
6. Enter the values for the remaining fields in **Add NewPod**.
7. Click **Browse** to select the Root CA certificate. For more information on Root CA certificate, see Managing Root CA Certificate.
8. Click **Upload Certificate** to upload the selected Root CA certificate.
9. Click **Register** to start the Pod registration. The newly created pod appears on the landing page.

> You can edit or delete pods, and update Rest API password from the landing page if the logged-in user has Pod Admin access.

Context Switching Between Pods

Context Switching Between Pods

Cisco VIM UM permits you to switch between two or more pods for a particular node. You can be an admin for one or more pods, and a user for some other pods simultaneously. The ability to access multiple pods helps you to maintain context and yet scale from a pod management point of view.

Following are the two ways to switch from one pod to another.

- Context Switching icon: **Context Switching** Icon is situated on the top right corner from the tool tip of the UI. Click **Context Switching** icon to view all the pods that you can access. The pod with a red dot indicates that the REST password entered during management node registration does not match with the current REST password for that particular node. In this case, the Pod admin or user must reach out to UI admin to update the password for that node. UI admin updates the password from **Manage Pods** in **Unified Management UI admin** portal.

- Switch between management nodes: Use dashboard to switch between management nodes. You can see all the pods in the table and navigate to any pod using a single click. If mouse pointer changes from hand or cursor to a red dot sign, it indicates that the REST Password entered during management node registration does not match with the current REST Password for that particular node.

Cisco VIM Pod Software Update

Cisco VIM Pod Software Update via UM

Software management of your Cisco VIM pods includes software update, reconfiguration of OpenStack services and password, and so on.

As part of the lifecycle management of the cloud, VIM can bring in patches like bug fixes related to code, security, and so on. Thereby, providing cloud management facility from software point of view. The software update of the cloud is achieved by uploading a valid tar file, following the initiation of a system update from the Unified Management.

To update Cisco VIM software, follow the below steps:

1. In the navigation pane, click **Post-Install > System Update**.
2. Click **Browse** and select the valid tar file.
3. Click **Open**.
4. Click **Upload** and **Update**. **Update started Successfully** message is displayed and update status is shown as **To Update**.
5. Click the hyperlink to view the reconfigure logs for install logs. Reconfigure status is available on the page or the dashboard under **POD Operation** details. A message **System Update has been initiated** is displayed. Logs front-ended by hyperlink are available in the section **Update Logs** which shows the progress of the update.
6. During software update, all other pod management activities are disabled.
7. Post-update, normal cloud management commences.
8. Once update is completed, you can see the status of update in the box below.
9. If log update fails, **Auto-RollBack** is initiated automatically. If log update is successful, you will have two options to be performed:
    a. Commit: To proceed with the update.
    b. Rollback: To cancel the update.
10. If auto-rollback fails during software update fails through Unified Management UI, the administrator must contact Cisco TAC for support. Do not re-try the update or delete the new or the old installer workspace.
11. If the update is successful and reboot is required for at least one compute node:
    a. Only commit or rollback is allowed.
    b. Following operations are not permitted:
        - Reconfigure
        - System update
        - Pod management

You can reboot the node, only after the commit or rollback operation.

Day 2 Reconfigure/Enablement

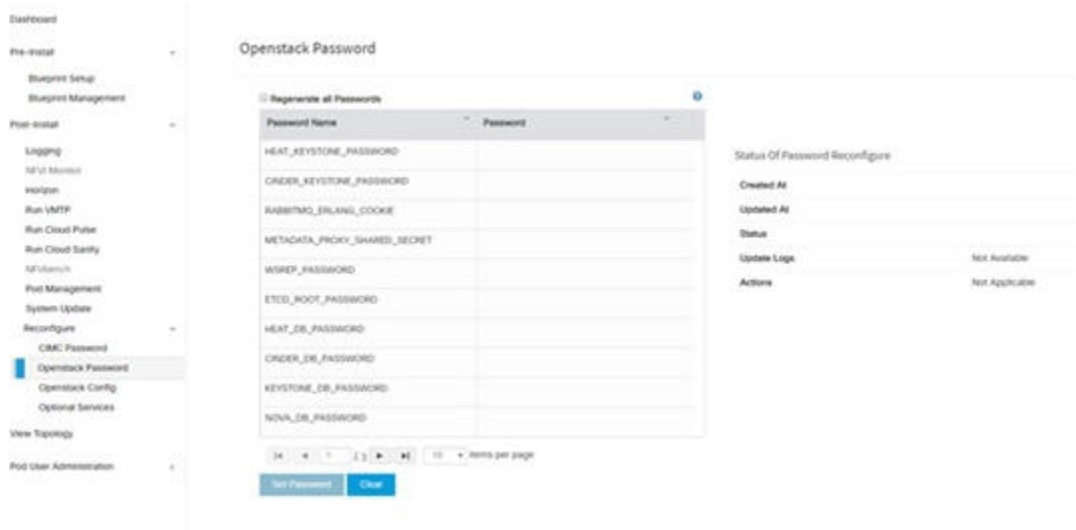
Reconfigure/Enablement of Features on Day 2

This section applies to pods that are successfully deployed. There are multiple sub-links available to manage the Day n operations of the pod. However, often UM cross-launches the relevant services, by delegating the actual rendering to the individual services.

Reconfiguration of OpenStack Passwords

There are two options to regenerate the passwords:

- Regenerate all passwords: Select **Regenerate all passwords** and click **Set Password**. This automatically regenerates all passwords in alphanumeric format.
- Regenerate single or more password: A specific password is set by doing an inline edit for any service like Horizon's ADMIN_USER_PASSWORD. Double click on the file under Password and enter the password to enable **Set Password**.



During the reconfiguration of password, all other pod management activities are disabled. Post-update, normal cloud management commences. If the password reconfiguration fails, all subsequent pod management operations are blocked. To resolve the situation through CLI, contact Cisco TAC.

Reconfiguration of OpenStack Services, TLS Certificates, and ELK Configurations

Cisco VIM supports the reconfiguration of OpenStack log level services, TLS certificates, and ELK configuration.

Following are the steps to reconfigure the OpenStack and other services:

1. In the navigation pane, click **Post-Install > Reconfigure Openstack Config**.
2. Click the specific item that you want to change and update. For example, to update the TLS certificate, click the path to the certificate location.
3. Enter **Set Config** to commence the process.

During the reconfiguration process, all other pod management activities are disabled. Post-update, normal cloud management commences. If reconfigure of OpenStack Services fails, all subsequent pod management operations are blocked.

To resolve the situation through CLI, contact Cisco TAC.

Reconfiguration of CIMC Password through Unified Management

Cisco VIM allows you to 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.

You need to match the following password rule to update the password:

- 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.

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

1. Log into **CISCO VIM Unified Management**.
2. In the navigation pane, select **Post-Install.**
3. Click **Reconfigure CIMC Password**.
4. You can reconfigure the CIMC Password at global level by adding new CIMC_COMMON Password. To reconfigure CIMC Password for individual servers, double-click the server password that you want to edit.
5. Click **Reconfigure** to initiate reconfigure process.

Re-configuration of Optional Services (High Level Flow)

Cisco VIM offers optional services such as heat, migration to Keystone v3, NFVBench, NFVIMON, and so on, that can be enabled post deployment of pod. You can enable these services in one-shot or selectively.

Listed below are the steps to enable optional services:

1. In the navigation pane, click Post-Install > Reconfigure Optional Services.
2. Choose the right services and update the fields with the right values.
3. Click Offline validation.
4. Once offline validation is successful, click **Reconfigure** to commence the process.

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

If reconfigured OpenStack services fail, all the subsequent pod management operations are blocked. To resolve the situation through CLI, contact Cisco TAC.

All reconfiguration features contain repeated re-deployment option set to True or False. If repeated re-deployment is set to True, you can change the values associated to the feature. If repeated re-deployment is set to False, you can deploy the feature only once. Un-install of the feature is only supported as an exception

Deployment Status :

Optional Features	Repeated re-deployment Option
APICINFO	False
DHCP reservation for VM MAC address	True
EXTERNAL_LB_VIP_FQDN	False
EXTERNAL_LB_VIP_TLS	False
INSTALL_MODE	True
HTTP_PROXY & HTTPS_PROXY	True
LDAP	True
NETWORKING	True
NFVBENCH	False
NFVIMON	True. Can be un-installed.
PODNAME	False
PROVIDER_VLAN_RANGES	True
SYSLOG_EXPORT_SETTINGS	False
TENANT_VLAN_RANGES	True
TORSWITCHINFO	False

VIM _ ADMINS	True
VMTP	False
VTS_PARAMETERS	False
AUTOBACKUP	True
Heat	False
Ironic	False
Cobbler	True
ES Remote Backup	True
CVIM-MON	True
NETAPP_SUPPORT	True
Enable Read-only OpenStack Admins	True
Base MAC address	True
VAULT	False
Cloud Settings	True
IPA	True
Trusted_vf on a per server basis	False

Reconfiguring Optional Features

1. Log into Cisco VIM UM.
2. In the navigation pane, expand the Post-Install section.
3. Click **Reconfiguring Optional Feature** through UM.
4. Enter the data for the following fields:

Name	Description
Heat	Enable Heat.
Enable Read-only OpenStack Admins	Check/uncheck Enable Read-only OpenStack Admins.
Keystone v3	Enable Keystone v3.
ENABLE_ESC_PRIV	Enable ENABLE_ESC_PRIV .
Autobackup	Enable/Disable Autobackup.
External LB VIP TLS	Enable External LB VIP TLS.
External LB VIP FQDN	Enter input as a string.
Pod Name	Enter Input as a string.
Tenant Vlan Ranges	Augment tenant vlan ranges input. For example: 3310:3315.
Provider VLAN Ranges	Enter input to tenant vlan ranges. For example: 3310:3315.
Install Mode	Select **Connected** or **Disconnected** from the drop-down list.
VAULT	Enable Vault, if it is not deployed on Day 0.
Cloud Settings	Following are the options: • **keystone_lockout_failure_attempts**: Number of incorrect password attempts before the user is locked out. Values are 0 by default for no lockout, and can be in the range of 0 to 10. • **keystone_lockout_duration**: Number of seconds a user is locked out. By default, it is 1800 for 30 minutes. Values are in the range of 300 (5 minutes) to a maximum of 86400 (24 hours).

	• **keystone_unique_last_password_count**: Forces the user to change their password to a value not used before. Default is 0 for no history check.Values are in the range of 0 to 10. • **keystone_minimum_password_age**: Restricts you to change their password at most every this many days. Default is 0 for no limit. Values are in the range of 0 to 2. • **horizon_session_timeout**: Number of seconds of inactivity before Horizon dashboard is logged out. Default is 1800 for 30 minutes. Values are in the range of 300 (5 minutes) to maximum of 86400 (24 hours).
Registry Setup Settings	• **Registry User Name**: It is a mandatory field. • **Registry Password**: The minimum length of the password is three. • **Registry Email**: It is a mandatory field. • **Registry Name**: It is a mandatory field, only when Cisco VIM Software Hub is enabled. For example, Registry FQDN name.
Syslog Export Settings	• **Remote Host** : Enter Syslog IP address. • **Protocol**: Only UDP is supported. • **Facility**: Defaults to local5. • **Severity**: Defaults to debug. • **Clients**: Defaults to ELK. • Port: Defaults to 514, but can be modified.
Configure ToR	True or False. Default is False.
ToR Switch Information	• **Name**: Enter the ToR switch name. • **Username**: Enter the ToR switch username. • **Password**: Enter the ToR switch Password. • **SSH IP**: Indicates ToR switch SSH IP Address. • **SSN Num**: ToR switch ssn num. output of show license host-id. • **VPC Peer Keepalive**: Peer Management IP. You need not define if there is no peer. • **VPC Domain**: Need not define if there is no peer. • **VPC Peer port**: Interface for vpc peer ports. • **VPC Peer VLAN Info**: vlan ids for vpc peer ports (optional). • **BR Management Port Info**: Management interface of the build node. • **BR Management PO Info**: Port channel number for the management interface of the build node. If setup data is ACI VLAN with ToR, then reconfigure options are: • **Host Name**: ToR switch name. • **VPC Peer Keep alive**: Peer Management IP. • **VPC Domain**: Do not define if there is no • **Node ID**: Integer, unique across all switches. ⚠ To add information for ToR Switch, click +
NFVBench	By default, it is set to False. • **Add ToR information connected to switch**: Select a ToR Switch and enter the Switch name. • **NIC Ports**: INT1 and INT2 optional input, enter the two port numbers of the 4-port 10G Intel NIC at the management node used for NFVBench. For example, eth1/5. For mechanism driver VPP, there are two optional fields in NFVBENCH if network option is available: • **VTEP IPs**: Mandatory for NFVBench with VXLAN. It must be comma separated IP pair in vxlan-tenant network, but not in the tenant pool. • **VNIs**: Mandatory for NFVBench with VXLAN, and must be comma separated vnid_id pairs. For mechanism driver VTS: **VTEP IPs**: Mandatory for VTS/VXLAN only. It must be comma separated IP pair belonging to tenant network segment, but not in the tenant network pool. ⚠ If ToR is already present in setup-data or already deployed, ToR information need not be added. By default, the ToR information switch name is mapped in NFV bench.
Swiftstack	• **Cluster End Point**: IP address of PAC (proxy-account-container) endpoint. • **Admin User**: Admin user for swift to authenticate in keystone. • **Admin Tenant**: The service tenant corresponding to the Account-Container used by Swiftstack. • **Reseller Prefix**: Reseller_prefix as configured for Keystone Auth,AuthToken support in Swiftstack E.g KEY_ • **Admin Password**: swiftstack_admin_password • **Protocol** drop-down list: http or https. ⚠ SwiftStack is only supported with Keystone v2. If you select Keystone v3, swiftstack will not be available for configuration.

LDAP with Keystone v3	• **Domain Name** field: Enter the Domain name. • **Object Class for Users** field: Enter a string as input. • **Object Class for Groups**: Enter a string. • **Domain Name Tree for Users**: Enter a string. • **Domain Name Tree for Groups** field: Enter a string. • **Suffix for Domain Name** Field: Enter a string. • **URL**: Enter a URL with port number. • **Domain Name for Bind User** field: Enter a string. • **Password**: Enter Password as string format. • **User Filter**: Enter filter name as string. • **User ID Attribute**: Enter a string. • **User Name Attribute**: Enter a string. • **User Mail Attribute**: Enter a string. • **Group Name Attribute**: Enter a string.
NFVI Monitoring	• **Master Admin IP**: Enter the input in IP format. • **Master 2 Admin IP**: Enter the input in IP format. • **Collector Management IP**: Enter the input in IP format **Collector VM1 info** • **Host Name** field: Enter Host Name as a string. • **CCUSER** field: password field Enter Password. • **Password** field: Enter password. • **Admin IP** field: Enter Input as IP format. • **Management IP** field: Enter Input as IP format. **Collector VM2 info** • **Host Name** field: Enter a string. • **CCUSER** field: Enter Password. • **Management IP** field: Enter Input as IP format. **Dispatcher** • **Rabbit MQ Username** Field: Enter a string. • **NFVIMON_ADMIN**: Enter a single string. Can have only one and is optional.
VTS Parameter	• **VTC SSH Username**: Enter the string • **VTC SSH Username** : Enter the password
VMTP	Check one of the options to specify a VMTP network: • Provider Network • External Network For provider network: • **Network Name** : Enter the name for the external network. • **IP Start** : Enter the starting floating IPv4 address. • **IP End** : Enter the ending floating IPv4 address. • **Gateway** : Enter the IPv4 address for the Gateway. • **DNS Server** : Enter the DNS server IPv4 address. • **Segmentation ID** field: Enter the segmentation ID. • **Subnet:** Enter the Subnet for Provider Network. For external network: • **Network Name**: Enter the name for the external network. • **Network IP Start**: Enter the starting floating IPv4 address. • **Network IP End**: Enter the ending floating IPv4 address. • **Network Gateway**: Enter the IPv4 address for the Gateway. • **DNS Server**: Enter the DNS server IPv4 address. • **Subnet:** Enter the Subnet for External Network.
Networking	To reconfigure networking, • **IP Tables**: Click Add (+) to add a table. Enter input as subnet format. E.g. 12.1.0.1/2 • **http_proxy_server**: Enter HTTP_PROXY_SERVER. E.g. <a.b.c.d:port> • **https_proxy_server**: Enter HTTP_PROXY_SERVER. E.g. <a.b.c.d:port> • **NTP Server**: Click Add (+) to add server. You can delete or edit the entered value, but you cannot delete all the data. A minimum of 1 server is required. Maximum of four NTP servers can be present. • **Domain Name Server**: Click Add (+) to add server. You can delete or edit the entered value, but cannot delete all the data. Minimum of 1 server is required, but maximum of three DNS servers can be present. • **Head-end replication**: Add VTEP IP address and comma separated VNI IDs. Multiple entries are allowed. You can change VTEP IP for individual compute/control servers. ⚠ Whenever HER is removed from both vxlan-tenant and vxlan-tenant, all the vtep ips associated with the computes are removed.

	• **Layer 3 BGP Adjacency**: Applicable to control servers only when VXLAN is enabled in NETWORK OPTIONS.IPs are picked up from management subnet, but not from IP pool. You can change the existing IP values if required. ⚠ In reconfigure optional services networking, you can reconfigure IP tables, or add http_proxy/https_proxy.
APICINFO	The input must be in the format. <ip1|host1>:[port]. For example: 12.1.0.12 ⚠ APIC hosts can be reconfigure minimum of 1 host and maximum of 3 hosts but not 2.
Vim_admins	• **Username**: Enter the User Name. To add a new root user, Click **+.** To remove the existing user, Click **-** • **admin hash password**: Enter the admin hash password and it must start with $6. ⚠ At least, one VimAdmin must be configured, when Permit root login is false.
Cobbler	**admin password hash:** It should start with '$6'. Use the command: `python -c 'import crypt; print crypt.crypt ("<plaintext_strong_password>")'`
ES Remote Backup	• **Service**: Displays NFS by default, if the remote NFS server is used. • **Remote Host**: It is the IP of the NFS server. • **Remote Path**: It is the path of the backup location in the remote server.
CVIM-MON	• **Low Frequency**: Enter the value such that it is higher than medium frequency. Minimum value is 1 minute. By default, it is set to 1 minute. • **Medium Frequency**: Enter the value such that it is more than high frequency. Minimum value is 30 seconds. By default, it is set to 30 seconds. • **High Frequency**: Enter the value such that the minimum value is 10 seconds. By default, it is set to 10 seconds. ⚠ Set **ui_access** to True in deployed Blueprint, to enable the Cisco VIM monitor link. This property is reconfigurable. If set to False, the link is disabled.
NETAPP_SUPPORT	• **Server port**: It is the port of NetApp management or API server. Select 80 for HTTP and 443 for HTTPS. • **Transport Type:** It is the port of NetApp management or API server. It can be HTTP or HTTPS. • **NetApp Cert Path**: It is the root ca path for NetApp cluster, only if protocol is HTTPS

5. Click **Offline Validation**.
6. If offline validation is successful, click **Reconfigure** to commence the process.

Pod Management for Active Blueprint

Pod Management for Active Blueprint

This option is available only to a pod, which is successfully deployed. There are multiple sub-links available to manage the day-n operation of the pod. However, often Insight cross-launches the relevant services, by 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:

1. Login as **POD User.**
2. Naviagte to **POD.**
3. Navigate to **Post-install**
4. Click **Monitoring**
5. The **Authentication Required** browser pop up is displayed.
6. Enter the **username** as admin.
7. 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.

   > ⚠ To view Kibana logs, you can click on **Click here to view Kibana logs in new tab** link

Cross Launching Horizon

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

1. In the navigation pane, click **Post-Install** > **Horizon**.
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 VM2Info**.

1. Login as **POD User.**
2. Naviagte to **POD.**
3. Navigate to **Post-install.**
4. Click **Reconfigure**.
5. Click **NFVI Monitoring**
6. Click the link **Click here to view NFVI monitoring**. You will be redirected to NFVI monitoring page.

Run VMTP

Cisco VIM 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 into 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**.

> ⚠ If VMTP stage is skipped or not run during blueprint Installation, the post installation is disabled.

Run CloudPulse

In Cisco VIM, an integrated tool called Cloud Pulse periodically checks the cloud services endpoint. The test results of these are reflected under the Cloud Pulse link. You can also run these API endpoint tests on-demand, and fetch the test results 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 NFVbench

You can execute **Run NFV Bench** for B and C series pod, through Cisco VIM Insight. On a pod running with Cisco VIM, 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

1. Log-in to **CISCO VIMInsight**.
2. In the Navigation pane, click **Post-Install** > **Run NFVBench.**
3. Click **NDR/PDR** test and complete the following fields.

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

Fixed Rate Test

1. Log in as **POD User.**
2. Navigate to **POD.**
3. Navigate to **Postinstall.**
4. Click **Run NFV Bench**.
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

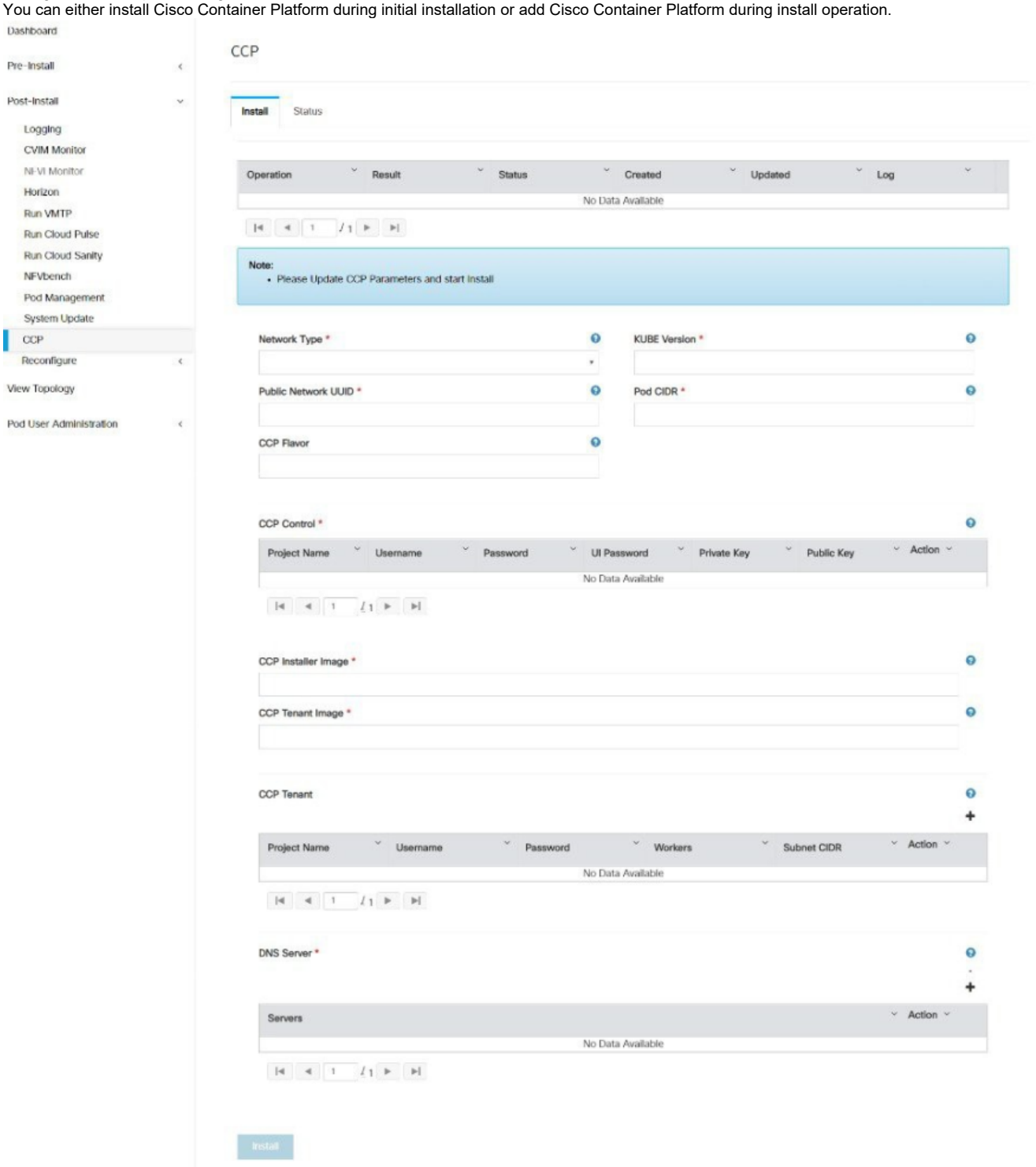
One of the key aspects of Cisco VIM is that it allows the admin to perform pod life-cycle management from a hardware and software perspective. The nodes of a given pod corrupt at times and Cisco VIM provides the ability to add, remove or replace nodes based on the respective roles with some restrictions. The following operations are allowed on a running pod:

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

2. **Add or Remove Computes Nodes**: You can replace N-compute nodes simultaneously. However, at any given point, at least one compute node must be active.
3. **Replace Control Nodes**: Double fault scenarios are not supported, while the replacement of one controller at a time is supported.

Cisco Container Platform

You can install, verify, and cleanup Cisco Container Platform for both B-series and C-series pod with OVS/VLAN tenant type through Cisco VIM Unified Management. On a pod running with Cisco VIM, choose a Cisco Container Platform link on the NAV menu.
You can either install Cisco Container Platform during initial installation or add Cisco Container Platform during install operation.



After successful installation, you can either do verify or cleanup operation.

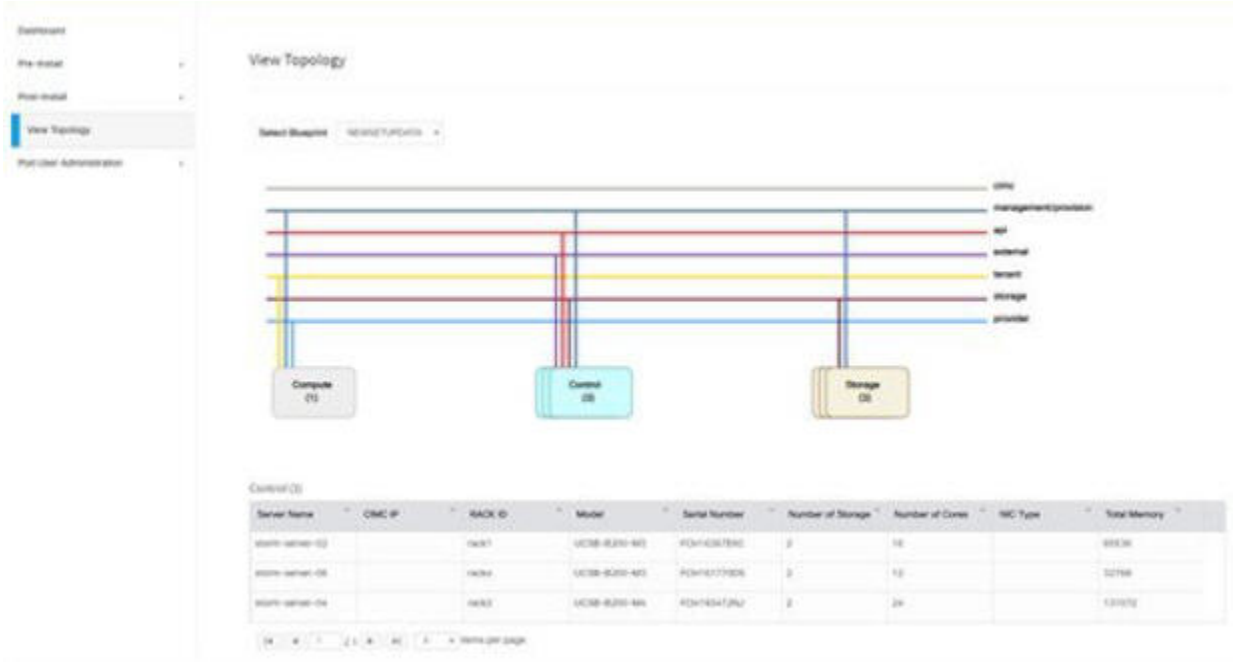
1. Log into **Cisco VIM Unified Management**.
2. In the navigation pane, click **Post-Install** >**CCP**.
3. Under **Install** tab, enter the following values if not defined during initial installation.

Name	Description
Network type	It can be tenant or provider.
Kube version	Version of Kubernetes to be installed
Public network UUID	UUID of Openstack external network or provider network.
Pod CIDR	Optionally, used for calico network.
Cisco Container Platform Flavor	Optional, but mandatory when NFV_HOSTS is enabled during Cisco Container Platform installation
Cisco Container Platform Control	**Project Name**:Tenant name to create in Openstack to host tenant cluster. It is mandatory for network type tenant and provider. **Username**: Username of openstack tenant. It is mandatory for network type tenant and provider. **Password**: Password for the Openstack tenant. It is mandatory for network type tenant and provider. **UI Password**: Password for Cisco Container Platform UI. It is mandatory for network type tenant and provider. **Private Key**: Private key used to SSH to VM must be ed25519. It is mandatory for network type tenant and provider. **Public Key**: Public key for Cisco Container Platform VMs, for example /root/ecdsa-key.pub. It is mandatory for network type tenant and provider. **Cisco Container Platform Subnet**: Subnet to deploy Cisco Container Platform. **Control plane installer subnet** : Subnet to create for bootstrap installer. It is mandatory for network type tenant. **Installer Subnet Gateway**: Gateway used for bootstrap installer. It is mandatory for network type tenant.
Cisco Container Platform Installer Image	Pointer to the Cisco Container Platform installer image (required)
Cisco Container Platform Tenant Image	Pointer to Cisco Container Platform tenant cluster image (required)
Cisco Container Platform Tenant	**Project Name**: Tenant name to create in Openstack to host tenant cluster. It is mandatory. **Username**: Username for openstack tenant. It is mandatory. **Password**: Password for tenant. It is mandatory. **Workers**: Number of kubernetes workers in tenant cluster. It is mandatory **Tenant Subnet CIDR**: Tenant subnet CIDR. It is mandatory.
DNS Server	DNS server to be reachable from cloud (required)

View Topology

View Topology

You can view the graphical representation of the control, compute, and storage node that is associated with the various network segments.



You can click **Control**, **Compute**, or **Storage** from the topology, to view the details of respective node.

Cisco VIM Update/Upgrade

Update/Upgrade

Prerequisites and Assumptions

Prerequisites/Assumptions for Update/Upgrade

During Cisco VIM update, ensure that no interference exists with external monitoring services.
To handle the potential of docker corruption post repo/kernel update, you must follow the below steps during VIM update irrespective of the update methodology (connected or disconnected).

- You must disable NFVIMON monitoring for all server CIMC, only if NFVIMON/Zenoss is used. This prevents the failure of VIM update, when Cisco VIM is deprived of CIMC login with valid credentials. Once Cisco VIM software update/commit or any other pod management operation is completed, you can re-enable Zenoss monitoring.
- If ACI fabric is integrated with NFVI, you must disable switch policy enforcement that can shutdown the ToR ports to which the NFVI server interfaces are connected, during software update. This is required as the MAC-moves for floating IP addresses happen during software update with L3 agent failover due to host package update and/or L3 agent container update. Multiple L3 agent failover can result in several Mac-moves in a short period of time. Fast Mac-moves over a five minute duration can potentially trigger N9K/ACI Mac-move policy violation, thereby causing an immediate shutdown of the server switch port.

Updating Cisco VIM in Running Cloud

Updating Cisco VIM in Running Cloud

Cisco VIM allows you to update all OpenStack and infrastructure services such as RabbitMQ, MariaDB, and HAProxy, and management node containers such as Cobbler, ELK, VMTP, and repo containers with almost no impact to the Cisco NFVI implementation.

Updates allows you to integrate Cisco VIM patch releases without redeploying the Cisco NFVI stack from the beginning. Updates have minimal service impact because they run serially component-by-component one node at a time. If an error occurs during an update, auto-rollback is triggered to return the cloud to the state that existed before the update is performed. After an update, you can check for any functional impacts on the cloud. If everything is fine, you can commit the update, to delete the old containers and old images from the nodes. If you see any functional cloud impact, you can perform a manual rollback to start the old containers again.

Before you begin a container update, ensure that:

- Updates are not supported for registry-related containers and authorized_keys.
- You cannot rollback the repo containers on the management node to an older version once updated, as the rollback deletes the node packages and causes the cloud to destabilize.
- Cloud sanity check is performed before the update is started, to prevent double-faults.

The following table provides various options to update OpenStack using Cisco VIM. The Internet options refer to management node connectivity to the Internet. If your management server lacks Internet access, you must have a staging server with Internet access to download the Cisco VIM installation artifacts to a USB stick. Ensure that you select either of the two options and stay with it for the entire lifecycle of the pod.

	Without Cisco VIM Unified Management	**With Cisco VIM Unified Management**
Without Internet	• Prepare the USB on a staging server • Plug the USB into the management node. • Follow the update procedure without Internet.	• Prepare the USB on a staging server • Plug the USB into the management node. • Follow the update procedure without Internet.
With Internet	• Download the .tgz file from the registry. • Follow the update steps with Internet.	• Download the .tgz file from the registry. • Follow the update steps with Internet procedure.

Updating Cisco VIM Using USB

Updating Cisco VIM Software Using USB

The following procedure describes how to load the Cisco VIM installation files onto a Cisco NFVI management node that does not have Internet access. Installation files include: *buildnode-K9.iso, buildnode-K9.qcow2, mercury-installer.tar.gz*, *ironic-images-K9.tar.gz, registry-2.6.2.tar.gz,* vim_upgrade_orchestrator.py and *all_check_sum_file.sign* file.

Before you begin

This procedure requires a CentOS 7 staging server (VM, laptop, or UCS server) with a 64 GB USB 2.0 drive. You can save the VIM installation files on a USB stick and then use the USB stick to load the installation files onto the management node. The installation files are around 24 GB in size. Downloading them to the USB drive might take several hours depending on the speed of your Internet connection. Before you begin, ensure that you disable the CentOS sleep mode

1. On the staging server, use yum to install the following packages:
   - PyYAML (yum install PyYAML)
   - python-requests (yum install python-requests
2. Connect to the Cisco VIM software download site using a web browser and login credentials provided by your account representative and download the getartifacts.py script from the external registry.

```
# download the new getartifacts.py file (see example below)
curl -o getartifacts.py -u '<username>:<password>'
https//cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/<3.4.3>/getartifacts.py
# Change the permission of getartificats.py
chmod +x getartifacts.py
```

3. Run the *getartifacts.py* script. The script formats the USB 2.0 drive and downloads the installation artifacts. Provide the registry username and password, the tag ID, and the USB partition on the staging server. For example:

   To identify the USB drive, execute the *lsblk* command before and after inserting the USB drive. The command displays a list of available block devices. The output delta helps to find the USB drive location. Provide the entire drive path in the –d option, instead of any partition.

```
sudo ./ getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc>
```

   Do not remove the USB drive during synchronization.

4. Verify the integrity of the downloaded artifacts and the container images:

```
# create a directory
sudo mkdir -p /mnt/Cisco
# /dev/sdc is the USB drive, same as supplied in get artifacts.py python script
sudo mount /dev/sdc1 /mnt/Cisco
cd /mnt/Cisco
# execute the verification script
./test-usb
# failures will be explicitly displayed on screen, sample success output below
# sample output of ./test-usb execution with 3.2.x release [root@mgmtnode Cisco]# /test-usb
INFO: Checking the integrity of this USB stick
INFO: Checking artifact buildnode-K9-13401.iso
INFO: Checking artifact registry-2.6.2-13401.tar.gz
INFO: Checking required layers:
INFO: 605 layer files passed checksum.
[root@mgmtnode Cisco]#
```

5. To resolve download artifact failures, unmount the USB and run the getartifacts command again with the *--retry* option:

```
sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> --retry
```

6. Mount the USB and then run the *test-usb* command to validate whether all the files are downloaded:

```
# /dev/sdc is the USB drive, same as supplied in get artifacts.py python script
sudo mount /dev/sda1 /mnt/Cisco
cd /mnt/Cisco
# execute the verification script
./test-usb
# In case of failures the out of the above command is explicitly displayed the same on the screen
```

7. After the synchronization is complete, unmount the USB drive:

```
sudo umount /mnt/Cisco
```

8. Remove the USB stick from the staging server and then insert it into the management node.
9. Complete the following steps to import the Cisco NFVI installation artifacts onto the management node:

    a. Identify the USB on the management node:

    ```
    blkid -L Cisco-VIM
    ```

    b. Mount the USB device on the management node:

    ```
    mount < /dev/sdc > /mnt/
    mkdir /root/cvim-update-media
    cd /root/cvim-update-media
    ```

    c. Extract the *import_artifacts.py* script:

    ```
    tar --no-same-owner -xvzf /mnt/Cisco/mercury-installer.tar.gz
    ```

    d. Unmount the USB device:

    ```
    umount /mnt/Cisco/
    ```

    e. Import the artifacts:

    ```
    cd /root/cvim-update-media/installer-<3.x.x>/tools/
    ./import_artifacts.sh
    ```

    f. Change directory and remove `/root/cvim-update-media`:

    ```
    ```

10. Execute the update from the old working directory:

```
cd $old_workspace/installer;
ciscovim update --file /var/cisco/artifacts/mercury-installer.tar.gz
```

After the update is complete, use only the newly created directory unless a rollback is planned.

11. Commit the update by running the following command:

```
ciscovim commit # from the new workspace
```

12. To revert the update changes before entering the *commit* command, use the following command:

```
ciscovim rollback # and then use older workspace
```

⚠ Do not run any other Cisco VIM actions when the update is in progress.

In Cisco VIM, if updates bring in Kernel changes, the reboot of the compute node with VNFs in ACTIVE state is postponed. This is done to mitigate the unpredictability of data plane outage when the compute nodes go for a reboot for the kernel changes to take effect, during the rolling upgrade process.

At the end of *ciscovim* update, the Cisco VIM orchestrator displays the following message on the console and logs:

```
Compute nodes require reboot Kernel updated
<compute_1_with_VM_running>
<compute_3_with_VM_running>
<compute_4_with_VM_running>
<compute_12_with_VM_running>
```

After the Kernel update on management node, reboot the compute node before proceeding. The logs for this run are available in:

```
<mgmt._ip_address>:/var/log/mercury/<UUID>
```

For Micropod, if the VM landed on the server has dual roles (control and compute), reboot the server and run ciscovim *cluster-recovery*

As the redundancy in controller and storage nodes are built into the product, the reboot of those nodes are automated during the software update.

The computes that does not have any VNFs in ACTIVE state are automatically rebooted during software update. To monitor and reboot the compute nodes through ciscovim cli, see the sections Managing Reboot of Cisco VIM Nodes and Managing Reboot Status of Cisco VIM Nodes.

No pod management operation is allowed until the reboot of all Cisco VIM nodes are successful.

Updating Cisco VIM Using Network Installation

Updating Cisco VIM Software Using Network Installation

1. From the download site that is provided by your Cisco account representative, download the *mercury-installer.gz*

   ```
   curl -o mercury-installer.tar.gz https://\{username}:{password}@cvim-registry.com/
   mercury-releases/cvim34-rhel7-osp13/releases/{release number}/ mercury-installer.tar.gz
   ```

   The link to the tar ball preceding is an example.
2. Execute the update from the old working directory:

   ⚠ Do not run any other Cisco VIM actions during an update.

   ```
   cd /root/installer-<tagid>
   ciscovim update --file /root/mercury-installer.tar.gz
   ```

   After the update is complete, use the newly created directory unless a rollback is planned.
3. Commit the update by running the following command:

   ```
   ciscovim commit
   ```

4. To revert the update changes before entering the commit command, enter:

   ```
   ciscovim rollback # and then use older workspace
   ```

   If the updates bring in Kernel changes, the reboot of the compute node with VNFs in ACTIVE state is postponed. This is done to mitigate the unpredictability of data plane outage when the compute nodes go for a reboot for the kernel changes to take effect, during the rolling upgrade process.
   At the end of *ciscovim* update, the Cisco VIM orchestrator displays the following message on the console and logs:

   ```
   Compute nodes require reboot Kernel updated
   <compute_1_with_VM_running>
   <compute_3_with_VM_running>
   <compute_4_with_VM_running>
   <compute_12_with_VM_running>
   ```

   After the Kernel update on the management node, reboot the compute node before proceeding further. The logs for this run are available in `<mgmt._ip_address>:/var/log/mercury/<UUID>`

   ⚠ The redundancy in controller and storage nodes are built into the product. The reboot of those nodes are automated during the software update.

   The computes that does not have any VNFs in ACTIVE state, are automatically rebooted during the software update. To monitor and reboot the compute nodes through ciscovim cli, see Managing Power and Reboot > *Managing Reboot of Cisco VIM Nodes* and *Managing Reboot Status of Cisco VIM Nodes*

   No pod management operation is allowed until the reboot of all Cisco VIM nodes is successful.

Upgrading Cisco VIM in Cloud

Upgrading Cisco VIM in Cloud

Types of Pod Upgrade

Type 1 Upgrade

Upgrade from Cisco VIM 2.4.x to Cisco VIM 3.4.3 (x=15, 16, 17 or 18) constitutes the following:

- Upgrade of RHEL from 7.4 to 7.6.
- Upgrade of OSP from 10.0 (Newton) to 13.0 (Queens).
- Upgrade of docker 1.10 (running thin-pool infrastructure) to 1.13 (overlay network).
- Upgrade of the REST API of the Cisco VIM installer.
- Ceph upgrade from Jewel to Luminous.

Type 2 Upgrade

Upgrade from Cisco VIM 3.2.x to Cisco VIM 3.4.3 (x=1, 2 or 3) constitutes the following:

- Upgrade within OSP 13.0 (OSP is updated as part of maintenance release)
- Upgrade within RHEL 7.6 (kernel is updated).
- Upgrade of the REST API of the Cisco VIM installer.

Based on the Cisco VIM image version, the administrator must refer to the appropriate upgrade section.

General Upgrade

Cisco VIM allows you to upgrade all OpenStack services, infrastructure services such as RabbitMQ, MariaDB, and HAProxy, and management node containers such as Cobbler, ELK, VMTP and repo containers. You can upgrade to new releases of OpenStack without redeploying the Cisco NFVI stack from the beginning. During upgrade, you can expect complete (Type 1 upgrade) to limited control plane (Type 2 upgrade) outage. As part of the upgrade, the REST API server managing the VIM orchestrator also gets upgraded using the script *vim_upgrade_orchestrator.py*. Hence, it is important to execute the upgrade as a foreground process in an environment like a VNC session.

Cisco VIM supports an upgrade from Cisco VIM 3.2.x to the current version of Cisco VIM.

As part of the Cisco VIM cloud upgrade:

- The upgrade script is used to automatically upgrade the REST API server that manages the VIM orchestrator.
- The setup_data.yaml file is automatically translated so that the setup_data.yaml file is compatible with the target release version.

For upgrade from Cisco VIM 2.4.x to Cisco VIM 3.4.3, take the backup of the management node post successful completion of the upgrade, reimage the management node with Cisco VIM 3.4.3 and restore the same.

For upgrade from Cisco VIM 3.2.x to Cisco VIM 3.4.3, power-cycle the management node post Cisco VIM upgrade to complete the upgrade process.

For upgrade from Cisco VIM 2.4.x, remove storage nodes or add storage nodes again so that ceph operates in bluestore mode rather than filestore mode. As the Ceph migration take a long time, plan for additional maintenance window post upgrade. Before initiating remove-storage, ensure that the CEPH health is HEALTH_OK.

Harmless traceback are seen in */var/log/messages* and */var/log/tuned/tuned.log* post Cisco VIM upgrade. Reboot of management node resolves the traceback. This traceback is not observed post restoration of the management node (from backup taken after successful upgrade).

The following table provides an overview of upgrade methods available to update OpenStack using Cisco VIM. The Internet options refer to management node connectivity to the Internet. If your management server lacks Internet access, you must have a staging server with Internet access to download the Cisco VIM installation artifacts to a USB drive. Ensure that you select one method and stay with it for the full pod lifecycle.

Upgrade Method	Without Cisco VIM Unified Management
Without Internet	• Prepare 1 USB 2.0 (64G) or 1 USB 3.0 (64G) on M4 or M5 staging server respectively and populate them with 3.4.3 artifacts. • Plug the USB into the management node. • Copy the vim_upgrade_orchestrator.py script and follow the steps given in the *Upgrade without Internet* procedure.
With Internet	Copy the vim_upgrade_orchestrator.py script and follow the steps given in the *Upgrade with Internet* procedure.

- The upgrade of VTS from 3.2.x to 3.4.3 is not supported.
- The upgrade from Cisco VIM 3.0.0 to Cisco VIM 3.4.3 is not supported.
- In case of upgrade failure, ensure that you do not try to recover the cloud by yourself. For help and recovery, contact Cisco Support.

Considerations

Before you begin an upgrade, consider the following:

1. For type 1 upgrade:
    a. Plan for cloud outage as it entails upgrade of docker infrastructure which is the foundation of Cisco VIM
    b. Ensure that your cloud is running with Keystone v3 prior to the upgrade.
    c. Post keystonev3 reconfiguration, all the custom or user created openrc files must be modified to use keystonev3. In addition, ESC/NSO must be reconfigured to use keystonev3 when connecting to OpenStack endpoint.
2. For type 2 upgrade, plan for control plane downtime as the upgrade involves changing the Kernel version.
3. Perform a cloud sanity check before initiating the upgrade, to prevent double faults.
4. Check CIMC logs for any hardware errors including disk errors.
5. No custom (non-CVIM) docker containers must be running on management node or control/compute/storage nodes.
6. If Cisco UCS is used, ensure that CIMC of all the servers is 2.0(13n) or greater.
7. Use the vim_upgrade_orchestrator.py script available as part of the 3.4.3 artifacts for upgrade. You have to save a copy of the upgrade script to the */root/ location* before upgrade.
8. For disconnected upgrade, the USB must be pre-populated with 3.4.3 artifacts.
9. Upgrade from either type to 3.4.3 is restricted to specific start and end points.
10. Upgrade of the cloud is supported in both connected and disconnected modes.
11. Upgrade of Unified Management on its standalone node is supported.
12. Cisco recommends you to not change the installation mode during upgrade.
13. No rollback option is available once upgrade is initiated. Hence, planning must be done before upgrade. If you face any issue after upgrade, reach out to Cisco TAC or BU to recover the cloud.
14. Post upgrade keystonev3 is the default authentication mechanism. The keystonev3 in OPTIONAL_SERVICES is not available in the system translated setup_data.yaml.
15. See Prerequisites and Assumptions for Cisco VIM update/upgrade and ensure that all conditions are met.
16. At a high level, the vim_upgrade_orchestrator.py script is broken into two logical steps to abort on failure. In case of failure, reach out to Cisco support for recovery. Cisco does not recommend you to recover the cloud on your own.

    The following are the two high level steps into which the vim_upgrade_orchestrator.py script is broken into:

    Pre-upgrade Check

    - Registry connectivity (if connected, installation is initiated).
    - Setup_data pre check: No UCSM_PLUGIN, sufficient storage pool size.
    - Backup the setup_data.yaml file, before translation.
    - Check and update INSTALL_MODE in the setup_data.yaml file (connected or disconnected).
    - Run cloud sanity on cloud from current workspace using ciscovim.
    - Check for reachability to all nodes including compute, controller, and storage.
    - Check if cloud is running with KeystoneV3. For clouds running with Cisco VIM 2.4.x, you must enable keystone v3 via a reconfigure before the upgrade. For information on how to enable keystone v3, see Cisco Virtualized Infrastructure Administrator Guide, 2.4.x.
    - No in-progress or failed operation exists in RestAPI database as part of pre-validation
    - If the setup is for Cisco VIM 2.2.x to 2.4.y to 3.4.x, the haproxy (self-signed) TLS certificate must be regenerated in 2.4.x workspace followed by ciscovim reconfigure.

    Upgrade to 3.4.3

    - Upgrade to 3.4.3 (in a VNC session). Based on the starting release, RHEL, OSP, and Docker are upgraded.
    - Backup the management node.
    - Run sanity test on cloud from 3.4.3.
    - Check for reachability to compute, controller, and storage nodes.

Upgrading Cisco VIM Using USB

Upgrading Cisco VIM Using USB

The following procedure describes how to load the Cisco VIM installation files onto a Cisco NFVI management node that does not have Internet access. Installation files include: *buildnode-K9.iso, buildnode-K9.qcow2, mercury-installer.tar.gz, ironic-images-K9.tar.gz, registry-2.6.2.tar.gz, vim_upgrade_orchestrator.py* and *all_check_sum_file.sign* file.

Before you begin

This procedure requires a CentOS 7 staging server (VM, laptop, or UCS server) with a 64 GB USB stick. You can download the VIM installation files using the staging server with Internet access (wired access is recommended), and save the files to a USB stick. You can use the USB stick to load the installation files onto the management node. The size of the installation files comes to around 24 GB, so downloading them to the USB stick might take several hours, depending on the speed of your Internet connection, so plan accordingly. Before you begin, disable the CentOS sleep mode.

1. On the staging server, use yum to install the following packages:
   - PyYAML (yum install PyYAML)
   - python-requests (yum install python-requests)
2. Connect to the Cisco VIM software download site using a web browser and login credentials provided by Cisco account representative and download the *getartifacts.py* script from the external registry.

```
# download the new getartifacts.py file (see example below)
curl -o getartifacts.py -u '<username>:<password>'
https//cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/3.4.3/getartifacts.py
# Change the permission of getartificats.py
chmod +x getartifacts.py
```

3. Run the *getartifacts.py* script. The script formats the USB 2.0 drive and downloads the installation artifacts. Provide the registry username and password, the tag ID, and the USB partition on the staging server.

   For example, to identify the USB stick, execute the *lsblk* command before and after inserting the USB stick. The command displays a list of available block devices. You can find the USB stick location from the delta output, and provide the entire drive path in the *–d* option instead of any partition.

```
sudo ./ getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc>
```

   Do not remove the USB stick during synchronization. Use *-U* option to download Ocata and Pike artifacts. This is applicable only for Cisco VIM 2.4.y to Cisco VIM 3.4.x upgrade.

4. Verify the integrity of the downloaded artifacts and container images.

```
# create a directory
sudo mkdir -p /mnt/Cisco
# /dev/sdc is the USB stick, same as supplied in get artifacts.py python script
sudo mount /dev/sdc1 /mnt/Cisco
cd /mnt/Cisco
# execute the verification script
./test-usb
# failures will be explicitly displayed on screen. A sample success output is shown
# sample output of ./test-usb execution with 3.4.3 release
[root@mgmtnode Cisco]# /test-usb
INFO: Checking the integrity of this USB stick
INFO: Checking artifact buildnode-K9-13401.iso
INFO: Checking artifact registry-2.6.2-13401.tar.gz
INFO: Checking required layers:
INFO: 605 layer files passed checksum.
[root@mgmtnode Cisco]#
```

5. To resolve download artifact failures, unmount the USB and run the getartifacts command again with the *--retry* option:

```
sudo ./getartifacts.py -t <tag_id> -u <username> -p <password> -d </dev/sdc> --retry
```

6. Mount the USB and run the *test-usb* command to validate if all the files are downloaded:

```
# /dev/sdc is the USB stick, same as supplied in get artifacts.py python script
sudo mount /dev/sda1 /mnt/Cisco
cd /mnt/Cisco
# execute the verification script
./test-usb
# In case of failures, the output of the above command will explicitly display the failure on the screen
```

7. After synchronization, unmount the USB stick.

```
sudo umount /mnt/Cisco
```

8. After synchronization, remove the USB stick from the staging server and insert the USB stick into the management node.
9. Insert the pre-populated USBs into the management node of the pod running 3.2.x/2.4.y (x<=4 or y =15, 16, 17 or 18).
10. Copy the *vim_upgrade_orchestrator.py* script available in Cisco VIM 3.4.3 artifacts in the `/root/` folder, to the management node of the pod running running 2.4.y/3.2.x (x<=4 or y =15, 16, 17 or 18).
11. Execute the update from the `/root/ location`:

```
# cd /root/
# chmod +x vim_upgrade_orchestrator.py
# ./vim_upgrade_orchestrator.py -i disconnected -s start_image_tag -n 3.4.3 [-y] # -y if you don't want
any interactive mode
# start_image_tag value can be: 2.4.y/3.2.x (x<=4, oy y=15,16,17, or 18)
```

After upgrade, start using the newly created directory.

> ⚠ Upgrade process takes several hours (> 6 hours), so execute this process in a VNC. If you do not have a VNC environment, execute the same from KVM console of the management node. Do not run this command in background or with nohup option as the upgrade will fail. Do not run any other Cisco VIM actions during upgrade.
>
> Ensure that REQUESTS_CA_BUNDLE is not set as an environment variable on the management node

12. Copy the management node backup created during the upgrade, and paste it into a separate server through rsync. For more information on backup, see Backup and Restore. For upgrade from Cisco VIM 2.4.y, re-image the management node with Cisco VIM 3.4.3 and then restore the management node with the backup snapshot taken as part of the upgrade. For more details, see Management Node on UCS C-series (M4/M5) or Management Node on Quanta Servers based on the type of management node that is used.
13. For pods getting upgraded from Cisco VIM 2.4.y, Ceph continues to run in filestore mode. Use separated tool *ceph_migration_status.py* provided in */installer-3.4.3/tools/* directory to figure out the mode of ceph used.

    a. Move each ceph node to bluestore mode by removing/adding storage nodes for fullon or hyper-converged pod. Before initiating each remove/add storage operation, ensure that Ceph is in HEALTH_OK state. For Micropod, you can achieve the same by replacing the controller.

    > ⚠ As ceph migration takes long time, it is recommended to take subsequent maintenance window for this activity.

    b. Ensure that CEPH is in HEALTH_OK before initiating each remove/add storage operation. Use the tool provided in the *installer-3.4.3 /tools/* directory to find out the ceph nodes that are pending for migration to bluestore. To execute the tool:

```
# cd /root/installer-3.4.3/tools/
# python ceph_migration_status.py
```

Upgrading Cisco VIM Using Network Installation

Upgrading Cisco VIM Using Network Installation

1. From the software download site provided by your Cisco account representative, download the`vim_upgrade_orchestrator.py curl -o vim_upgrade_orchestrator.py` file.

   For example:

   ```
   https://{username}:{password}@cvim-registry.com/mercury-releases/cvim34-rhel7-osp13/releases/{release number}/vim_upgrade_orchestrator.py
   ```

2. Execute the upgrade from the */root/* directory:

   ```
   $ cd /root/
   # chmod +x vim_upgrade_orchestrator.py
   #./vim_upgrade_orchestrator.py -i connected -s start_image_tag -n <3.4.3 or 3.4.4> [-y] # -y if no interactive mode is required.
   # start_image_tag value can be: 2.4.y/3.2.x (x<=4, oy y=15,16,17, or 18)
   ```


   - As the upgrade process takes more than 6 hours, execute this process in a VNC. If you do not have a VNC environment, execute the same from KVM console of the management node. Ensure that you do not run this command in background or with *nohup* option to avoid failure of upgrade. During the upgrade, do not run other Cisco VIM actions.
   - Ensure that REQUESTS_CA_BUNDLE is not set as an environment variable on the management node.

   After the upgrade, use the newly created directory to continue from step 12 listed in the section Upgrading Cisco VIM Using USB. Ensures built-in redundancy for controller and standalone storage nodes. The reboot of these nodes are automatic during the software upgrade from 3.x.
   The computes that does not have any VNFs in ACTIVE state are automatically rebooted during the software upgrade.

   - No pod management operation is allowed until the reboot of all Cisco VIM nodes is successful.
   - In case of upgrade failure, ensure that you do not try to recover the cloud by yourself. For help and recovery, contact Cisco Support.

   To monitor and reboot the compute nodes through *ciscovim* CLI, see the sections *Managing Reboot of Cisco VIM Nodes* and *Managing Reboot Status of Cisco VIM Nodes* under Managing Power and Reboot

BIOS/BMC/Firmware Update

Update of BIOS/BMC/Firmware

BIOS/BMC/Firmware Update Overview

Overview of BIOS/BMC/Firmware Update

To provide a seamless operation experience, tools to upgrade/update the BIOS/BMC/firmware for Cisco UCS C-series and Quanta servers are provided.

For Cisco UCS-C series, the tool uses the HUU image provided by Cisco to update the CIMC and firmware.

For Quanta, the support for automated BIOS/BMC/firmware upgrade is available.

Cisco UCS Firmware Upgrade

Cisco UCS Firmware Upgrade

In Cisco VIM 2.4.2, the Cisco Host Upgrade Utility (HUU) tool developed using Cisco Integrated Management Controller (IMC) Python SDK module (imcsdk-0.9.2.0) is leveraged automatically to upgrade all firmware components running on Cisco UCS C-Series servers.

> ⚠ The wrapper tool only updates the CIMC bundle packages, as the entire Cisco IMC Software bundle (that includes CIMC, BIOS, adapter and storage controller firmware images through HUU images) is updated by default. Adequate planning is required for CIMC upgrade, as it causes the server to get rebooted.

For Cisco VIM 2.4, the CIMC upgrade tool supports the:

- Upgrade of CIMC bundle images for C-series only.
- Concurrent upgrade of CIMC bundle images on multiple C-series servers.
- Pre-validation check for server type and available HUU images.
- Support of the external http server, Cisco VIM Software Hub, or Cisco VIM Management node for the target CIMC upgrade image mounts.
- Checks if the cloud is deployed successfully, and notifies the user with a proper message.
- Checks if selected hosts have any active VMs running on them and notifies the user with a proper message.
- Generation of consolidated summary on firmware version status, on completing the pre-upgrade and post-upgrade.

> ⚠
> - Firmware upgrade is supported only on UCS C-series platform and not on UCS B-series and HP platforms.
> - If you upgrade CIMC firmware on an existing cloud deployment, it might impact the cloud functionality as the firmware upgrade reboots the host. Hence, ensure that the cloud is operational, post CIMC firmware upgrade.

To check if the cloud is operational, execute the following steps:

- Run the cloud sanity.
- If cloud sanity failure occurs, run cluster recovery and then re-run cloud sanity.

Also for the upgrade operation to work, ensure that the image has the following syntax:

```
ucs-<server_type>huu<version_number>.iso; for example ucs-c220m4-huu-2.0.13n.iso or ucs-c240m4-huu-2.0.13n.iso;
```

> ⚠ Running the UCS Firmware upgrade on host(s) running active VMs results in downtime on those VMs.

Limitations

The following Cisco VIM management operations are not allowed when the firmware upgrade is in progress:

- POD management operations: Addition, removal or replacement of nodes.
- Cisco VIM software update.
- Cisco VIM software upgrade.
- Reconfiguration of Cisco VIM features.

Tools Usage

The CIMC upgrade utility is a standalone python file (ucsc_host_upgrade_utility) which is located under `<cvim_install_dir>/tools/` directory.

To use the tool, execute the following command:

```
[root@hiccup-mgmt-228 tools]# python ucsc_host_upgrade_utility.py -h
usage: ucsc_host_upgrade_utility.py [-h] [--file SETUPFILELOCATION]
                                    [--http-server HTTP_SERVER_IP]
                                    [--sds-server SDS_SERVER_NAME]
                                    [--server-uname UNAME]
                                    [--server-pwd PASSWD]
                                    [--huu-image-path HUU_IMAGE_PATH]
                                    [--host HOSTS] [--exclude-hosts E_HOSTS]
```

```
                                                                    [-y]
Script to perform firmware upgrade
optional arguments:
-h, --help                                  show this help message and exit
--file SETUPFILELOCATION, -f SETUPFILELOCATION
                                            Optional, if not defined will read the setup_data.yaml in /root
/openstack-configs dir for CIMC information of servers;
                                             To override, provide a valid YAML file with the CIMC
Credentials.
--http-server HTTP_SERVER_IP, -hs HTTP_SERVER_IP
                                            Optional, only needed if a http server is used to host the
target CIMC bundle image(s).
--sds-server SDS_SERVER_NAME, -sds SDS_SERVER_NAME
                                            Optional, only needed if a Software Distribution Server (SDS)
is used to host the target CIMC bundle image(s).
--server-uname UNAME, -u UNAME
                                            Optional, only needed if a http server is used to host the
target CIMC bundle image(s).
--server-pwd PASSWD, -p PASSWD
                                            Optional, only needed if a http server is used to host the
target CIMC bundle image(s).
--huu-image-path HUU_IMAGE_PATH, -path HUU_IMAGE_PATH
                                            Comma separated absolute path of the HUU ISO file(s);
                                            In the case of a web server hosting the files, provide the
absolute path of the URL that includes the file names; that is, exclude
                                            the scheme://host/ part

--host HOSTS            Comma separated list of host names targeted for CIMC bundle upgrade defined in the
target setup_data.yaml
--exclude-hosts E_HOSTS, -e E_HOSTS
                                            Comma separated list of hostnames excluded for CIMC bundle
upgrade defined in the target setup_data.yaml
-y, -yes
[root@hiccup-mgmt-228 tools]#
```

If the target CIMC upgrade images are available on Cisco VIM Management node, use the below command:

```
python ucsc_host_upgrade_utility.py [--file <setup_data_test.yaml/cimc_servers.yaml>] -path <huu_image_paths>
```

If the target CIMC upgrade images are hosted in an external http server that is reachable from the Cisco VIM Management node and CIMC of the servers, use the below command:

```
python ucsc_host_upgrade_utility.py [--file <setup_data_test.yaml/cimc_servers.yaml>]
-hs <http_server_ip/hostname> -u
<https_server_un> -path <http_server_pwd> -path <huu_image_paths>
```

If the target CIMC upgrade images are hosted in Ciso VIM Software Hub, use the below command:

```
python ucsc_host_upgrade_utility.py --file [setup_data_test.yaml/cimc_servers.yaml] -sds
[Ciso VIM Software Hub_server_ip/hostname] -u
[sds_server_un] -path [sds_server_pwd] -path [huu_image_paths]
```


Prerequisites to use Ciso VIM Software Hub for hosting the target CIMC bundle image(s) are:

- Ciso VIM Software Hub server must be reachable from the management node over HTTPS.
- Ciso VIM Software Hub server TLS certificate must be trusted by the management node to make TLS connection in verified context

If setup_data.yaml file is not available, you can create it using the below command:

```
# UCSC (C-series) sample format of yaml file to specify the CIMC details
SERVERS:
server-1:
cimc_info:
cimc_ip: "cimc-ip-address"
```

```
cimc_username: "cimc-user-name"
cimc_password: "cimc-password"
server-2:
cimc_info:
cimc_ip: "cimc-ip-address"
cimc_username: "cimc-user-name"
cimc_password: "cimc-password"
server-3:
cimc_info:
cimc_ip: "cimc-ip-address"
cimc_username: "cimc-user-name"
cimc_password: "cimc-password"
```


As the upgrade of CIMC takes more than an hour, execute this process in a VNC. If you do not have a VNC environment, execute the same from KVM console of the management node. Do not run this command in background or with nohup option.

Quanta Firmware Upgrade

Quanta Firmware Upgrade

From release Cisco VIM 3.2.1, the Quanta firmware upgrade utility tool upgrades the BMC, BIOS, and NVM firmware versions on Quanta servers.

> ⚠ The wrapper tool only updates the BMC, BIOS and NVM versions based on the provided firmware packages. Adequate planning is required for Quanta firmware upgrade, as it causes the server to get rebooted.

For Cisco VIM 3.2.1, the Quanta firmware upgrade tool supports:

- Upgrade of BMC, BIOS and NVM for Quanta servers only.
- Concurrent upgrade of firmware on multiple Quanta servers.
- Pre-validation if another firmware flashing is in progress.
- Generation of consolidated summary on firmware version status, on completing the pre-upgrade and post-upgrade.

> ⚠ If you upgrade Quanta firmware on an existing cloud deployment, it might impact the cloud functionality as the firmware upgrade reboots the host. Hence, ensure that the cloud is operational, post Quanta firmware upgrade.

To check if the cloud is operational, do the following:

1. Run the cloud sanity.
2. If cloud sanity fails, run cluster recovery and then re-run the cloud sanity.

For the upgrade to work, ensure that you specify the proper firmware-package bundle with proper name and version of the components (BMC/BIOS/NVM). Few examples given below:

- BIOS firmware package file name must start with a prefix BIOS_XXXX.zip.
- BMC firmware package file name must start with a prefix BMC_XXX.zip.
- NVM firmware package file name must contain NVMXXXXX.zip.

> ⚠ Running the BMC/BIOS/NVM firmware upgrade on host(s) running active VM results in downtime on those VMs.

Limitations

The following Cisco VIM management operations are not allowed when the firmware upgrade is in progress:

- Pod management operations: Addition, removal or replacement of nodes.
- Cisco VIM software update.
- Cisco VIM software upgrade.
- Reconfiguration of Cisco VIM features.

Tools Usage

The Quanta upgrade utility is a standalone python file `quanta_firmware_upgrade.py` which is located under `<cvim_install_dir>/tools/` directory.

To use the tool, execute the following command:

```
[root@mgmt-node tools]# ./quanta_firmware_upgrade.py -h
usage: quanta_firmware_upgrade.py [-h] [--hosts HOSTS]
                                  [--exclude-hosts EXCLUDE_HOSTS]
                                  [--ignore-flash-status] [--no-preserve] [-v]
                                  [-y] [--bmc-only | --bios-only | --nvm-only]
                                  --setupfile SETUPFILE --firmware-package
                                  FIRMWARE_PACKAGE

Script to update BMC and BIOS firmware on Quanta server

optional arguments:
  -h, --help            show this help message and exit
  --hosts HOSTS         comma separated list of servers defined in
                        setup_data.yaml file target for firmware update
```

```
  --exclude-hosts EXCLUDE_HOSTS
                        comma separated list of servers defined in
                        setup_data.yaml file to exclude for firmware update
  --ignore-flash-status
                        ignore flash status, needed for older BMC firmware
                        where it lacks the support and continue with BMC/BIOS
                        firmware update
  --no-preserve         do not preserve BMC or BIOS setting during firmware
                        update
  -v, --verbose         enable verbose output
  -y, --yes             skip prompt
  --bmc-only            update BMC firmware only
  --bios-only           update BIOS firmware only
  --nvm-only            update Intel Ethernet NVM only

required arguments:
  --setupfile SETUPFILE
                        setup_data.yaml file location
  --firmware-package FIRMWARE_PACKAGE
                        Firmware package ZIP file location
```

For upgrade BMC only, use the below command:

```
./quanta_firmware_upgrade.py --setupfile <setup-data.yaml> --firmware-package <bmc/bios_update_package.zip> --
bmc-only
```

For upgrade BIOS only, use the below command:

```
./quanta_firmware_upgrade.py --setupfile <setup-data.yaml> --firmware-package <bmc/bios_update_package.zip> --
bios-only
```

For upgrade NVM only, use the below command:

```
./quanta_firmware_upgrade.py --setupfile <setup-data.yaml> --firmware-package <nvm_update_package.zip> --nvm-
only
```


- If you do not specify any option for particular component with specified BIOS/BMC firmware package, the utility upgrades in the order of BMC followed by BIOS but not NVM.
- If you are planning to update both the BMC and the BIOS separately, always update the BMC first and then the BIOS.
- To upgrade NVM, you need to specify --nvm-only option with NVM firmware package, otherwise upgrade fails.
- NVM firmware upgrade does not reboot the servers by default. You need to reboot the nodes manually to complete the upgrade process.

As some of the servers running old firmware are upgrading to latest firmware, password might be reset to default.
You need to manually reset the password by following the below steps:

1. Login to the UI using the factory default **admin** and **cmb9.admin**
2. Once logged-in, you are prompted with a message **First Login or Password Expired. You need to change your password**.

You need `--ignore-flash-status` option for older BMC firmware as it lacks support, and continue with BMC firmware update.
Example:

```
./quanta_firmware_upgrade.py --setupfile <setup-data.yaml> --firmware-package <bmc_update_package.zip> --bmc-
only --ignore-flash-status
```


As the upgrade of BIOS/BMC takes more than 30 minutes, it is imperative to execute this process in a VNC. If you do not have a VNC environment, execute the same from KVM console of the management node. Do not run this command in background or with nohup option.

Intel FPGA PAC N3000 Firmware Update Support

Intel FPGA Programmable Acceleration Card (PAC) N3000 Firmware Update Support

Overview

Intel FPGA PAC N3000 firmware update script updates all the accelerated compute nodes installed with Intel N3000 card.

The tool checks and performs the following:

- Upgrade from version 1.0 non-secure mode to 1.1 secure mode support.
- Program the unsigned user image into FPGA's user flash region.
- Update the onboard XL710 chips to user provided firmware.

Two ways to update the firmware are:

- Fresh installation of Cisco VIM 3.4.3.
- Manual update using the script packaged in Cisco VIM's tools directory.

Method 1: Fresh installation of Cisco VIM 3.4.3

1. Add the following configuration to *setup_data.yaml* configuration file before pod deployment:

```
setup_data.yaml
===============
<..snip..>
# Optional section, Intel FPGA N3000 firmware version control configuration:
# Specify particular unsigned user image to flash N3000's FPGA and/or update
# N3000's XL710 firmware during install process. As part of unsigned user
# image flashing process, N3000 card will also be upgrade to version 1.1 to
# support secure mode.
# Can specify 1) just "user_image_bitstream_id" and "user_image_file" or
#             2) just "xl710_config_file" and "xl710_image_file" or
#             3) both 1 and 2 options
#
# IMPORTANT: User will have to supply the firmware files and have it placed in
# /root/openstack-configs/ directory.
INTEL_N3000_FIRMWARE:
  user_image_bitstream_id: '<user image bitstream id, starting with 0x>'
  user_image_file: <unsigned user image file; filename only, no path>
  xl710_config_file: <XL710 nvmupdate config file; filename only, no path>
  xl710_image_file: <XL710 nvamupdate image file; filename only, no path>
<..snip..>
```

2. Copy the unsigned user image obtained from the vendor to */root/openstack-configs/* directory.
3. Copy the XL710 configuration and image files to */root/openstack-configs/* directory.
4. Perform pod deployment and update the Intel N3000 firmware during installation.

> ⚠ To complete an update, an additional time of two hours is taken.

Method 2: Using Script packaged in Cisco VIM's tools directory

1. Create an one-time user configuration file containing information about the firmware update:

```
config_file.yaml
================
# Can specify 1) just "user_image_bitstream_id" and "user_image_file" or
#             2) just "xl710_config_file" and "xl710_image_file" or
#             3) both 1 and 2 options
#
# IMPORTANT: You must supply the firmware files and have it placed in
# /root/openstack-configs/ directory.
INTEL_N3000_FIRMWARE:
  user_image_bitstream_id: '<user image bitstream id, starting with 0x>'
  user_image_file: <unsigned user image file; filename only, no path>
  xl710_config_file: <XL710 nvmupdate config file; filename only, no path>
  xl710_image_file: <XL710 nvamupdate image file; filename only, no path>
```

2. Copy the XL710 configuration and image files to */root/openstack-configs/* directory
3. On the already deployed pod, run following script in the Cisco VIM installer's tools directory:

```
cd /root/installer-3.4.3/tools
./intel-fpga-n3000-firmware-update.py -c /root/config_file.yaml
```


Depending on the number of cards and firmwares to flash, it may take up to two hours to complete.

Script Usage

```
[root@mgmt-node tools]# ./intel-fpga-n3000-firmware-update.py -h
usage: intel-fpga-n3000-firmware-update.py [-h] [-c CONFIG_FILE]
                                           [--check-only] [--hosts HOSTS] [-y]
                                           [-v]

Script to update Intel FPGA N3000 firmware on all Compute node

optional arguments:
  -h, --help            show this help message and exit
  -c CONFIG_FILE, --config-file CONFIG_FILE
                        one-time use config file containing just
  INTEL_N3000_FIRMWARE  section relevant to Intel FPGA
                        N3000 firmware update, please refer to
                        setup_data.yaml.C_Series_EXAMPLE for more info
  --check-only          perform firmware version check only
  --hosts HOSTS         comma separated list of Compute node defined in
                        setup_data.yaml file target for Intel FPGA N3000
                        firmware update
  -y, --yes             assumed yes, skip prompt
  -v, --verbose enable  verbose output
```

Sample Configuration

Configuration for User-provided Image and XL710

```
INTEL_N3000_FIRMWARE:
  user_image_bitstream_id: '0x2392920A010501'
  user_image_file: phase1_turbo4g_2x1x25g_1fvl_raw_20ww02_unsigned.bin
  xl710_config_file: nvmupdate_25G_0D58.cfg
  xl710_image_file: PSG_XL710_7p00_CFGID2p61_XLAUI_DID_0D58_K32246_800052B0.bin
```

Configuration for Image Files

```
[root@mgmt-node ~]# ls -l /root/openstack-configs/* | grep -E "\.bin|\.cfg"
-rw-r--r--. 1 root root      435 Feb 27 18:53 /root/openstack-configs/nvmupdate_25G_0D58.cfg
-rw-r--r--. 1 root root 45089792 Feb 20 12:20 /root/openstack-configs
/phase1_turbo4g_2x1x25g_1fvl_raw_20ww02_unsigned.bin
-rw-r--r--. 1 root root  4194304 Feb 27 18:54 /root/openstack-configs
/PSG_XL710_7p00_CFGID2p61_XLAUI_DID_0D58_K32246_800052B0.bin
```

Sample Output

```
[root@mgmt-node tools]# ./intel-fpga-n3000-firmware-update.py -c /root/phase1_firmware.yaml --hosts quincy-
compute-1,quincy-compute-2


Starting Intel FPGA N3000 update script
Full log can be found at /var/log/mercury/n3000_firmware_update-20200228151100673979.log
Checking Intel FPGA N3000 firmware on accelerated Compute node(s)
+------------------+---------------+---------------------+------------------+
|      Server      |   Management  | Accelerated Compute | Update Available |
+------------------+---------------+---------------------+------------------+
| quincy-compute-1 | 10.11.216.101 |         Yes         |        Yes       |
| quincy-compute-2 | 10.11.216.102 |         Yes         |        Yes       |
+------------------+---------------+---------------------+------------------+
Following accelerated Compute node(s) will be impacted as part of firmware update:

quincy-compute-1,quincy-compute-2


Any Nova, Neutron, and Telegraf services running on accelerated Compute node(s) will be stopped!!!
At the end of firmware update, accelerated Compute node(s) will be power cycle!!!
Would you like to continue? <y|n> y


Starting Intel FPGA N3000 firmware update process, this may take up to 2+ hours!!!
Successfully executed Intel FPGA N3000 firmware update script
```

Configuration

Configuration

Setup Configuration File

Setup Configuration File

To make the Cisco VIM installation simple, repeatable, and predictable for the end user, the *setup_data,yaml* is used to drive the cloud configuration. Depending on its nature, some of the parameters must be set on Day 0, while others can be set and enabled in the cloud via a reconfigure option. You can install and configure the Cisco VIM deployment using the *setup_data.yaml.*

If you are installing Cisco Insight, see Unified Management

Ensure that you take extreme care while creating the configuration file, as certain changes (for example, network, API) in the configuration after deployment, causes a stack redeployment with the exception (example: NFVIMON, of adding and removing nodes and so on).

> ⚠ Any change done to the pod networking layout plan configured in *setup_data.yaml* requires the pod to be reinstalled.

If your configuration is correct, the installation is done smoothly.

Recommendations

- Use a YAML editor on Linux (PyCharm, Komodo or vi/vim with YAML plugin) to edit this file. Do not copy the examples shown below into your YAML file, as your browser might render the characters differently.
- Generate the file in a Linux environment.

If you are using the Cisco VIM installer, you cannot update the OpenStack configuration files (for example, ml2_conf.ini, and other files) directly. All OpenStack configurations must be available in the *setup_data.yaml* file. This ensures that the installer with a view of the OpenStack deployment can reliably perform pod management, software updates, and upgrades. This ensures a consistent and repeatable installation.

ToR Management

ToR Management

Overview

For the servers to participate in the cloud, they must be connected to ToRs. Cisco VIM is agnostic to the ToR type, as long as you configure the right VLANs (OpenStack control, data plane) on the relevant ports of the ToR. Also, there exists a Layer 2 domain for the servers to PxE boot. However, if you choose to have Nexus as the ToR with or without ACI as the fabric, they can take advantage of auto-configuration of the ToRs. Also, if the ACI plugin or NCS is used as ToR, then this feature is mandatory.

Auto-configuration

Cisco VIM provides complete automation of the cloud deployment. It automates Day 0 configuration of N9xxx series Top of Rack (ToR) switches. This feature is optional and applicable to the pods running with or without ACI with N9K as ToR. The auto-ToR feature simplifies the deployment, but has restrictions on the configuration of the switch ports connected to the servers. Also, L3-out and spine level configurations are outside the scope of Cisco VIM's automation. For ToR switch details related to ACI, see Enabling ACI.

Cisco VIM automates post Power-On Auto Provisioning (post-POAP) configuration on ToR with one or more pairs of identical Cisco N9K series switches. The Day 0 ToR automation configures the interfaces that are connected to the management (br_mgmt), control, compute, and storage nodes of the pod. In addition, it configures the VPC peer link interfaces for ToR pairs. The automation handles both B and C-series pods. The automation includes configuration of the edge ports in the leaf switches off which the hosts hang-out and the VPC peer link between the switches.
The auto-configuration feature does not include the configuration of the spine switches and the connectivity between the leaf and the spine or the upstream link of the spine switches that carry the external VLAN connectivity.

As the feature is a post-POAP automation provisioning, ensure that the management interface, vrf, and admin user are pre-provisioned on each ToR switch. Also, you must enable SSH to each ToR from the management node.

The recommended N9K switch software versions are 7.0(3)I4(6), 7.0(3)I6(1), and 9.3(2)

Bootstrapping the ToR image is still a manual process. Ensure that the installer API interface (br_api) is up and running on the management node with SSH enabled. You can access each ToR through its management interface from the Cisco VIM management node using SSH.

Configuration Setup for B-series or C-series with N9K as ToR

The automated ToR configuration details are provided in two parts in the mercury *setup_data.yaml* file. The common information is available in the TORSWITCHINFO section, whereas the information on individual switch ports connected to specific nodes is available under SERVERS section for C-series and UCSM-COMMON section for B-series.

If the TORSWITCHINFO section is not provided or CONFIGURE_TORS attribute under TORSWITCHINFO is set to False or not provided, all the ToR provisioning related steps are skipped. The ToR section contains the attributes related to ToR connection, configuration for the management node interface, and vPC peer details in case of ToR pairs.

The port-channel number for the vPC peer link interfaces is derived from the vpc domain. The ToRs are paired with each other based on their corresponding vpc_peer_link addresses.

```
TORSWITCHINFO:
 CONFIGURE_TORS: True
 SWITCHDETAILS:
 -
   hostname: K09-n9k-a # mandatory
   username: admin # mandatory
   password: <ssh password> # mandatory
```

```
   ssh_ip: <a.b.c.d> # mandatory
   ssn_num: <xyz>. # optional, output of show license host-id
   vpc_peer_keepalive: <f.g.h.i> # peer switch ssh ip
   vpc_domain: <int>
   vpc_peer_port_info: <'eth1/45,eth1/46,eth1/47'>
   vpc_peer_vlan_info: <'NNNN,NNNN-NNNN'> # optional
   br_mgmt_port_info: 'eth1/19'. # only in 1 switch pair
   br_mgmt_po_info: <'NN'> # only in 1 switch pair
 -
   hostname: K09-n9k-a # mandatory
   username: admin # mandatory
   password: <ssh password> # mandatory
   ssh_ip: <a.b.c.d> # mandatory
   ssn_num: <xyz>. # optional, output of show license host-id
   vpc_peer_keepalive: <f.g.h.i> # peer switch ssh ip
   vpc_domain: <int>
   vpc_peer_port_info: <'eth1/45,eth1/46,eth1/47'>
   vpc_peer_vlan_info: <'NNNN,NNNN-NNNN'> # optional
   br_mgmt_port_info: 'eth1/19'. # only in 1 switch pair
   br_mgmt_po_info: <'NN'> # only in 1 switch pair
```


- Attributes for vpc peer vlan info and vpc domain have to match across each ToR pair.
- Attributes br_mgmt_po_info and br_mgmt_port_info have to match across ToR pairs. However, they must be defined only in ToR pairs where the management node is hanging off.
- Attribute for vpc_peer_vlan_info is optional.If it is not specified, it derives a list of VLAN ids from the host or FI facing interfaces and br_mgmt interface.
- Attribute for ssn_num which represents the chassis serial number is optional.

You can obtain the chassis serial number by executing the following command on each of the ToRs:

```
show license host-id
```

In the case of B-series, Cisco VIM configures the UCSMCOMMON section to declare the interface configuration under *tor_info_fi* and *tor_info_fi_redundant* for the FI (fabric inter-connect).

ToR names need to match with names provided in the TORSWITCHINFO section.

```
UCSMCOMMON:
 ucsm_ip: <p.q.r.s>,
 ucsm_password: <redacted>,
 ucsm_resource_prefix: <str>,
 ucsm_username: admin,
 tor_info_fi: {po: <int>, K09-n9k-a: eth1/<int>, K09-n9k-b: eth1/<int>},
 tor_info_fi_redundant: {po: <int>, K09-n9k-a: eth1/<int>, K09-n9k-b: eth1/<int>}
```

In the above example of B-Series, *tor_info* is not declared in the SERVERS section as all the server (controller, compute, and storage) connectivity is through the FI declared in the UCSCOMMON section. The VLANs for the FI facing interfaces are derived from the NETWORK segment ROLES for the controller, compute, and storage nodes.

Server-level setup-data Information for C-series

For C-series based pod, the switch port interface mapping for each of the controller, compute, and storage nodes are defined in the SERVERS > tor_info section. Cisco VIM driven cloud has a notion control (samx) and data (pet). Information present under tor_info always reflects the switch ports participating in OpenStack control (samx) pet. For deployments where the control and data plane are collapsed (for example, pods running on Cisco VIC), the tor_info represents the switch ports that participate in both the roles.

```
SERVERS:
 controller-1:
   rack_info: {rack_id: rack43X} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: <int>, B9-TOR-9K-1: eth1/<int>, B9-TOR-9K-2: eth1/<int>}
 controller-2:
   rack_info: {rack_id: rack43Y} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: 7, B9-TOR-9K-1: eth1/7, B9-TOR-9K-2: eth1/7}
```

```
 controller-3:
   rack_info: {rack_id: rack43Z} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: 9, B9-TOR-9K-1: eth1/9, B9-TOR-9K-2: eth1/9}
 compute-1:
   rack_info: {rack_id: rack43} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: 11, B9-TOR-9K-1: eth1/11, B9-TOR-9K-2: eth1/11}
 compute-2:
   rack_info: {rack_id: rack43} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: 13, B9-TOR-9K-1: eth1/13, B9-TOR-9K-2: eth1/13}
 storage-1:
   rack_info: {rack_id: rack43} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: 14, B9-TOR-9K-1: eth1/14, B9-TOR-9K-2: eth1/14}
 storage-2:
   rack_info: {rack_id: rack43} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: 15, B9-TOR-9K-1: eth1/15, B9-TOR-9K-2: eth1/15}
 storage-3:
   rack_info: {rack_id: rack43} cimc_info: {cimc_ip: <ip_addr>}
   tor_info: {po: 16, B9-TOR-9K-1: eth1/16, B9-TOR-9K-2: eth1/16}
```

VLANs for host facing interfaces are derived from NETWORK section, based on the server ROLES definition of each server and their corresponding network profile roles assigned for each segment.

Server-level setup_data Information for C-series with Intel NIC

When you configure a C-series pod to run in a complete Intel NIC environment, the OpenStack control (samx) and data (pet) plane are on different switch ports. As a result, an additional section called *dp_tor_info* is introduced to reflect the switch relevant port to server mapping, that is, control plane and data plane traffic are broken out into two separate interfaces with relevant VLANs (control plane VLANs for tor_info and data plane VLAN for dp_tor_info) applied on each of the interfaces facing the controller and compute nodes.

```
c43b-control-1:
 rack_info: {rack_id: rack43}
 cimc_info: {cimc_ip: <ip_addr>}
 tor_info: {po: 9, K09-n9k-a: 'eth1/9, eth1/12'}
 dp_tor_info: {po: 12, K09-n9k-a: 'eth1/12, eth1/12'}
c43b-compute-1:
 rack_info: {rack_id: rack43} cimc_info: {cimc_ip: <ip_addr>}
 tor_info: {po: 10, K09-n9k-a: 'eth1/10, eth1/13'}
 dp_tor_info: {po: 13, K09-n9k-a: 'eth1/13, eth1/13'}
```

Server-level setup_data Information for C-series with Intel NIC using SRIOV

When you configure a C-series pod to support SRIOV with Intel NIC, a third construct is introduced to allow SRIOV traffic onto the compute nodes. Switch ports configured for SRIOV are not placed in a port-channel. VLAN applied to the SRIOV interface is limited to that of the provider VLANs that are defined under the PROVIDER_VLAN_RANGES in the *setup_data.yaml* file.

```
c43b-compute-1:
 rack_info: {rack_id: rack43}
 cimc_info: {cimc_ip: <ip_addr>}
 tor_info: {po: 10, K09-n9k-a: 'eth1/10, eth1/13'}
 dp_tor_info: {po: 13, K09-n9k-a: 'eth1/13, eth1/13'}
 sriov_tor_info: { K09-n9k-a: eth1/33, K09-n9k-b: eth1/33}
```


For a dedicated storage node, only tor_info is applicable. In case of micro or hyper-converged pod, it is the controllers and computes that define the storage node switch mapping, respectively.

Custom N9K Configuration Support

Custom configuration is an optional procedure. The *setup_data.yaml* file contains an optional CUSTOM_CONFIG section to support custom configuration. Under the CUSTOM_CONFIG section, you can add raw CLI commands at the global, port-channel, and switch port level. CUSTOM_CONFIG is applied at the time of bootstrapping and add-interface workflow steps. You must provide the right switch configuration as the orchestration blindly applies it to the switch.

A sample snippet of the *setup_data.yaml* file with custom configuration is given below:

```
TORSWITCHINFO:
CONFIGURE_TORS: true CUSTOM_CONFIG:

GLOBAL:

[<'cli line 1'>,

<'cli
line 2'>,] PORTCHANNEL:

[<'cli
line 1'>] SWITCHPORT:

[<'cli
line 1'>,

<'cli line 2'>,]
```

ToR Configuration for NCS-5500

The following caveats apply to a Cisco VIM deployment with NCS as ToR:

- BGP: For a fresh installation of Cisco VIM, assure no BGP configuration is present on the NCS, otherwise the peering between the two NCS does not come up properly. Remove the existing BGP configuration if any. If additional BGP complementary configuration is needed, add it after a successful Cisco VIM installation.
- Segment-Routing: The global block of segment routing IDs must be pre-defined by the admin. Ensure that the prefix defined within the *setup_data.yaml* is within the segment routing global block range.
- NCS Interface Naming: A set of interface naming variations exist, but supports only the following: [Te0/0/0/0, TenGigE0/0/0/0, Gi0/0/0/0, Hu0/0/1/0, HundredGigE 0/0/1/0, FortyGigE0/0/0/0].
- Any manual adjustments to the ISIS or L2VPN sections (on top of the configuration provided by the Cisco VIM automation) causes subsequent Cisco VIM installation to fail.
- As only a pair of NCS-5500 is supported, ensure that you choose the right NCS model.
- With NCS as ToR, only Cisco C-series servers on Intel NIC are supported.

For a Cisco VIM running with NCS-5500, auto-ToR is a must.

The Cisco VIM *setup_data.yaml* configuration file is used as an input file to drive the configuration of NCS-5500.

The *setup_data.yaml* file contains the following three sections:

Section	Description
TORSWITCHINFO	This section provides general information.
SERVERS	(For C-series) This section provides information on the switch ports that are connected to the specific nodes. When the Micropod is configured to run in a complete Intel NIC environment with NCS-5500 as the ToR, the SERVER level configurations include *tor_info* (for control plane) and *dp_tor_info* (data plane) sections. Control plane and data plane traffic are broken out into two separate interfaces with bridge domains applied on each of the control and data interfaces facing each for the controller and compute nodes. *sriov_tor_info* is defined for computes participating in SRIOV.
MULTI_SEGMENT_ROUTING_INFO	This section provides information related to routing.

NCS-5500 supports a Micropod with additional computes running on Intel 710 NICs with no SR-IOV having VPP mechanism driver.

Cisco VIM supports maximum of two NCS-5500 within a single pod.

The following snippet shows an example of the mercury *setup_data.yaml* configuration file for NCS-5500:

```
TORSWITCHINFO:


  CONFIGURE_TORS: true # Mandatory
```

```
  TOR_TYPE: NCS-5500   #Mandatory

  SWITCHDETAILS:

  -
   hostname: <NCS-5500-1>   # hostname of NCS-5500-1
   username: admin
   password: <ssh_password of NCS-5500-1>
   ssh_ip: <ssh_ip_address of NCS-5500-1>
   vpc_peer_keepalive: <ssh IP address of the peer NCS-5500-2>
   br_mgmt_port_info: <interface of which br_mgmt of management node is hanging of NCS-5500-1>
   br_mgmt_po_info: <int; bundle Ethernet interface to pxe the management node>
   vpc_peer_port_info: <local interface to which peer NCS-5500 is connected, "," separated, max of 2 entries>' >
   vpc_peer_port_address: <local address with mask for vpc_peer_port_info, "," separated, max of 2 entries>'
can have a mask of /31>
   isis_loopback_addr: <local isis loopback interface address without mask> # assumes /32
   isis_net_entity_title: <isis network_entity_title>
   isis_prefix_sid: <int between 16000-1048575> # has to be unique in the ISIS domain and depends on the global
segment routing block define by the
admin

  -
   hostname: <NCS-5500-2> # hostname of NCS-5500-2
   username: admin
   password: <ssh_password of NCS-5500-2>
   ssh_ip: <ssh_ip_address of NCS-5500-2>
   vpc_peer_keepalive: <ssh IP address of the peer NCS-5500-1>
   br_mgmt_port_info: <interface of which br_mgmt of management node is hanging of NCS-5500-2>
   br_mgmt_po_info: <int; bundle Ethernet interface to pxe the management node>
   vpc_peer_port_info: <local interface to which peer NCS-5500 is connected>,"," separated, max of two entries
   vpc_peer_port_address: <local address with mask for vpc_peer_port_info>,"," separated, max of two entries
  isis_loopback_addr: <local isis loopback interface address without mask> # assumes /32
  isis_net_entity_title: <isis network_entity_title>
  isis_prefix_sid: <int between 16000-1048575> Must be unique in ISIS domain and depends on the global segment
routing block defined by the admin. Not allowed when ESI_PREFIX is defined

  splitter_opt_4_10: 'FortyGigE<C/D/X/Y>,HundredGigE<E/F/A/B>' # Optional for NCS-5500, only when splitter is
needed on per switch basis (that is, the peer switch may or maynot have theentry)

SERVER SECTION FOR C SERIES:

SERVERS:
  a27-fretta-micro-1:
    cimc_info: {cimc_ip: 172.28.121.172}
    dp_tor_info: {NCS-5500-1: TenGigE0/0/0/1, NCS-5500-2: TenGigE0/0/0/1, po: 1}
    hardware_info: {VIC_slot: MLOM}
    rack_info:{rack_id: RackA}
    tor_info: {NCS-5500-1: TenGigE0/0/0/0, NCS-5500-2: TenGigE0/0/0/0, po: 2} # Optional
    sriov_tor_info: {NCS-5500-1: TenGigE0/0/0/6, NCS-5500-2: TenGigE0/0/0/6} or
    sriov_tor_info: {NCS-5500-1: 'TenGigE0/0/0/6, TenGigE0/0/0/7', NCS-5500-2: 'TenGigE0/0/0/6,TenGigE0/0/0/7'}


  a27-fretta-micro-2:
    cimc_info: {cimc_ip: 172.28.121.174}
    dp_tor_info: {NCS-5500-1: TenGigE0/0/0/3, NCS-5500-2: TenGigE0/0/0/3, po: 3}
    hardware_info: {VIC_slot: MLOM}
    rack_info: {rack_id: RackB}
    tor_info: {NCS-5500-1: TenGigE0/0/0/2, NCS-5500-2: TenGigE0/0/0/2, po: 4}

 a27-fretta-micro-3:
   cimc_info: {cimc_ip: 172.28.121.175}
   dp_tor_info: {NCS-5500-1:TenGigE0/0/0/5, NCS-5500-2: TenGigE0/0/0/5, po: 5}
   hardware_info: {VIC_slot: MLOM}
   rack_info:{rack_id: RackC} # optional
   sriov_tor_info: {NCS-5500-1: 'TenGigE0/0/0/8, TenGigE0/0/0/9', NCS-5500-2: 'TenGigE0/0/0/8, TenGigE0/0/0/9'}

#Note: if sriov is defined, it need not be present on all servers; However, when present on a given server, the
number of SRIOV port need to be 4 and consistent across the servers. Also,set the INTEL_SRIOV_PHYS_PORTS to 4,
when using SRIOV with NCS-5500 as ToR. Set the value of INTEL_SRIOV_VFS as per the settings of your VNF (see
details later for the default values, etc)
```

```
   tor_info: {NCS-5500-1: TenGigE0/0/0/4, NCS-5500-2: TenGigE0/0/0/4, po: 6}

MULTI_SEGMENT_ROUTING_INFO:
  bgp_as_num: <1 to 65535>
  isis_area_tag: <string>
  loopback_name: <loopback<0-2147483647>>
  api_bundle_id: <1 to 65535>
  api_bridge_domain: <string> #Optional, only needed when br_api of mgmt node is also going via NCS-5500; #this
item and api_bundle_ids are
mutually exclusive

  ext_bridge_domain: <string> # user pre-provisions physical, bundle interface, subinterface and external BD"
for external uplink and provides
external BD info in the setup_data
```

Customization of Cisco NCS 5500 Configuration for Ethernet Segment ID and Route-Target

Cisco VIM automatically generates the Ethernet Segment Identifier (ESI) for EVPN segments (as defined under each Bundle-Ether interface) and route-targets during Cisco NCS 5500 ToR configuration.
You can set the ESI for EVPN segments only during day-0 configuration. To customize the configuration, define the following in the setup_data as part of the day-0 configuration:

```
ESI_PREFIX: 91.<Pod_number>.<pod_region_number>.00.00.00.00
```

Sample ESI

```
evpn
 interface Bundle-Ether<BE#> ethernet-segment
 ethernet-segment identifier type 0 91.<Pod_number>.<pod_region_number>.00.00.00.00.00.00.<BE#_in_hex>
 Example:
 evpn
 interface Bundle-Ether10
 ethernet-segment
 ethernet-segment identifier type 0 91.05.02.00.00.00.00.00.0a
```

If ESI defined in RFC 7432 is appended with the Bundle ID in hex, it will add up to a total of 9 octects, that is, the ESI_PREFIX must have a max length of 7 octects.
Similar to ESI_PREFIX, Cisco VIM supports custom-defined route-targets for management, storage, and tenant network segment, when Cisco NCS 5500 is set as ToR switch. This configuration is optional on per network segment basis, but Cisco VIM generates route-target automatically if not defined. To avail this configuration, the pod administrator must define a rt_suffix and rt_prefix in each network segment as listed below:

```
NETWORKING:
  networks:
    - gateway: 5.0.0.1
      pool: [5.0.0.11 to 5.0.0.50]
      segments: [management, provision]
      subnet: 5.0.0.0/24
      vlan_id: 200
      rt_prefix: <Local to POD>
      rt_suffix: < Region>:< pod_region_number >
   -
     gateway: 172.25.34.161
     segments: [storage]
     subnet: 172.25.34.160/28
     vlan_id: 2438
     rt_prefix: <Local to POD>
     rt_suffix: < Region>:< pod_region_number >
```

Resultant Route-Target

```
<Local to POD>:<Region>< POD number in the region><vlan_id>
```

Example:

```
3000:10100214
```

Each route-target is unique with its respective VLAN-id. Route targets associated with tenant VLANs are generated by appending each VLAN id from TENANT_VLAN_RANGES to the *rt_suffix* and *rt_prefix* defined in the network segments.

Resulting route-targets (*rt_prefix*", plus :, plus *rt_suffix*, plus the VLAN ID) must not exceed the six octets as per RFC 4360 for the Extended Communities. The maximum value is eight octets with the first two being reserved for type information.

NCS Day 0 Configuration (Prior to starting Cisco VIM installation)

You must define the following configuration on the NCS before starting Cisco VIM installation:

```
line default
exec-timeout 0 0

SSH:
ssh server v2
ssh server vrf default
ssh server netconf port 831
ssh server netconf vrf default ssh timeout 60
ssh
server rate-limit 600

USERNAME:

username admin
group root-lr
group cisco-support
secret 0 <password>
```


For SSH to work, generate a key using *crypto key generate rsa*.

Prerequisites for Segment Routing Global Block and ISIS Prefix

An admin must be pre-define the segment routing configuration as given in the following example:

```
segment-routing
global-block 16000 20000
The prefix within the ISIS setup_data.yaml configuration has to be within the global-block IDs.
Example:

TORSWITCHINFO:
  CONFIGURE_TORS: true

  SWITCHDETAILS:
    -  {br_mgmt_po_info:1, br_mgmt_port_info: TenGigE0/0/0/10, hostname: a25-ncs5500-1-ru30,
isis_loopback_addr: 10.10.10.10,
    isis_net_entity_title: 49.0001.1720.1625.5011.00, isis_prefix_sid: 16001, password:
    CTO1234!, ssh_ip: 172.28.123.176, username: admin, vpc_peer_keepalive:
    172.28.123.177, vpc_peer_port_address: '100.100.100.2/29,100.100.101.2/29',vpc_peer_port_info:'HundredGigE0
/0/1/4,HundredGigE0/0/1/5'}

   -  {br_mgmt_po_info: 1, br_mgmt_port_info: TenGigE0/0/0/10, hostname: a25-ncs5500-2-ru29,
isis_loopback_addr: 20.20.20.20,
   isis_net_entity_title: 49.0001.1720.1625.4022.00, isis_prefix_sid: 16002, password: CTO1234!, ssh_ip:
172.28.123.177, username: admin,
   vpc_peer_keepalive: 172.28.123.176, vpc_peer_port_address: '100.100.100.3/29,100.100.101.3/29',
vpc_peer_port_info:
'   HundredGigE0/0/1/2,HundredGigE0/0/1/3'}

 TOR_TYPE: NCS-5500
```

Prerequisites for API and External Network Segments with NCS-5500 as ToR

Pre-provision the NCS-5500 with the bridge domains for API and external network segments. The configured bridge domain names for API and external must be the same as those defined in *setup_data.yaml* (api_bridge_domain and ext_bridge_domain) under the MULTI_SEGMENT_ROUTING_INFO section defined above.
A check on each NCS-5500 must show the following:

```
RP/0/RP0/CPU0:NCS-5500-2#sh run l2vpn bridge group cvim
l2vpn
 bridge group cvim
          bridge-domain api
 l2vpn bridge group cvim
        bridge-domain external
```

During deployment of NCS-5500 as ToR, Cisco supports the workloads of the provider network along with the tenant network.

Listed below are some of the assumptions under which this combination works.

- Provider network segment must be available from Day 0.
- Few of the PROVIDER_VLAN_RANGES must be defined. You can always expand the PROVIDER_VLAN_RANGES with an additional VLAN range (minimum starting VLAN range is 2) so that the maximum number of PROVIDER_VLAN_RANGES and TENANT_VLAN_RANGES should add up to 200.
- Bridge domain for provider starts with prefix: provider VLANId. It is created manually on the NCS-5500 before the Cisco VIM deployment begins and upstream interfaces are configured.

Support and Pre-requisites for Provider Network with NCS-Concept

In a deployment of NCS-5500 as ToR, along with the tenant network, Cisco supports provider networks. The following points are key to use provider_networks with NCS as ToR:

- Provider network segment has to be defined on Day 0. Also, a handful of PROVIDER_VLAN_RANGES must be defined in the *setup_data.yaml.*

  > ⚠ You cannot add it after a Cisco VIM deployment.

- The PROVIDER_VLAN_RANGES can be extended after the Cisco VIM installation, by running reconfiguration with an updated *setup_data.yaml* (minimum starting VLAN range is two, for example, PROVIDER_VLAN_RANGES: 3200:3202 (existing range), 3204:3206 (newly added range)).
- The maximum number of PROVIDER_VLAN_RANGES and TENANT_VLAN_RANGES must not exceed 600.
- Bridge domain for provider starts with prefix: provider<VLANId> and are created manually on the NCS-5500 before the Cisco VIM deployment begins with necessary upstream interfaces configured.

Pre-requisites for Provider Network with NCS-5500 as ToR

Provider network support requires the following pre-requisites:

1. Define the network and provider VLAN ranges sections in *setup_data.yaml* as given below:

   ```
   NETWORKING:
   -
     segments: [provider] vlan_id: None
     PROVIDER_VLAN_RANGES: 127,3406:3409
   ```

2. Pre-provisioning the NCS with bridge-domains for corresponding VLANs and plumbing the uplink configuration into these bridge-domains:

   ```
   RP/0/RP0/CPU0:NCS-5500-2#sh run l2vpn bridge group cvim
   l2vpn
   bridge group cvim
   bridge-domain provider127

   l2vpn
   bridge group cvim
   bridge-domain provider3406

   l2vpn
   bridge group cvim
   bridge-domain provider3407
   ```

- Cisco VIM configures all the host facing subinterfaces for these provider VLANs and EVIs, and plumb them into each of the pre-provisioned provider bridge-domains.
- When pre-provisioning bridge-domain, ensure that the BD names follow the naming convention of provider<*vlan-id*>.

ToR Configuration with ACI Fabric

Cisco VIM integrates with ACI in three different ways:

1. *ships in the night* where the switch ports are pre-configured with relevant VLANs ahead of time.
2. ToR configuration without the APIC plugin using ACI API.

In all these cases, openvswitch is used as the mechanism driver.

In the case of *ships in the night* model, all the relevant configurations are done static and done ahead of time.

If ACI plugin is not used, Cisco VIM invokes the APIC APIs to pre-provision the right set of VLANs (along with the Day 0 aspects) on the corresponding server ports ahead of time.

For details on integration with and without the APIC plugin and the relevant ToR configuration, see Enabling ACI.

Servers and Network Option

Servers and Network Option

Overview

Cisco VIM supports C-series pod running with either all Intel 710X NICs or Cisco VICs for control and data plane. In the Intel NIC setup, M4 and M5 (Micropod) based pods must have 2-4 port and 1 or 2 4 port X710 respectively, for control and data plane connectivity. The orchestrator identifies the NIC support, based on the following INTEL_NIC_SUPPORT values:

- False -This is the default value. The orchestrator assumes that all the servers have Cisco VIC.
- True - The orchestrator assumes that all the servers have Intel NIC.

To define the value, set the following configuration in the *setup_data.yaml* file:

```
# INTEL_NIC_SUPPORT: <True or False>
```

The X710 based NIC redundancy is enabled by default for M4-based Intel NIC system, but not for M5-based Intel NIC system. For more information, see UCS C-Series Network Topologies.

To bring in NIC redundancy across the X710s for M5-based Intel NIC systems, define the following global parameters in the *setup_data.yaml* file:

```
NIC_LEVEL_REDUNDANCY: <True or False> # optional and only applies when INTEL_NIC_SUPPORT is set to True
```

A C-series pod with Intel NIC also supports SRIOV as an option, when defined in a setup_data.
To enable SRIOV as an option, define a value in the range 1-32 where 32 is maximum number of INTEL_SRIOV_VFS: <integer>.

In the C-series pod running with 4-port Intel 710 card, 1 port (port #c) from each of the Intel NICs are used for SRIOV by default. However, some VNFs need additional SRIOV ports to function. To meet the requirement, an additional variable is introduced in the *setup_data.yaml* file to include a second port (port d) of the Intel NIC for SRIOV.
To adjust the number of SRIOV ports, set the following option in the *setup_data.yaml* file:

```
#INTEL_SRIOV_PHYS_PORTS: <2 or 4>
```

The parameter INTEL_SRIOV_PHYS_PORTS is optional and takes the value two, or four or eight (only in M5 based pods). If not defined, value of two is used. For SRIOV support on NCS-5500, the value must be four for INTEL_SRIOV_PHYS_PORTS.
In M5 Micropod environment with NIC_LEVEL_REDUNDANCY as false, a single X710 is used for control/data plane and an additional XL710 or 2-port X710 is used for SRIOV, where INTEL_SRIOV_PHYS_PORTS takes a value of 2.

From Cisco VIM 3.4.4 with pure Intel NIC pod, you can combine control plane and date plane on the same pair of ports (use total of 2 ports) or individually separated one pair of ports for control plane and another pair of ports for data plane (use total of 4 ports).

- True - control plane and date plane on the same pair of ports (Default for third-party platform)

  samxpet
  |-samxpet0
  |-samxpet1

- False - individually separated one pair of ports for control plane and another pair of ports for data plane (Default for UCS C-series platform)

  samx
  |-samx0
  |-samx1

pet
|-pet0
|-pet1

```
# COMBINE_CPDP: <True or False>   # optional and only applies when
#                                 # INTEL_NIC_SUPPORT is set to True
```

SRIOV Support on Cisco VIC Pod

Cisco VIM supports M4-based C-series pod running with one two-port Cisco VIC for control plane and two two-port Intel 520s or two two-port XL710 for SRIOV (called VIC/NIC deployment). It also supports M5-based C-series pod running with one 2-port 40G Cisco VIC for control plane and two 2-port XL710 for SRIOV.
The orchestrator identifies the VIC/NIC support based on the following CISCO_VIC_INTEL_SRIOV values:

- False-This is the default value. The orchestrator assumes that all the servers have Cisco VIC.
- True-The orchestrator assumes that all the servers have Intel NIC.

To define the value, use the command:

```
CISCO_VIC_INTEL_SRIOV: <True or False>
```

A C-series M4 pod running Cisco VIC/Intel NIC (2x520 or 2xXL710) supports SRIOV on the Intel NIC.

A C-series M5 pod running Cisco VIC/Intel NIC (2xXXV710 or 2xXL710) supports SRIOV on the Intel NIC. In the case of 25G and 40G BOM, the Cisco VIC is 1457 or 1387, respectively.

To enable SRIOV, define the below parameter with a value in the range 1-63 (63 is maximum) for X520 or 1-32 (32 is maximum) for XL710 or XXV710: INTEL_SRIOV_VFS: <integer>.

By default in the M4 C-series pods running with Cisco VIC and Intel 520/XL710, the control plane runs on the Cisco VIC ports and all the four ports in the Intel NIC are used for SRIOV.

In C-Series M5 pods running with 40G Cisco VIC and Intel XL710, the control plane runs on the Cisco VIC ports and all the four or eight ports from the two intel XL710 are used for SRIOV. Similarly in the case of 25G M5 pod (25G Cisco VIC and Intel XXV710), the same layout applies.

In M5-based VIC/NIC pods, define INTEL_SRIOV_PHYS_PORTS: <4 or 8>, with default value as 4, to indicate the number of ports participating in SRIOV.

In the pods running with CISCO_VIC_INTEL_SRIOV option, some computes can run only with Cisco VIC without SRIOV option if they do not have Intel NIC cards.
Define the following parameter in the *setup_data.yaml* file to setup the SRIOV card type:

```
#SRIOV_CARD_TYPE: <X520 or XL710>   # for M4 based computes
#SRIOV_CARD_TYPE: <XXV710 or XL710> # for M5 based computes
```

M4 compute supports different types of the card (X520 and XL710), with a pod supporting computes having different SRIOV card types.

1. If SRIOV_CARD_TYPE is not provided, Cisco VIM chooses the first two slots from all SRIOV compute nodes.
2. If SRIOV_CARD_TYPE is provided, Cisco VIM chooses the first two slots matching the target card type from each of the SRIOV compute nodes, so that a match between intent and reality exists.

For Quanta-based pods, the SRIOV slot order starts from the higher slot number, that is, for NUMA, NIC at higher slot has value 0, 2. You can override this, by defining the following as ascending, in which case NIC at higher slot has value of 1, 3.

```
# SRIOV_SLOT_ORDER: <ascending or descending> # Optional, applicable for Quanta-based pods
```


From Cisco VIM 2.4.4 onwards, some computes have XL710 while others have X520 for SRIOV in M4 settings. This is achieved by defining the SRIOV_CARD_TYPE at a per compute level (see the SERVERS section of the setup_data in example file).

From Cisco VIM 2.4.9 onwards, 40G based M5 computes are supported.

From Cisco VIM 2.4.15, 40G based M5 controller and Ceph nodes can be mixed with 10G based M4 VIC/NIC pods.

Support of 25G VIC and NIC

From Cisco VIM 3.4.0, Cisco VIC 1457 and Intel XXV710 are supported in some specific BOM configuration. The first one is a combination where the control plane is running on two ports (A and C by default) of Cisco 1457 and data plane is running over VPP on the two ports of the Intel XXV710. In this configuration, there is a second XXV710 NIC for SRIOV. To realize this configuration of Cisco VIC and Intel NIC baremetal combination without creating any Cisco vNICs, the option of INTEL_NIC_SUPPORT must be set to true.

```
CISCO_VIC_SUPPORT: true
INTEL_NIC_SUPPORT: true
INTEL_SRIOV_PHYS_PORTS: 2
INTEL_SRIOV_VFS: 16
```

The above option can also be used with openvswitch as the mechanism driver. If the above option is chosen for Cisco 1457 VIC, by default port A and C of the VIC are used for the control plane. To use the port A and B of the Cisco VIC for samx, you can define an optional variable globally or at a per-server level.

Following is the snippet of how to define the configuration in the *setup_data.yaml* file:

```
SERVER_COMMON:
  # Optional global config to change VIC's port channel enable configuration
  # option, from default True to False.  Applicable only for Cisco VIC that
  # support Port Channel, like UCS VIC 1457 25Gbps network adapter.
  #VIC_port_channel_enable: <True or False>
  # This can also be specified or
  # overridden at per server level
  # under server's hardware_info section.
```

A global configuration option is available to change VIC's admin FEC mode from default 'Auto' to either 'Off', 'cl74', or 'cl91' mode and to adapt to different types of switches. This is applicable only for Cisco VIC that supports changing the admin FEC mode like UCS VIC 1457 25Gbps network adapter.

The following is the snippet in the *setup_data.yaml* file to realize this configuration for the pod.

```
SERVER_COMMON:
  ....
  #VIC_admin_fec_mode: <Auto, Off, cl74, or cl91>
# This can be specified or overridden at per server level under server's hardware_info section.
```

Cisco M4 (VIC 1227) based VTS pods support additional M5 computes running on Cisco 1457 VIC. Additionally, OVS based Cisco M5 VIC (1457) with XXV710 NIC pods is supported. In this combination, the control and data plane run on Cisco 1457 VIC, with four ports of XXV710 Intel NIC dedicated for SRIOV.

Support of Third-party Compute in Hybrid Mode (HP DL360 Gen9)

Cisco VIM 2.4 introduces the first third-party compute. The first SKU chosen is HPE ProLiant DL360 Gen9. With this support, the Cisco VIM software is flexible enough to accommodate other SKUs. In Cisco VIM 2.4, the supported deployment is a full-on pod, with OVS as the mechanism driver, where the management, control, and storage nodes are based on existing Cisco UCS c220/240M4 BOM, and the compute nodes are on HPE ProLiant DL360 Gen9 hardware. From Cisco VIM 2.4.5 onwards, Cisco VIM supports the same HP SKU with both HP and HPE brand.

To minimize changes to the existing orchestration workflow and Insight UI, the existing Cisco VIC+NIC combo deployment scenario is reused to handle HP as a third-party compute. This reduces the changes needed for the hardware topology and *setup_data.yaml* configuration file. For details on NIC settings to enable HPE ProLiant DL360 Gen9 third-party compute, see **Intel NIC Support for SRIOV**

For Quanta servers, the support of third-party has been extended to all nodes (servers in control, compute, storage and management role.

The following table shows the port type mapping between Cisco UCS C-Series, HPE ProLiant DL360 and Quanta as compute:

Port Type	Cisco UCS c220/c240 Compute	HPEProLiantDL360Gen9 Compute	Quanta Server
Control and Data Plane	M4: MLOM - 1 x VIC 1227 M5: MLOM - 1 x VIC 1387 M5 MLOM - 1 x VIC 1457 M5: Intel - 1 or 2 x X710 DA4	FlexLOM - HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter	OCP 25G 2 port xxv710 based card
SRIOV	M4: PCIe - Intel X520-DA2 10 Gbps or Intel XL710 DA2 40 Gbps 2 port NIC M5: PCIe - Intel XL710 DA2 40 Gbps 2 port NIC M5: PCIe - Intel XXV710 DA2 25 Gbps 2 port NIC M5: PCIe - Intel X710 DA4 10 Gbps 4 port NIC	PCIe - HP Ethernet 10Gb 2-port 560SFP+ Adapter	PCIe - Intel xxv710 DA2 25 Gbps 2 port NIC

As this deployment does not support auto-ToR configuration, the TOR switch must have trunk configuration with native VLAN, jumbo MTU, and no LACP suspend-individual on the control and data plane switch ports.
Sample Nexus 9000 port-channel configuration is as follows:

```
interface port-channel30

description compute-server-hp-1 control and data plane
switchport mode trunk

switchport trunk native vlan 201
spanning-tree port type edge trunk
spanning-tree bpdufilter enable
mtu 9216

no lacp suspend-individual
vpc 30

!
interface Ethernet1/30

description compute-server-hp-1 flexlom port 1
switchport mode trunk

switchport trunk native vlan 201
mtu 9216

channel-group 30 mode active
```

Once the physical connection to the ToR switches and switch ports configuration is completed, enable/add the following additional variables in the *setup_data.yaml* configuration file:

```
CISCO_VIC_INTEL_SRIOV: True
INTEL_SRIOV_VFS: 63
```

Support of M4/M5 BOM in a Pod

With the transition of UCS from M4 to M5, there is a need to support M5 hardware in an existing M4 pods, so that the lifecycle management of the nodes through the EOL/EOS process of M4 can also be supported. Assuming that the additional M5 nodes have the same number of CPU cores, memory, and disk size (generation of the components can vary), the following table lists the NIC level compatibility matrix between M4 and M5 node.

Scenarios	Compute Type	1 x Cisco VIC 1227 (10G)	1 x Cisco VIC 1387 (40G)	1 x Cisco VIC 1457 (25G)	2 x Intel NIC X520 (10G)	2 x Intel NIC XL710 (40G)	2 x Intel NIC XXV710 (25G)	1 x Intel NIC X710-DA2 (10G)	2 x Intel NIC X710-DA4 (10G)
Scenario 1	Existing M4								
	New M5								
Scenario 2	Existing M4								
	New M5								
Scenario 3*	Existing M4								
	New M5								
Scenario 4	Existing M4								
	New M5								

- Scenario 3 is applicable only to NGENA BOM
- The M5 BOM for control and ceph nodes is also supported as mentioned in the table above, but you must drop the SRIOV and pet interface aspects of the NIC card from the target node.

Remote Registry Credentials

```
REGISTRY_USERNAME: '<username>'
REGISTRY_PASSWORD: '<password>'
REGISTRY_EMAIL: '<email@address.com>'
REGISTRY_NAME: <hostname of CiscoVIM software Hub'> # optional only if CiscoVIM software Hub is used
```

Common CIMC Access Information for C-series Pod

```
CIMC-COMMON:
cimc_username: "admin"
cimc_password: <"password">
```

UCSM Common Access Information for B-series Pod

```
UCSMCOMMON:
 ucsm_username: "admin"
 ucsm_password: <"password">
 ucsm_ip: <"a.b.c.d">
 ucsm_resource_prefix: <"skull"> # max of 6 chars
 ENABLE_UCSM_PLUGIN: <True> #optional; If True, Cisco-UCSM is used. If not defined, default is False
 MRAID_CARD: <True or False>
```

⚠ In Cisco VIM 3.x, UCSM plugin support is not enabled.

Configure Cobbler

```
## Cobbler specific information.
## kickstart:    static values as listed below
## cobbler_username: cobbler #username to access cobbler server; static value of Cobbler; not user configurable
## admin_username: root # static value of root; not user configurable
## admin_ssh_keys: This is a generated key which is put on the hosts.

## This is needed for the next install step, using Ansible.

COBBLER:

pxe_timeout: 45. # Optional parameter (in minutes); min of 30 and max of 120, defaults to 45 mins
cobbler_username: cobbler   #cobbler UI user; currently statically mapped to cobbler; not user configurable
admin_username: root       # cobbler admin user; currently statically mapped to root; not user configurable
#admin_password_hash has be the output from:

# python -c "import crypt; print crypt.crypt('<plaintext password>')"
admin_password_hash: <Please generate the admin pwd hash using the step above; verify the output starts with $6>

admin_ssh_keys:  # Optional parameter

- ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAoMrVHLwpDJX8j2DiE55WtJ5NWdiryP5+FjvPEZcjLdtdWaWA7W dP6EBaeskmyyU9B8ZJr1uClIN
/sT6yD3gw6IkQ73Y6bl1kZxu/ZlcUUSNY4RVjSAz52/oLKs6n3wqKnn7rQuLGEZDvXnyLbqMoxHdc4PDFWiGXdlg5DIVGigO9KUncPK
cisco@cisco-server

kickstart:               # not user configurable, optional
control: ucs-b-and-c-series.ks
compute: ucs-b-and-c-series.ks
block_storage: ucs-b-and-c-series.ks
```

Configure Network

```
NETWORKING:

domain_name:domain.example.com

#max of 4 NTP servers
ntp_servers:
-  <1.ntp.example.com>
-  <2.ntp.example2.com >
or
ntp_servers: ['2001:c5c0:1234:5678:1002::1', 15.0.0.254]    <== support for IPv6 address


#max of 3 DNS servers
domain_name_servers:
- <a.b.c.d>
or
domain_name_servers: ['2001:c5c0:1234:5678:1002::5', 15.0.0.1]    <== support for IPv6 address


http_proxy_server: <a.b.c.d:port> # optional, needed if install is through internet, and the pod is behind a
proxy
https_proxy_server: <a.b.c.d:port> # optional, needed if install is through internet, and the pod is behind a
proxy
admin_source_networks: # optional, host based firewall to include an allowed list of admin's source IP (v4 or
v6)

- 10.0.0.0/8

- 172.16.0.0/12

- <"2001:xxxx::/64">
```

External access to the management node is made through the IP address configured on the br_api interface. To provide additional security for this connection, an optional *admin_source_networks* parameter is provided. When specified, the access to administrator services is allowed only from the IP addresses specified on this list.

Use this setting with care, as a misconfiguration can lock out an administrator from accessing the management node through the network. Recovery can be done by logging in through the console and reconfiguring this setting.

Define Network Segments

```
networks:

-  # CIMC network section is applicable only for B-series
vlan_id: <107>

subnet: <10.30.115.192/28> # true routable network
gateway: <10.30.115.193>

pool:
 - 10.30.115.194 to 10.30.115.206
segments:
- cimc
-
vlan_id: <int>

subnet: <cidr with mask> # true routable network
gateway: <ipv4_address >
ipv6_gateway: <ipv6_address>  <== required if IPv6 based OpenStack public API is enabled
ipv6_subnet: < v6 cidr with mask>

segments:

- api
-
vlan_id: <int>
```

```
subnet: <cidr/mask>
gateway: <ipaddress>
pool:
# specify the pool range in form of <start_ip> to <end_ip>, IPs without the "to"
# is treated as an individual IP and is used for configuring

-
ip_address_1 to ip_address_2 in the current network segment

# optional, required if managemen_ipv6 is defined at server level
ipv6_gateway: <ipv6_address>
ipv6_subnet: <v6 cidr with mask>
ipv6_pool: ['ipv6_address_1 to ipv6_address_2']

segments: #management and provisioning are always the same
-  management
-  provision


# OVS-VLAN requires VLAN-id as "None"

# LinuxBridge-VXLAN requires valid VLAN-id

-
vlan_id: <vlan_id or None>
subnet: <v4_cidr w/ mask>
gateway: <v4 ip address>
pool:
- ip_address_1 to ip_address_2 in the current network segment

segments:
- tenant
-
vlan_id: <vlan_id>
subnet: <v4_cidr w/mask>
gateway: <ipv4_addr>

pool:
-
ip_address_1 to ip_address_2 in the current network segment

segments:
- storage
# optional network "external"
-
vlan_id: <int>
segments:
-
external
# optional network "provider"; None for C-series, vlan range for B-series
-
vlan_id: "<None or 3200-3210>"
segments:

-
provider
```

For PODTYPE: ceph, the storage segment needs to be replaced with segment named "cluster". Also, for central ceph pod, the only other segment allowed is management/provision.

Define Server Roles

In the Roles section, add the host name of the servers and their corresponding roles. In case of Micropod, specify the same server names under control, compute, and ceph. Ensure that the number of servers under each role must be three for Micropod. You can optionally expand the Micropod to include additional computes. In the case of Hyperconverged deployment (HC), all storage nodes act as compute nodes, but not vice-versa.

In the case of Edge pod (to support low latency workloads without persistent storage), specify the same server names under control (total of three), and compute role (there is no server with storage role). You can optionally expand the edge pod, to include additional computes. The edge pod can connect to a central Ceph cluster via its management network, so that the Ceph cluster offers glance image service.

The central Ceph cluster to which the edge pods are communicating to for the glance image service is called the Ceph pod-type. For the pod-type *ceph*, specify the same server names under *cephcontrol* (total of three), and *cephosd* role. You can optionally expand the ceph pod to include additional cephosd nodes.

```
ROLES:-> for PODTYPE: fullon
  control:
    Your-Controller-Server-1-HostName
    Your-Controller-Server-2-HostName
    Your-Controller-Server-3-HostName

  compute:
    Your-Compute-Server-1-HostName
    Your-Compute-Server-2-HostName
    Your-Compute-Server-n-HostName

  block_storage:
    Your-Ceph-Server-1-HostName
    Your-Ceph-Server-2-HostName
    Your-Ceph-Server-3-HostName

ROLES:-> for PODTYPE: micro
  control:
    Your-Server-1-HostName
    Your-Server-2-HostName
    Your-Server-3-HostName

  compute:
    Your-Server-1-HostName
    Your-Server-2-HostName
    Your-Server-3-HostName
    Your-Server-4-HostName (optional expansion of computes)
    Your-Server-5-HostName (optional expansion of computes)

  block_storage:
    Your-Server-1-HostName
    Your-Server-2-HostName
    Your-Server-3-HostName

ROLES:-> for PODTYPE: UMHC
  control:
    Your-Controller-Server-1-HostName
    Your-Controller-Server-2-HostName
    Your-Contoller-Server-3-HostName

  compute:
    Your-Compute-Server-1-HostName
    Your-Compute-Server-2-HostName
    Your_HC_Server-1_HostName
    Your_HC_Server-2_HostName
    Your_HC_Server-3_HostName

  block_storage:
    Your_HC_Server-1_HostName
    Your_HC_Server-2_HostName
    Your_HC_Server-3_HostName

ROLES: -> for PODTYPE: edge
  control:
    Your-Server-1-HostName
    Your-Server-2-HostName
    Your-Server-3-HostName

  compute:
    Your-Server-1-HostName
    Your-Server-2-HostName
```

```
    Your-Server-3-HostName
    Your-Server-4-HostName (optional expansion of computes)
    Your-Server-5-HostName (optional expansion of computes)


ROLES: -> for PODTYPE: ceph
  cephcontrol:
     Your-Server-1-HostName
     Your-Server-2-HostName
     Your-Server-3-HostName

  cephosd:
     Your-Server-1-HostName
     Your-Server-2-HostName
     Your-Server-3-HostName
     Your-Server-4-HostName (optional expansion of Ceph OSD Nodes)
     Your-Server-5-HostName (optional expansion of Ceph OSD Nodes)
```


- The maximum length of non-FQDN hostname is 32 characters. The maximum length of Your-Controller-Server-1-HostName hostname is 32 characters in both the ROLES and SERVERS section.
- The maximum length including the FQDN is 64 characters, where the hostname can only have characters that are in any combination of "A-Za-z0-9-.", and the TLD is not all numeric.
- Cisco VIM does not allow "_" in the hostnames.
- For enabling IPA, hostname for all servers including the management node must be in lower case FQDN (RFC4120) and belongs to ip_domain_name

Cisco VIM introduces the notion of Micropod to address solutions that have requirements of high availability, with limited compute and storage needs. In this deployment model, the control, compute, and storage services reside on each of the three nodes that constitute the pod. Cisco VIM also supports the expansion of the Micropod to accommodate additional compute nodes. Each cloud application can decide the type of pod needed based on their resource (memory, storage consumption) requirements. The Micropod option supports only OVS/VLAN (with Cisco-VIC or Intel 710 NIC) or VPP/VLAN (only on Intel NIC) on a specific BOM.

To enable the Micropod option, update the setup_data as follows:

```
PODTYPE: micro
```

Cisco VIM supports the hyper-convergence (UMHC) option of UMHC and NGENAHC. The UMHC option supports only OVS/VLAN with a combination of Cisco-VIC and Intel 520 NIC on a specific BOM, while the NGENAHC option supports only VPP/VLAN with control plane over Cisco VIC and data plane over two-port Intel X-710.

To enable the hyper-convergence with (UMHC) option, update the *setup_data* as follows:

```
PODTYPE: UMHC
```

To enable the hyper-convergence with NGENAHC option, update the setup_data as follows:

```
PODTYPE: NENAHC
```

On Quanta server, you can also enable edge cloud functionality for low-latency workloads, for example, vRAN that does not need persistent storage. To enable such deployment, update the setup_data as follows:

```
PODTYPE: edge
```

If the edge pod is communicating with a central Ceph cluster that is managed by Cisco VIM, update the *setup_data* for the respective central-ceph cluster as follows:

```
PODTYPE: ceph
```

Define Servers - Rack (C-Series, Quanta) Pod

⚠ The maximum length of host name is 32 characters.

```
# For enabling IPA, hostname for all servers including the management node must be in lower case FQDN (RFC4120)
and belongs to ipa_domain_name

SERVERS:

 Your_Controller_Server-1_HostName:
   cimc_info: {'cimc_ip': <IPv4 or IPv6>}
   rack_info: {'rack_id': 'RackA'}

   #hardware_info: {'VIC_slot': '7'} # optional; only needed if vNICs need to be created on a specific slot,
for example, slot 7
   #management_ip: <static_ip from management pool> #optional, if defined for one server, must be defined for
all nodes
   #cimc username, password at a server level is only needed if it is different from the one defined in the
CIMC-COMMON section
   # management_ipv6: <Fixed ipv6 from the management_ipv6 pool> # <== optional, allow manual static IPv6
addressing, also if defined management_ip has to be defined

   #storage_ip: <Fixed ip from the storage pool> # optional. If defined for one server or if management_ip has
to be defined, then it must be defined for all.
   #DISABLE_HYPERTHREADING: <True or False> # <== optional, override the global Hyper-Threading configuration


 Your_Controller_Server-2_HostName:
  cimc_info: {'cimc_ip': '<v4 or v6>', 'cimc_username': 'admin','cimc_password': 'abc123'}
  rack_info: {'rack_id': 'RackB'}

Your_Controller_Server-3_HostName:

  cimc_info: {'cimc_ip': '<v4 or v6>'}
  rack_info: {'rack_id': 'RackC'}
  hardware_info: {'VIC_slot':'7'} # optional only if a specific VNIC needs to be chosen

Your_Compute-1_HostName:
  cimc_info: {'cimc_ip': '<v4 or v6>}
  rack_info: {'rack_id': 'RackA'}
  hardware_info: {'VIC_slot': '3'} # optional only if specific VNIC needs to be chosen
  VM_HUGHPAGE_PERCENTAGE: <0 - 100>  # optional only for compute nodes and when NFV_HOSTS: ALL and
MECHANISM_DRIVER: openvswitch
  VM_HUGHPAGE_SIZE: <2M or 1G> # optional, only for compute nodes and when NFV_HOSTS is ALL and
MECHANISM_DRIVER is openvswitch
  trusted_vf: <True or False> # optional, only for compute nodes which have in SRIOV, can be enabled via
reconfigure
  rx_tx_queue_size: <512 or 1024> # optional, only for compute nodes
  NOVA_CPU_ALLOCATION_RATIO: 1.0 <float, range: 0.958-16.0>   # <== optional, override the
NOVA_CPU_ALLOCATION_RATIO configuration defined in openstack_config.yaml
  NOVA_RAM_ALLOCATION_RATIO: 1.0 <float, range: 1.0-4.0>      # <== optional, override the
NOVA_RAM_ALLOCATION_RATIO configuration defined in openstack_config.yaml

  hardware_info: {'VIC_slot': '<7>', SRIOV_CARD_TYPE: <XL710 or X520 or XXV710>,
  VIC_port_channel_enable: <True or False>, VIC_admin_fec_mode: <Auto, Off, cl74, or cl91>,
  root_drive_type: <HDD or SSD or M.2_SATA, NUM_GPU_CARDS: < 0 to 6>} } # VIC_Slot is optional, defined for
location of Cisco VIC,
  VIC_port_channel_enable is optional and applicable to 1457 based VIC where one wants to use port A and B to
connect to ToR (instead of port A and C),
  VIC_admin_fec_mode is optional and used when the ToR needs explicit configuration of fec mode. Unless
deviating from the default BOM, the option of root_drive_type can be   skipped. However, the defining the
option of M.2 is mandatory on a per server basis if it is used as a booting media for a given
server.
Note the option of M.2 is only valid for UCS M5 systems. NUM_GPU_CARDS is optional and can vary on a per server
basis.

Your_Storage HostName:
  cimc_info: {'cimc_ip': 'v4 or v6'} rack_info: {'rack_id': 'RackA'}
  hardware_info: {osd_disk_type: <HDD or SSD>} # optional only when the pod is multi-backend ceph, and a
minimum of three storage servers should be available for each backend type. It is recommended to have 4 nodes
for each storage type
```

SRIOV_CARD_TYPE option is valid only when CISCO_VIC_INTEL_SRIOV is True and can be defined at per compute level for in a pod.

If it is not defined at a per compute level, the global value is taken for that compute.

If not defined at the compute level nor at the global level, the default of X520 is set. The compute can be standalone or hyper-converged node.

Cisco VIM installation requires the controller node Rack IDs to be unique, to indicate the physical rack location so that physical redundancy is provided within the controllers. If all the controller nodes are installed in the same rack, you must assign a unique rack ID to prepare for future releases of Cisco VIM that include rack redundancy. However, compute and storage nodes do not have rack ID restrictions.

For Central Ceph cluster, swap the *storage_ip* with *cluster_ip*

Define Servers - B-Series Pod

For UCS B-Series servers, the maximum length of hostname is 16 characters.

```
# For enabling IPA, hostname for all servers including the management node must be in lower case FQDN (RFC4120)
and belongs to ip_domain_name

SERVERS:
 Your_Controller_Server-1_HostName:
 rack_info: {'rack_id': 'rack2'}
 ucsm_info: {'server_type': 'blade', 'chassis_id': 1, 'blade_id': 1}

 Your_Controller_Server-2_HostName:
 rack_info: {'rack_id': 'rack3'}
 ucsm_info: {'server_type': 'blade', 'chassis_id': 2, 'blade_id': 1}

Your_Controller_Server-3_HostName:
 rack_info: {'rack_id': 'rack4'} ucsm_info: {'server_type': 'blade', 'chassis_id': 2, 'blade_id': 4}
 #management_ip: <static_ip from management pool> #optional, if defined for one server, has to be defined for
all nodes
 #storage_ip: <Fixed ip from the storage pool> # optional but if defined for one server, then it must be
defined for all, also if defined management_ip has to be defined

 Your_Compute-1_HostName:
 rack_info: {'rack_id': 'rack2'}
 ucsm_info: {'server_type': 'blade', 'chassis_id': 2, 'blade_id': 2}
 .. add more computes as needed
 Your_Storage-1_HostName:
 rack_info: {'rack_id': 'rack2'}
 ucsm_info: {'server_type': 'rack', 'rack-unit_id': 1}

 Your_Storage-2_HostName:
 rack_info: {'rack_id': 'rack3'}
 ucsm_info: {'server_type': 'rack', 'rack-unit_id': 2}

 Your_Storage-3_HostName:
 rack_info: {'rack_id': 'rack4'}
 ucsm_info: {'server_type': 'rack', 'rack-unit_id': 3}
 # max # of chassis id: 24
 # max # of blade id: 8
 # max # of rack-unit_id: 96
```

- Cisco VIM requires the controller rack IDs to be unique, to indicate the physical rack location and provide physical redundancy for controllers.
- If your controllers are all in the same rack, you must still assign a unique rack ID to the controllers to provide for future rack redundancy. Compute and storage nodes have no rack ID restrictions.

Server Common

In the SERVER_COMMON section, options to define parameters at a global or per role type are available. Options include platform vendor, root_drive_type, VIC_admin_fec_mode, and so on.

```
SERVER_COMMON:
 server_username: root   # not user configurable

# Optional global config to change VIC's Port Channel Enable configuration
# option, from default True to False.  Applicable only for Cisco VIC that
# support Port Channel, like UCS VIC 1457 25Gbps network adapter.
#VIC_port_channel_enable: <True or False>  # This can also be specified or
                                           # overrided at per server level
                                           # under server's hardware_info
                                           # section.
# Optional global config to change VIC's admin FEC mode, from default 'Auto'
# to either 'Off', 'cl74', or 'cl91' mode.  Applicable only for Cisco VIC
# that support changing the admin FEC mode, like UCS VIC 1457 25Gbps network
# adapter.
#VIC_admin_fec_mode: <Auto, Off, cl74, or cl91>  # This can also be specified
                                                 # or overrided at per server
                                                 # level under server's
                                                 # hardware_info section.
# Optional value, allow static override value for platform vendor and/or root drive type for Operating System
install instead of dynamic discovery at runtime.
#
# vendor, allowed values:
#   CSCO - Cisco Systems Inc
#   HPE  - Hewlett Packard Enterprise
#   QCT  - Quanta Cloud Technology Inc
# root_drive_type, allowed values:
#   HDD or SSD - drive locate in front or rear drive bay
#   M.2_SATA   - internal SSD drive (mandatory config if booting off M.2 SATA
#                                    SSD, not valid for M4 platform)
#   NVMe       - internal NVMe drive (mandatory config if booting off M.2
#                                     NVMe)
# num_root_drive: Optional field, number of drives to use for root/boot
#                 virtual drive, valid range from 0 to 26
#                 - 0 for all available drives
#                 - 1 to 26 (this value includes dedicated hot spare count)
# root_drive_raid_level: Optional field, RAID level to use for creating the
#                        root/boot virtual drive
#                        - raid0 (require at least 1 drive)
#                        - raid1 (require at least 2 drives)
#                        - raid5 (require at least 3 drives)
#                        - raid6/raid10 (require at least 4 drives)
# root_drive_raid_spare: Optional field, number of drives to reserve as
#                        dedicated hot spare for the RAIDed root/boot virtual
#                        drive, valid range from 0 to 4
#
#  vendor: <CSCO or QCT>    <= Global level vendor override, all servers
#  control:
#    hardware_info:         <= Role level override, all controls
#      vendor: <CSCO or QCT>
#      root_drive_type: <HDD, SSD, M.2_SATA, or NVMe>
#  compute:
#    hardware_info:         <= Role level override, all computes
#      vendor: <CSCO, HPE, or QCT>
#      root_drive_type: <HDD, SSD, M.2_SATA, or NVMe>
#      num_root_drive: <0 to 26>
#      root_drive_raid_level: <raid0, raid1, raid5, raid6, or raid10>
#      root_drive_raid_spare: <0 to 4>
#  block_storage:
#    hardware_info:         <= Role level override, all storages
#      vendor: <CSCO or QCT>
#
```

OpenStack Configuration

OpenStack Configuration

OpenStack Admin Credentials

```
ADMIN_USER: <admin>
ADMIN_TENANT_NAME: <admin tenant>
```

OpenStack HAProxy and Virtual Router Redundancy Protocol Configuration

Following are the configuration parameters:

- external_lb_vip_address: An externally routable ipv4 address in API network.
- external_lb_vip_ipv6_address: An externally routable ipv6 address in API network.
- VIRTUAL_ROUTER_ID: vrrp_router_id #for example: 49 (range of 1-255).
- internal_lb_vip_address: <Internal IP address on management network>.
- internal_lb_vip_ipv6_address: <Internal IPv6 address on management network> # optional, only for dual stack environment.

OpenStack DNS Name Configuration

For web and REST interfaces, names are commonly used instead of IP addresses. You can set the optional *external_lb_vip_fqdn* parameter to assign a name that resolves to the external_lb_vip_address as given below:

```
external_lb_vip_fqdn: host or DNS name matching external_lb_vip_address
```

You must configure the services to ensure that the name and address matches. Resolution can be made through DNS and the Linux /etc/hosts files, or through other options supported on your hosts. The Cisco VIM installer adds an entry to */etc/hosts* on the management and other Cisco NFVI nodes to ensure that this resolution can be made from within the pod. You must ensure that the resolution can be made from any desired host outside the pod.

OpenStack TLS and HTTPS Configuration

Enabling TLS is important to ensure that the Cisco VIM network is secure. TLS encrypts and authenticates communication to the cloud endpoints. When TLS is enabled, two additional pieces of information must be provided to the installer: *haproxy.pem* and haproxy-ca-crt. These must be placed in the ~ */installer-xxxx/openstack-configs* directory.

- *haproxy.pem* is the server side certificate file in PEM format. It must include the server certificate, any intermediate certificates, and the private key for the server. The common name of the certificate must match the external_lb_vip_address and/or the external_lb_vip_fqdn as configured in the *setup_data.yaml* file.
- *haproxy-ca.crt* is the certificate of the trusted authority that signed the server-side.

For production cloud, these certificates are provided by a trusted third-party CA according to your company IT policy. For cloud test or evaluation, self-signed certificates are used quickly enable TLS. For convenience, the installer includes a script that creates and install self-signed certificates.

> ⚠ As these certificates are generated by this tool for testing purposes, do not use these certificates for production.

To use this tool, make the following changes to the setup data file and run the tool:

```
external_lb_vip_address: <IP address on external network>
external_lb_vip_tls: True
external_lb_vip_fqdn: host or DNS name matching external_lb_vip_address (if FQDN is needed)
```

To run the tool, from the */working_dir/* directory, execute the command:

```
#./tools/tls_cert_gen.sh -f openstack-configs/setup_data.yaml
```

OpenStack Glance Configuration with Dedicated Ceph or Netapp

For OpenStack Glance (the OpenStack image service), the dedicated Ceph object storage configuration is given below. As the Ceph and Glance keys are generated during the Ceph installation, you do not need to specify the keys in *setup_data.yaml* file.

```
STORE_BACKEND: ceph/netapp #supported as 'ceph' for ceph backend store;and netapp for netapp backend
```

CPU Allocation for Controllers in Micro and Edge Pods

As the controller node is shared with other types of nodes in Micropod (storage and compute) or edge pod (compute), there are deployments where the number of CPU cores allocated to the controller must be higher than the default value of two. From Cisco VIM 3.4.1, NR_RESERVED_ HOST_PCORES option is available only on fresh installation for Micropod and edge pod. The values lie in the range of 2 to 6.

You can configure this option by updating the *setup_data.yaml* file as given below:

```
# Number of cores associated to controllers in a micro or edge pod deployment, # default value if not defined
is 2
#NR_RESERVED_HOST_PCORES: <2 - 6>
```

CPU Allocation for Ceph in Hyper-converged or Micropod Systems

As the storage node is shared with other types of nodes (for example, compute node for Hyper-converged and control/compute nodes for Micropod), there are deployments where the number of CPU cores allocated to the Ceph role must be greater than the default value of two. From Cisco VIM 2.4.2, the option CEPH_OSD_RESEREVED_PCORES is available only on fresh installation for Micropod and Hyper-converged pods.
This option is set using the following commands in *setup_data,* where the value can range between 2 and 12.

```
# Number of cores associated to CEPH-OSD in a micro, UMHC or NGNENAHC deployment.
# default value if not defined is 2
# CEPH_OSD_RESERVED_PCORES: <2 - 12>
```

Ceph Placement Group Information (Optional)

If you need to change the default percentages for placement group calculation, use this section to indicate the amount of data you expect in cinder/glance /nova. For NOVA_BOOT_FROM local, provide the values for cinder and glance. Additionally, for NOVA_BOOT_FROM ceph, provide *nova_percentage_da ta* for ephemeral data. All percentages need to add up to 100.

If no information is provided,

- code defaults to 60% cinder and 40% glance for NOVA_BOOT_FROM local.
- code defaults to 40% cinder, 30% glance and 30% nova ephemeral for NOVA_BOOT_FROM ceph.

You cannot change these values after deployment using update or reconfiguration.

```
For NOVA_BOOT_FROM local
CEPH_PG_INFO: {cinder_percentage_data: x, glance_percentage_data: y} # where x and y are integers and must add
up to 100

For NOVA_BOOT_FROM Ceph
CEPH_PG_INFO: {cinder_percentage_data: x, glance_percentage_data: y, nova_percentage_data: z}
where x, y and z are integers and must add up to 100
```

OpenStack Glance Configuration

```
STORE_BACKEND: <ceph or netapp based on backend storage>
```

OpenStack Cinder Configuration with Dedicated Ceph/Netapp

For OpenStack Cinder (the OpenStack storage service), the dedicated Ceph object storage configuration is given below.

```
VOLUME_DRIVER: ceph/netapp
```

Ensure that you do not change it. As the Ceph and Cinder keys are generated during the Ceph installation, you need not specify the keys in *setup_data.yaml* file. Use the *vgs* command to check your volume groups available on your controller nodes. The controller nodes run the Cinder volume containers and hold the volume groups for use by Cinder. If you have available disks and want to create a new volume group for Cinder use the *vgcreate* command.

OpenStack Settings on PODTYPE: Ceph for Glance Image service

Following are the examples for central_ceph setup_data details:

```
STORE_BACKEND: 'ceph' VOLUME_DRIVER: 'ceph'
```

OpenStack Settings on PODTYPE: Edge for Glance Image service

For the edge pod installation to be successful, the central Ceph cluster with which it communicates for glance image service must be up and running. For the edge pod to communicate with the central Ceph cluster, the following configurations are needed:

```
MON_HOSTS: <3 IPv4 or IPv6 addresses, of the cephcontrol servers in the central ceph cluster>
MON_MEMBERS: <3 IPv4 or IPv6 addresses of the cephcontrol servers in the central ceph cluster>
CLUSTER_ID: <ceph_cluster_id> to fetch the CLUSTER_ID of the central ceph cluster, ssh to the management node
of the "ceph" pod, and execute the following:
#cat /root/openstack-configs/ceph/fetch/ceph_cluster_uuid.conf to get the CLUSTER_ID GLANCE_RBD_POOL: images

GLANCE_CLIENT_KEY: <key_info> to fetch the GLANCE_CLIENT_KEY, ssh to the management node of the "ceph" pod, and
execute the following:
# cd /root/openstack-configs/ceph/fetch/
# ls to get the UUID
# cd /root/openstack-configs/ceph/fetch/<UUID>/
# cat etc/ceph/ceph.client.glance.keyring
```

OpenStack Nova Configuration

To reduce the boot time, the NOVA_BOOT_FROM parameter is set to local for Cisco VIM. While this reduces the boot time, it does not provide Ceph back end redundancy. For typical NFVI workloads, you must not enable this option (it will default to local). To overwrite it, you can set NOVA_BOOT_FROM to Ceph . This is applicable only when the backend is ceph. For Netapp, no entry for this parameter is allowed.

```
#Nova boot from CEPH/local
 NOVA_BOOT_FROM: <ceph or local> #optional, if not defined will default to local
```

OpenStack Neutron Configuration

Following is the OpenStack Neutron configuration:

```
# ML2 Conf - reference implementation of OVS/VLAN

MECHANISM_DRIVERS:
openvswitch TENANT_NETWORK_TYPES: "VLAN"

# VLAN ranges can be a single continuous range or comma separated discontinuous range
TENANT_VLAN_RANGES: <a:b,c:d>  # with a minimum of 2 VLANs

# Jumbo MTU functionality.
# ENABLE_JUMBO_FRAMES: True for provider networks, just specifying the provider in the segments under the
```

```
NETWORKING section is enough.
# Use phys_prov as physical_network name when creating a provider network
```

Ensure that you include the PROVIDER_VLAN_RANGES information in the *setup_data* as given in the following syntax:

```
PROVIDER_VLAN_RANGES: <a,b:c,d:e>, where the VLAN ranges can be a continuous range or comma separated
discontinuous range.
```


When creating an external or provider network, use physical_network=phys_ext (need to be specified) or physical_network=phys_prov (need to be specified), respectively.

The JUMBO_MTU functionality is available only for OVS over VLAN in a UCS B-Series pod. In a VLAN setup, by default, the MTU size is set to 1500 (1450 for VXLAN) and 8972 bytes. When JUMBO_MTU is enabled (with 28 bytes left for the header), the VLAN MTU is 9000 and VXLAN is 8950.

VPP VLAN

VPP VLAN

If you are installing Cisco VIM with VPP/VLAN, the mechanism driver in the setup_yaml file should reflect the same.

Cisco VPP/VLAN Mechanism Driver Configuration

```
MECHANISM_DRIVERS: vpp
TENANT_NETWORK_TYPES: "VLAN"
TENANT_VLAN_RANGES: <START>:<END># arbitrary VLAN range***
NFV_HOSTS: ALL
NR_RESERVED_VSWITCH_PCORES: <int> #Optional, defaults to 2. Values in the range 2 to 4 to increase performance
by allocating more cores to VPP
```

Cisco VTS Mechanism

Cisco VTS Mechanism

If you are installing Cisco VIM with Cisco VTS, you must enter the Cisco VTS parameters in Cisco VIM **setup_data.yaml** file.

Cisco VTS Driver Configuration

```
MECHANISM_DRIVERS: vts
TENANT_NETWORK_TYPES: "VLAN"
TENANT_VLAN_RANGES: <START>:<END> # arbitrary VLAN range***
ENABLE_JUMBO_FRAMES: True
```


VLAN range overlap on the physical network can occur if a hardware VTEP is configured on a top of rack (ToR) switch, where VTEPs are Virtual Extensible Local Area Network (VXLAN) tunnel end points.

NFV Parameters

```
NFV_HOSTS: ALL

# Only enabled when NFV_HOSTS
is set to ALL ##########################################

## Only 2 Values allowed is:
2M or 1G (defaults to 2M) #VM_HUGEPAGE_SIZE: 2M or 1G

Along with supporting it globally,Cisco VIM also supports VM_HUGEPAGE_SIZE on a per server basis with OVS/vts
/vpp/aci
as mechanism driver.

SERVERS:

compute-server-1:
VM_HUGEPAGE_SIZE: <2M or 1G> # <== optional

## Percentage of huge pages assigned to VM

## On NFV_HOSTS enabled hosts, VM memory can be a combination of regular pages and huge ## pages. This setting
sets
the ratio. By default, all VM memories (100%) have huge pages.


## Only input of type integer is allowed, in the range of 0-100 (including 0 and 100)
# values < 100 is only supported for mechanism driver of openvswitch or ACI
#VM_HUGEPAGE_PERCENTAGE: 100


Along with supporting it globally, Cisco VIM also supports VM_HUGEPAGE_PERCENTAGE on a per server basis with
OVS/ACI as mechanism driver.

SERVERS:
compute-server-1:

VM_HUGEPAGE_PERCENTAGE: <0 to 100> # <== optional, only for
mechanism driver openvswitch/aci
```

If you use a huge page, the memory used in the flavor must be exact multiples of the huge page sizes. For example, memory must be multiple of 2 if 2M huge page is used, and multiple of 1024 if 1G huge page is used.

VMTP Parameters

```
VMTP_VALIDATION parameters: #Required if vmtp is enabled VMTP_VALIDATION:
VTS_NET:#Required if VMTP is enabled for VTS (for VTS only this block is needed)

ENABLED: <true or false>
```

Networking Parameters

```
NETWORKING:
 ...
 networks:
 ...-
 vlan_id: <VLAN to carry VTS tenant traffic># required for VTS
 subnet: <subnet IP cidr>
 gateway: <tenant GW IP>
 pool:"<begin tenant IP> to <end tenant IP>"# ***
 segments:
 -tenant
```

The tenant network pool size has to take into account the IP addresses that are statically assigned through the VTS VTSR VM bootstrap configuration. For more information, see Cisco VTS.

Cisco VTS Parameters

```
VTS_PARAMETERS:
VTS_USERNAME: 'admin'                  # Required to be 'admin'
VTS_PASSWORD: <VTC UI password>
VTS_NCS_IP:   <VTC mx-net IP>          # VTC mx-net VIP for VTC HA (cannot be in mx-net pool range)
VTS_SITE_UUID: <VTS site uuid>          # VTS SITE UUID mandatory VTS parameter (Unique Pod UUID to indicate
                                          which pod the VTS is controlling)
VTC_SSH_USERNAME: '<vtc_ssh_username>' # Required parameter when VTS Day0 is enabled or running VMTP
VTC_SSH_PASSWORD: '<vtc_ssh_password>' # Required parameter when VTS Day0 is enabled or running VMTP

VTS_Day0_PARAMETERS:
VTS_2.5 mandates the VTC inventory generation and day0 configuration for VTF's to register.
without VTS_DAY0 the cloud is not operational as VTF does not register to VTC. Hence all cloud operations fail.
This is a boolean variable set as True or False. If set True, VTC day0 can be configured by the Cisco VIM
Installer.
By default values is 'False', i.e. if VTS_DAY0 is not set, the orchestrator sets it internally to 'False'
VTS_DAY0: '<True|False>'

## Optional, BGP_ASN:
   BGP_ASN: int  # Optional, min=1, max=65535;   if it is not defined, the default to 23
## Optional, MANAGED:
   MANAGED : <TRUE OR FALSE> #Optional; if it is true, tor_info in SERVERS becomes mandatory, CONFIGURE_TORS
under
                                  TORSWITCHINFO should be false and VTS deployment mode is managed.
```

For mx-net IP pool configuration, you must consider the IP addresses that are allocated to the VTC (VTS_NCS_IP). For more information, see Cisco VTS.

NFV Host

NFV Host

NFV host configuration describes how to configure NFV hosts and Cisco VIM monitoring.

Cisco VIM supports CPU pinning and huge page on the compute nodes. To enable non-uniform memory access (NUMA), you can use ALL (case insensitive) to configure all compute nodes. For VTS and VPP/VLAN, only the value of ALL is allowed. For OVS/VLAN, alternatively, you can list the compute nodes where NUMA must be enabled.

```
# For VPP and VTS, only
NFV_HOSTS: ALL is allowed NFV_HOSTS: ALL
or
NFV_HOSTS: ['compute-server-1']
```

By default, hyper-threading is enabled across compute nodes in Cisco VIM. Based on certain VNF characteristics, you can disable hyper-threading across the pod on day-0. You can also disable it on a single compute node on day-n, by updating the setup_data and removing or adding compute nodes. To disable hyper-threading, update the setup_data with the following name or value pair before starting the installation.

```
DISABLE_HYPERTHREADING: True or False; this is optional and default value is false
```

Supporting RMA for Auto-ToR

Supporting Return Merchandise Authorization for Auto-ToR

When Cisco VIM cloud uses auto-ToR configuration to manage switch ports, you need to replace the existing switches if one malfunctions.

Consider the following assumptions made during RMA of ToR with auto-ToR configuration:

- When a switch is getting RMAed, it is in a virtual port-channel (vPC) mode with another switch to support full switch redundancy.
- You can replace multiple switches through Cisco VIM CLI, but only one switch from each pair.
- Administrator is responsible for manual configuration of the spine connection and L3 Out for the ToR.

When replacing the ToR, ensure that you use same server ports to have minimal changes in the setup_data. Also, ensure that the new ToR name is same as the one that you are replacing.

To initiate ToR RMA, take a backup of the setupdata file and update it manually with the configuration details by running the following command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/  update the setup_data to include the
changes associated to the ToR that needs to be RMAs
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml -rma_tors <"," separated target
ToRs>
```

Optional Services

Optional Services

Heat, Ceilometer, LBaaS

Heat, Ceilometer, and LBaaS Support

Heat Support

OpenStack Heat is an orchestration service that allows you to spin up multiple instances, logical networks, and other cloud services in an automated fashion. To enable Heat, add the following in the *setup_data.yaml*.

```
# Optional Services:
OPTIONAL_SERVICE_LIST:
-  heat
```

To disable heat, remove the Optional Services section from the *setup_data.yaml* file.

> ⚠ Auto-scaling is not supported in Cisco VIM.

Ceilometer Support

The reference implementation of ceilometer is available from Cisco VIM 3.0.0 onwards. The ceilometer service can be brought in as a Day 0 option for fullon pod. To enable this service, update the *setup_data.yaml* with the following:

```
#Optional Services:
OPTIONAL_SERVICE_LIST:
- ceilometer
```

> ⚠ Ceilometer is enabled, when the pod type is fullon.

Load Balancer as a Service (LBaaS) Support

The reference implementation of LBaaS is available from the release Cisco VIM 3.2.2 onwards. The *lbaas* service is available as a Day 0 option. To enable this service, update the *setup_data.yaml* with the following:

```
Optional Services:
 OPTIONAL_SERVICE_LIST:
- lbaas
```

TAAS Support

TAAS Support

Overview

Cisco VIM 3.4.1 supports Tap As a Server (TAAS) with Open vSwitch (OVS) as the mechanism driver. You can enable the TAAS service in CVIM as a Day 0 or Day 2 option.

To enable this service, update the **setup_data.yaml** file with the following information:

```
# Optional Services:
OPTIONAL_SERVICE_LIST:
-        taas
```

There are additional configurations that need to be set at the infrastructure level to enable TAAS. For example, the gateway information of the tenant network must be set as the virtual IP in the HSRP configuration on the ToR.

Setting up Remote TAAS OVS

You must perform the following steps to set up a remote TAAS OVS, where traffic is mirrored from the pod VM to a destination outside the pod:

1. Create a GRE network and subnet in OpenStack with the destination address of the mirrored traffic.
   The network provider segment (GRE ID) must be more than 5000.

   ```
   # openstack network create --provider-network-type gre --provider-segment 5001 mirror_gre_network
   # openstack subnet create --network mirror_gre_network  --subnet-range 14.14.14.0/24 mirror_gre_subnet
   ```

2. Create a port for the GRE network with the IP address of the destination of the mirrored traffic.
   The configured IP address must be reachable from the TORs default gateway address of the tenant network.

   ```
   # openstack port create --network mirror_gre_network --fixed-ip subnet=mirror_gre_subnet,
   ip-address=14.14.14.14 mirror_gre__remote_port
   ```

3. Check the route towards the GRE termination point on both TORs:

   ```
   # sh ip route 14.14.14.14
   IP Route Table for VRF "default"
   '*' denotes best ucast next-hop
   '**' denotes best mcast next-hop
   '[x/y]' denotes [preference/metric]
   '%<string>' in via output denotes VRF <string>
   14.14.14.0/24, ubest/mbest: 1/0
   *via 11.11.11.6, [1/0], 1d01h, static
   ```

4. Check ping towards GRE termination point on both TORs:

   ```
   # ping 14.14.14.14
   PING 14.14.14.14 (14.14.14.14): 56 data bytes
   64 bytes from 14.14.14.14: icmp_seq=0 ttl=63 time=0.7 ms
   ```

5. Ensure that the source VM and its ports are active:

   ```
   # openstack server list -f value c33c38b6-48da-42eb-aeb9-9fac58f0a4c0
   server_dst ACTIVE network_destination=20.20.20.7 RHEL-guest-image m1.small
   # openstack port list -f value 0b7c731c-9193-4c58-aadf-102cc5b67cd6 fa:16:3e:9e:6d:d9
   ip_address='10.10.10.4', subnet_id='fca8955f-7de4-46d7-8cc2-89e1cafb530b' ACTIVE
   ```

6. Create the tap-service using the **neutron tap-service-create --port remote_gre_port_id** command.

```
neutron tap-service-create --port c0f4d618-6f09-40aa-9667-0eeeea1a710d --name remote_destination
```

7. Create tap-flow using the **neutron tap-flow-create --port mirrored_VM_port_id --tap-service tap_service_id --direction both** command.

```
neutron tap-flow-create --port 0b7c731c-9193-4c58-aadf-102cc5b67cd6
--tap-service 7e0f7976-b31c-459e-a2b8-2bc698961eb2 --direction both --name source1_to_remote_destination1
```

8. Check **ping** to or from the source VM.

   ⚠ VM should be up and running before traffic mirroring starts.

   On the mirrored VM, use the **ping** command as shown in the example below:

```
ping 192.168.1.1 -I ethX
```

9. Start traffic capture on the mirroring destination point and check if the mirrored traffic has been received.
   On remote gre termination point, execute the following command:

```
tcpdump -enni eth0 proto 47
```

Setting up Local TaaS OVS

You must perform the following steps to set up a local TAAS OVS, where traffic is mirrored from one VM to another VM inside the pod:

1. Ensure that the mirroring traffic source and destination VMs and their ports are active.

```
# openstack server list -f value c33c38b6-48da-42eb-aeb9-9fac58f0a4c0 server_dst ACTIVE
network_destination=20.20.20.7 RHEL-guest-image m1.small
491d11b3-a204-4b90-b843-87d76c33656f server_src ACTIVE network_source=10.10.10.4 RHEL-guest-image m1.
small
# openstack port list -f value 0b7c731c-9193-4c58-aadf-102cc5b67cd6 fa:16:3e:9e:6d:d9
ip_address='10.10.10.4',
subnet_id='fca8955f-7de4-46d7-8cc2-89e1cafb530b' ACTIVE f46be971-3ac3-49f0-bcbf-5018c74280f2 fa:16:3e:43:
46:da
ip_address='20.20.20.7', subnet_id='a5044731-b9b5-44c8-8f6f-ae4937e49d52' ACTIVE
```

   ⚠ Mirroring traffic source and destination VMs can belong to different networks.

2. Create a tap-service using the **neutron tap-service-create --port destination_VM_port_id** command.

```
neutron tap-service-create --port c0f4d618-6f09-40aa-9667-0eeeea1a710d --name remote_destination
```

3. Create a tap-flow using the **neutron tap-flow-create -port source_VM_port_id -tap-service tap_service_id --direction both** command.

```
neutron tap-flow-create --port 0b7c731c-9193-4c58-aadf-102cc5b67cd6 --tap-service 7e0f7976-b31c-459e-
a2b8-2bc698961eb2 --direction both --name source1_to_remote_destination1
```

4. Check **ping** to or from source VM. On a mirrored VM, use the **ping** command.

```
ping 192.168.1.1 -I ethX
```

5. Start traffic capture on the mirroring destination VM and check if the mirrored traffic has been received.

Ironic Support

Ironic Support

Overview

The reference implementation of ironic is available for Cisco VIM. You can implement the ironic service as a Day 0 or a reconfigure option. You can not disable this service after you enable it.

Ironic support is available only on Cisco UCS C M4 and M5 baremetal servers when Cisco VIM is deployed with OVS or VPP as the mechanism driver. You can use only Nexus 9K as the ToR for Cisco VIM with the ironic service. The ironic interface on the bare metal servers for OpenStack can either be an MLOM interface or the onboard LOM port. Cisco VIM with the ironic service supports only the configuration of a single interface on the baremetal server. This interface can be one of the above-mentioned ports, or if you want to bond ports, Cisco VIM configures an available bond 0 interface on the user deployed image.

Cisco VIM supports the bonding of MLOM or onboard LOM ports from Release 3.4.1. You must deploy the ToR used for Ironic service in the Nexus mode.

You must have one separate network segment that is used for ironic management and ironic inspector. The inspector is a service used to automate the creation of the OpenStack baremetal port with a switch interface, for example, eth 1/39 and MAC address information of both the switch MAC and server interface MAC apart from automatically adding the deploy image information to the ironic node.
You must ensure that the ironic management, ironic inspector, Cisco VIM management, and ironic CIMC networks are routed to each other.

The Cisco VIM management must be able to reach:

- Ironic management network and vice-versa
- CIMC network of the ironic nodes so that the Cisco VIM controller servers can directly reach the CIMC IP of the ironic servers.

To enable network reachability:

- All three networks such as Cisco VIM management, Ironic management, and CIMC must be private networks with SVI interfaces on the ToR.
- You must deploy a routed network for all three network segments. In this case, Cisco VIM does not require SVI interfaces on the ToR.

> ⚠ It is mandatory to include the ironic management or ironic inspector VLANs on the ToR interfaces connected to all the mercury controller servers. You must manually configure this setting if the Cisco VIM auto-ToR feature is not enabled.

Deploying Ironic

Follow the below steps for ironic deployment, before installing Cisco VIM:

1. Create a separate **ironic_inventory.yaml** with CIMC or IPMI details of the servers to be used as ironic baremetals. If you want to bond interfaces on the baremetal server, ensure that you configure the corresponding portgroups field with information about the interfaces. For example, you can refer:

   ```
   /root/installer-XXX/openstack-configs/ironic_inventory.yaml
   ```

   Save this file with your ironic server details in **/root/installer-XXX/openstack-configs/ironic_inventory.yaml.**
2. Specify the ironic management or ironic inspector VLAN in all control interfaces of the mercury controller servers, if Cisco VIM auto-ToR feature is not enabled. This configuration is required to perform ironic introspection to transfer the images from the controller to the baremetal server.
3. If you deploy ironic in the Nexus mode of ToR and you do not want to bond interfaces, you must manually configure the ToR interface connected to the server. Ensure that no existing configuration exists on the interface of the ToR connected to the baremetal. The interface must be in ACCESS mode. You must set only the ironic inspector VLAN as the access VLAN. If you configure portgroups in the **ironic_inventory.yaml** file to enable bonding, you do not have to manually configure the ToR as Cisco VIM configures it.
4. If you deploy ironic in an ACI mode testbed, you must ensure that ironic management network VLAN and all the tenant VLANs from setup_data are configured on the interface of the ToR connected to the baremetal the ironic inspector VLAN. The interface is in TRUNK mode. You need to set the ironic inspector network as the native VLAN.
5. Verify if the following configurations are done in the baremetal server CIMC before proceeding:

   - Check if IPMI connections are allowed over LAN.
   - In the BIOS configured boot order, only PXE boot is present and available as the first option. If the deployment is over MLOM, you must set the bootorder slot as MLOM. If you use the onboard NIC, you must set the slot as L.
   - PXE is enabled in VNIC adapters if VNICs are used as the interface for ironic. You can skip this step if you deploy ironic on the onboard LOM interface.
   - Set the VLAN mode on the VNIC used as TRUNK, if VNICs are used as the interface for ironic. You can skip this step if you deploy ironic on the onboard LOM interface.

- Turn on the baremetal node to access all parameters of CIMC. Cisco VIM installer verifies the node at step 1.
- Ensure that the Cisco UCS servers used as baremetal nodes have a RAID controller card and that a virtual raid has been created. All hard disks must be set in online or JBOD mode.

- Disable LLDP on Cisco VIC adaptor of all the servers used for ironic by executing the following steps and rebooting the server:

```
sh admin@X.X.X.X (CIMC IP)
C240-FCH1832V1HW# scope chassis
C240-FCH1832V1HW /chassis # show adapter
C240-FCH1832V1HW /chassis # scope adapter <PCI slot>
C240-FCH1832V1HW /chassis/adapter # set lldp disabled
C240-FCH1832V1HW*# commit
C240-FCH1832V1HW /chassis/adapter # show detail <To Verify LLDP is disabled>
```

To enable this service, update the **setup_data.yaml** file with the following configuration:

```
# Optional Services:
OPTIONAL_SERVICE_LIST:
-        ironic

IRONIC:
IRONIC_SWITCHDETAILS: # list of switches off which the ironic servers are hanging. This is mainly
used to provide ironic switch details to neutron
-        {hostname: <switch_name>, password: <password>, ssh_ip: <ssh_ip>, username:
<switch_admin_username>, switch_type: <"Nexus", "ACI", or "BypassNeutron">}


NETWORKING:
......
-        gateway: <gateway_information> # Mandatory if ironic is present pool: [<ip_add_start_1 to
ip_add_end_2>]
segments:  [ironic] subnet: <subnet with/mask>
vlan_id: <unique vlan id across the pod>
inspector_pool: [ip_add_3 to ip_add_4, ip_add_5 to ip_add_6, ip_add_7 to ip_add_8] (# of entry
pool : 3, same network as ironic but doesn't overlap with the pool of IPs defined
in the ironic segment)
# alternate format for pool (# of entry pool : 3)
-        ip_add_3 to ip_add_4
-        ip_add_5 to ip_add_6
-        ip_add_7 to ip_add_8
```

Container Support

Container Support

Overview

Cisco VIM supports VM, baremetal, or container-based workloads. To support the container-based workloads, Cisco VIM hosts Cisco Container Platform as an application. The orchestrator creates a common OpenStack tenant and deploys the Cisco Container Platform control plane on it. The orchestrator can also create a tenant cluster if needed.

The Kubernetes clusters deployed are multi-master clusters with three master nodes and N worker nodes. The Cisco Container Platform control plane consists of three masters and three workers. The master and worker nodes run as VMs on OpenStack.

Assumptions to Enable Cisco Container Platform on Cisco VIM

- Cisco VIM is up and running on the pod.
- Cisco Container Platform is deployed during Day 0 or Day 2 as part of reconfiguration.
- Cisco Container Platform workload runs as an OpenStack tenant.
- Cisco Container Platform control plane VMs and all tenant cluster VMs are up and running.
- A user must pre-exist for the OpenStack tenant where Cisco Container Platform can run.
- The virtual IP (VIP) for the Cisco Container Platform Installer is either a provider or a floating IP address in the tenant.
- SSH key in tenant has SSH access to the Cisco Container Platform control plane VMs.
- Cisco Container Platform is run on a floating IP address-based or a provider-based environment:
    - If the Cisco Container Platform is running on a floating IP address-based environment, managed L3 connectivity is used for networking. A public external network is used to host a minimum of 10 floating IP addresses.
    - If the Cisco Container Platform is running on a provider network, managed L3 connectivity is not used for networking. A public provider network is used for connecting to hosts and load balancers. A minimum of 20 IP addresses is required.

Prerequisites for Installing Cisco Container Platform

- Use the installer in the VM of Cisco VIM to create a new OpenStack tenant and to deploy the Cisco Container Platform control plane. You can use the control plane API to create multiple tenant clusters.
- Use the Calico network plugin as an overlay.
- For persistent storage, use Cinder as the storage provider. When a Kubernetes-based workload request is received for a persistent volume, dynamic persistent storage is automatically created.
- The external TLS must be enabled in the cloud via external_lb_vip_tls being set to True.
- In a dual stack environment, Cisco Container Platform over IPv6 is only supported.
- For Cisco Container Platform over IPv6, ensure that ENABLE_ESC_PRIV is set to True on Day 0 or via reconfiguration option.
- Ensure that LBaaS is enabled in the optional_service_list. If LBaaS is not enabled, follow these steps:

    a. Update the *setup_data.yaml* file to include LBaaS.

    ```
    OPTIONAL_SERVICE_LIST: [heat, lbaas]
    ```

    b. Run the following command:

    ```
    ciscovm reconfigure --setupfile <path to new setupfile containing lbass>;
    ```

Installing Cisco Container Platform

Follow these steps to install Cisco Container Platform on Cisco VIM:

1. Generate a ssh key of ecdsa type using the command:

    ```
    # ssh-keygen -f /root/ecdsa-key -t ecdsa -b 521 (Press Enter till keys are generated)
    ```

2. Download the tenant and installer images from the following link:
   https://software.cisco.com/download/redirect?config=f174642094aaf0e227b898e07fbb9d39
3. Establish the networking type (tenant or provider), based on which the CCP_DEPLOYMENT section is defined in the setup_data.

4. Update the *setup_data.yaml* with the following information. Ensure that you configure the items that are needed for the tenant or provider network environment.

```
CCP_DEPLOYMENT: # Parameters for CCP Deployment Optional services LBAAS mandatory
CCP_CONTROL: # Installer creates a new tenant in Openstack based on below information and set all quotas
in that tenant
UI_PASSWORD: <UI_PASSWORD> # password for CCP UI (required)
ccp_subnet_cidr: <ip_address/mask> # subnet to create to deploy CCP control plane
(required for tenant network should be removed for provider network)
installer_subnet_cidr: <ip_address/mask> # subnet to create for bootstrap installer
(required for tenant network should be removed for provider network)
installer_subnet_gw: <ip_address> # gateway to use for bootstrap installer (required for tenant network
should be removed for provider network)
password: <password> # password for the Openstack tenant (required)
private_key: <absolute path for ed25519 based key> # private key to be used to SSH
to VM must be ed25519 (required)
project_name: <tenant_name> # Tenant name to create for CCP control Plane installer will create this
Openstack tenant (required)
public_key: <absolute path for ed25519 based public key> # Public key for CCP VMs,
e.g. /root/ecdsa-key.pub
username: <string> # username for the CCP control plane tenant (required)
CCP_INSTALLER_IMAGE: <qcow2 absolute image path> # Pointer to the CCP Installer image (required)
CCP_TENANT: # Test only option not supported in production to create demo tenant cluster using CCP API
(Optional NA in production)
password: <password> # password for tenant (required)
project_name: <project_name> # tenant name to create in Openstack to host tenant cluster (required)
username: <username> # username for openstack tenant (required)
workers: 1 # no of kubernetes workers in tenant cluster (required)
subnet_cidr: <ip_address/mask> # tenant subnet CIDR
CCP_TENANT_IMAGE: <qcow based abs path of tenant cluster image> # Pointer to CCP tenant cluster image
(required)
DNS_SERVER: [list of length 1 for DNS servers] # DNS server to be reachable from cloud(required) Based
on CCP over IPv4 or IPv6, DNS_SERVER input has to be of the same type
KUBE_VERSION: <x.y.z> # Version of Kubernetes to install (required) normally can be deciphered from
tenant image name; e.g. 2.3.4
NETWORK_TYPE: <tenant or provider> # Network Type valid values provider or tenant network (required)
POD_CIDR: <ip_address/mask> # POD CIDR to use for calico network optional if not to be changed
(optional); Mandatory for IPv6, and is of IPv6 address if CCP needs to run over IPv6. For CCP based off
IPv6, only IPv6 based CCP cluster is allowed; CCP over IPv6 is only allowed for mechanism driver of
openvswitch; Also, for
CCP over IPv6, DNS_SERVER is of type IPv6 and ENABLE_ESC_PRIV must be true.

PUBLIC_NETWORK_UUID: <UUID of Openstack external network or provider network; Fake UUID incase of Day-0
Install > (optional initially but mandatory when ccp is being run)
CCP_FLAVOR: <flavor> optional initially, but mandatory when NFV_HOSTS is enabled during ccp installation.
```

5. To enable Cisco Container Platform on Cisco VIM on Day 0, update the *setup_data.yaml* file to include the CCP_DEPLOYMENT section and execute the standard ciscovim install command.
   After the installation, update the PUBLIC_NETWORK_UUID from the output of neutron net-list after sourcing openrc from */root/openstack-configs* and CCP_FLAVOR.

   ⚠ CCP install with NO DHCP on provider network is not supported.

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# # update the setup_data to update the PUBLIC_NETWORK_UUID and CCP_FLAVOR information
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ccp install --setupfile /root/MyDir/setup_data.yaml
```

6. Install Cisco Container Platform:

```
# ciscovim ccp install --setupfile <path_to_setup_file>
```

7. After the installation is done, execute the following command to see Cisco Container Platform control plane login URL information:

```
# ciscovim ccp show
```

8. You can login to the Cisco Container Platform control plane UI with the credentials provided in the *setup_data.yaml* file. Username defaults to admin and password is available in the setupdata UI_PASSWORD.

> ⚠ Running subsequent Cisco Container Platform install operation is not supported. You need to run the cleanup before running the installation again. The only operation allowed post-installation is *ccp verify*.

9. To initiate Cisco Container Platform verification, use the following command

```
# ciscovim ccp verify
```

10. To initiate Cisco Container Platform upgrade, enter the command:

```
# ciscovim ccp upgrade -setupfile /<PATH TO SETUPFILE>
```

> ⚠ As the Cisco Container Platform upgrade preserves installation and verification status, you can check them after executing **ciscovim ccp show** command. The only operation allowed after Cisco Container Platform upgrade is verify and cleanup.

11. Copy the original setupfile from openstack-configs and remove the Cisco Container Platform section, and then execute Cisco Container Platform cleanup of control cluster using the following command. This initiates cleaning of the control cluster and deletes the instances, project and users that were created as a part of Cisco Container Platform installation.

```
# ciscovim ccp cleanup --delete-control -setupfile /<PATH TO SETUPFILE>
```

12. To verify the status of the Cisco Container Platform cluster, use the command:

```
ciscovim ccp show
```

By default, all logs are dumped in the following directory /var/log/mercury/<random_uuid>.\
For example:

```
/var/log/mercury/7194a863-90aa-41ea-915e-2fb99d4d9b68/ccp_install_mon_jul__1_17:04:53_2019.log
```

Each operation on the Cisco Container Platform creates a new UUID. You can view the logs of that specific operation within UUID. You can execute the **`ciscovim last-run-status`** command post each operation, to check which log file got generated in the last operation that is executed on the Cisco Container Platform.

Ciscovim client (ciscovimclient) supports the following actions for Cisco Container Platform:

```
ciscovim help ccp
usage: ciscovim ccp [--delete-control] [-y] [--setupfile <setupdata_file>]
<install|upgrade|verify|cleanup|show>

Execute opertaions for CCP
Positional arguments:
<install|upgrade|verify|cleanup|show>
The control command to perform

Optional arguments:
--delete-control Destroy CCP Control Cluster.
-y, --yes Yes option to perform the action
--setupfile <setupdata_file> User setup_data.yaml required only for install, upgrade and cleanup.
```

Syntax Description of ciscovim

install	This operation executes control cluster deployment. (--setupfile is a mandatory argument that needs to be passed with install action).
verify	This operation executes tenant cluster deployment and removes the tenant cluster once completed.
cleanup	This operation removes the control cluster user and project from OpenStack. This also removes the control cluster as well.

upgrade	This operation upgrades the cluster with the latest images and kube version (if changed). The only keys allowed to modify with the upgrade are CCP INSTALLER IMAGE, CCP TENANT IMAGE AND KUBE VERSION.
	`Host queen`
	`HostName 172.29.84.114`
	`User root`

show	This operation lists down all the operations executed on Cisco Container Platform.

For more information on installing Cisco Container Platform, see https://www.cisco.com/c/en/us/support/cloud-systems-management/container-platform/products-installation-guides-list.html.

LDAP Support

LDAP Support

Overview

To continue enhancing the security portfolio and multi-tenancy with the use of domains, Keystone v3 support is now default in Cisco VIM 3.0.0. The OpenStack service authentication can be delegated to an external LDAP server, if the authorization is done by Keystone v3. To enable LDAP integration, the LDAP endpoint must be reachable from all the controller nodes that run OpenStack Keystone Identity Service. To benefit LDAP support with Keystone v3 feature, the setup_data must be augmented with the following information during the pod installation.

```
LDAP:

domain: <Domain specific name>

user_objectclass: <objectClass for Users> # e.g organizational Person
group_objectclass: <objectClass for Groups> # e.g. groupOfNames
user_tree_dn: '<DN tree for Users>' # e.g. 'ou=Users,dc=cisco,dc=com'
group_tree_dn: '<DN tree for Groups>' # e.g. 'ou=Groups,dc=cisco,dc=com'
suffix: '<suffix for DN>' # e.g. 'dc=cisco,dc=com'
url: '<ldap:// host:port>' # e.g. 'ldap://172.26.233.104:389'
user: '<DN of bind user>' # e.g.'dc=admin,dc=cisco,dc=com'
password: <password> # e.g. password of bind user
user_filter: '(memberOf=CN=os-users,OU=OS-Groups,DC=mercury,DC=local)' # Optional
user_id_attribute: sAMAccountName
user_name_attribute: sAMAccountName
user_mail_attribute: mail            #
Optional group_name_attribute: sAMAccountName
group_filter: '(&(objectClass=group)(|(cn=server-ops)(cn=admins)))' # Optional
group_member_attribute: memberUid  # Optional
group_id_attribute: gidNumber   # Optional
group_members_are_ids: True     # Optional
chase_referrals: <True or False>   # Optional
```

Conditions for LDAP user and password parameters:

- 1 – Can be optional (for group option).
- 2 – It must be mutually inclusive.
- 3 – If defined, it cannot be empty.

> ⚠ The parameter values may differ based on the directory service provider. For example: OpenLDAP or Microsoft Active Directory.

Integrating Identity with LDAP over TLS

The automation supports keystone integration with LDAP over TLS. To enable TLS, the CA root certificate must be presented as part of the **/root /openstack-configs/haproxy-ca.crt** file. The url parameter within the LDAP stanza must be set to *ldaps*.

url parameter supports the following format:

```
url: '<ldaps | ldap>://<FQDN | IP-Address>:[port]'
```

The protocol can be LDAP for non-SSL or LDAP if TLS is to be enabled.

The LDAP host can be a fully-qualified domain name (FQDN) or an IP address depending on how the SSL certificates are generated.

The port number is optional and if it is not provided it is assumed that the LDAP services are running on the default ports. For example: 389 for non-SSL and 636 for SSL. However, if these ports are not the default ports, then non-standard port numbers must be provided.

Support for Anonymous LDAP Bind

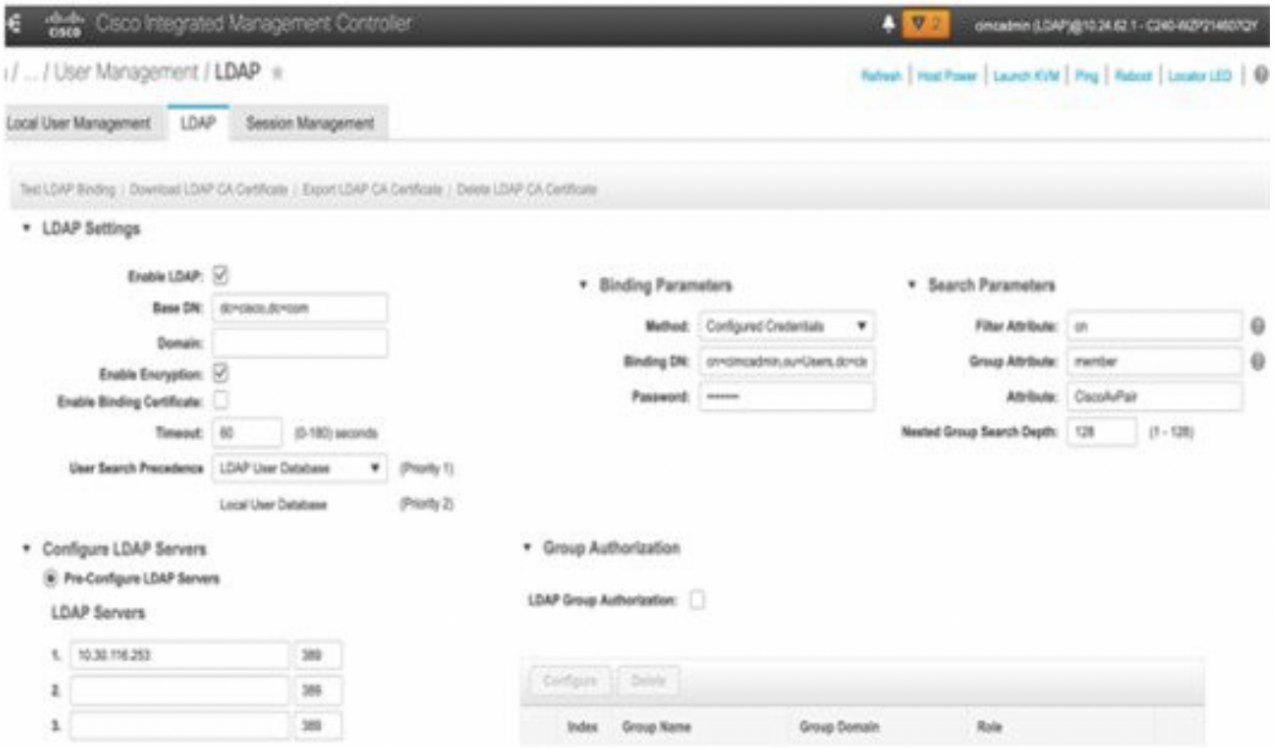
The automation provides support for anonymous simple bind where the LDAP configuration for a user representing the **bindDN** and **password** is optional and may not be provided.

> ⚠ Ensure that the LDAP server allows the clients to bind and search anonymously.

CIMC Authentication Using LDAP

Cisco VIM optionally supports the login of designated users into the CIMC using LDAP authentication. Enabling LDAP authentication for CIMC is a manual day-0 process and outside the scope of Cisco VIM automation. Once the LDAP authentication is setup, you must update the setup_data with the CIMC administration information that authenticates against LDAP, so that Cisco VIM works seamlessly.

The figure below is a snapshot of the CIMC configuration to authenticate using LDAP.



Baremetal Instances

Baremetal Instances

Launching OpenStack Baremetal Instances

You can use OpenStack Ironic service to launch baremetal instances once it is enabled through Cisco VIM.

1. Follow the pre-VIM deployment steps as given in the section Enabling Ironic Post Installation
2. Deploy VIM
3. After the deployment, run the following commands:

```
# openstack baremetal node list --> Once VIM installation is completed, the ironic node will move to
available state and
        is ready for use.
```

4. If you want to add more ironic nodes after VIM installation, execute the pre-VIM deployment steps and then add nodes. Use correct cimc credentials for $USER, $PASS, and $ADDRESS.

```
# openstack baremetal node create
--network-interface neutron --driver pxe_ipmitool
--name new-node-$ADDRESS \
--driver-info ipmi_username=$USER \
--driver-info ipmi_password=$PASS \
--driver-info ipmi_address=$ADDRESS
# openstack baremetal node manage $NODE_UUID
# openstack baremetal node inspect $NODE_UUID
```

5. Once inspection is completed, run the below commands:

```
openstack baremetal node show $NODE_UUID  to verify node's resources and capabilities set during inspection
process
openstack baremetal port list --> to verify ports. It should have one port of a baremetal node.
openstack baremetal node provide $NODE_UUID --> This PXE boots the deploy image via cleaning and sets node to
available
once done. Do this for all of the ironic nodes.
```

Deploying Baremetal Instances

Once the ironic nodes are available for use, you can launch an instance on the baremetal using the following steps:

1. Create the Nova baremetal flavor:

```
nova flavor-create my-baremetal-flavor auto $RAM_MB $DISK_GB $CPU
nova flavor-key my-baremetal-flavor set capabilities:boot_option="local"
nova flavor-key my-baremetal-flavor set capabilities:disk_label="gpt"
```

   The trait name should match with the baremetal node. Here, it is CUSTOM_BAREMETAL.

```
nova flavor-key my-baremetal-flavor set trait:CUSTOM_BAREMETAL=required
```

2. Add user images into glance. For example, if you are using ubuntu image, use the following commands:

```
IMAGE_OS=ubuntu
MY_VMLINUZ_UUID=$(glance image-create --name user-image-${IMAGE_OS}.vmlinuz --disk-format aki
--container-format aki < user-image-${IMAGE_OS}.vmlinuz | awk '/ id /{print $4}')
MY_INITRD_UUID=$(glance image-create --name user-image-${IMAGE_OS}.initrd --disk-format ari
--container-format ari < user-image-${IMAGE_OS}.initrd | awk '/ id /{print $4}')
```

```
glance image-create --name user-image-${IMAGE_OS}.qcow2 --disk-format qcow2 --container-format bare
--property kernel_id=$MY_VMLINUZ_UUID --property ramdisk_id=$MY_INITRD_UUID <
user-image-${IMAGE_OS}.qcow2
```

3. Use the following commands, to create the neutron tenant network to be used with the bare metal node:

```
# openstack network create my-tenant-net-name
# openstack subnet create --network my-tenant-net-name --subnet-range X.X.X.X/XX --ip-version 4
  my_tenant_subnet_name
```

4. Create a simple cloud-init script to log into the node after the instance is up:

   Example

```
#cloud-config
password: Lab1234!
chpasswd: { expire: False }
ssh_pwauth: True
```

   If this is an ACI or BypassNeutron mode testbed, add the following to the cloud-init script:
   Example

```
#cloud-config
password: Lab1234!
chpasswd: { expire: False }
ssh_pwauth: True
runcmd:
- ip link add link enp6s0 name enp6s0.3086 type vlan id <3086 - this will be the segment_id of your
tenant net>
- ip link set dev enp6s0.<3086> up
- dhclient enp6s0.<3086>
```

5. Boot the bare metal node using the below command:

```
# openstack server create --flavor <baremetal_flavor uuid> --image <centos/ubuntu image uuid> --nic
net-id=<tenant network uuid> --config-drive true --user-data user-data.txt <instance-name>
```


For the creation of host aggregates, do not include controller servers as part of the aggregate.

When ironic services are deployed, create a separate nova flavor for your VM instances. Do not use the above referenced baremetal flavor. When launching a VM instance, use the VM flavor. Additionally, update your VM flavor to contain the following condition :

```
# nova flavor-key <vm-flavor> set capabilities:hypervisor_type="s!= ironic"
```

VM Resizing and Migration

VM Resizing and Migration

VM Resizing

VM resize is the process of changing the flavor of an existing VM. Using VM resize, you can upscale a VM based on your needs. The size of a VM is indicated by the flavor, based on which the VM is launched.

Resizing an instance means using a different flavor for the instance. By default, the resizing process creates the newly sized instance on a new node, if more than one compute node exists and the resources are available. By default, the software allows you to change the RAM size, VDISK size, or VCPU count of an OpenStack instance using nova resize. Simultaneous or individual adjustment of properties for the target VM is allowed. If there is no suitable flavor for the new properties of the VM, you can create a new one.

```
nova resize [--poll] <server> <flavor>
```

The resize process takes some time as the VM boots up with the new specifications. For example, the Deploying a Cisco CSR (size in MB) would take approximately 60mins. After the resize process, execute `nova resize-confirm <server>` to overwrite the old VM image with the new one. If you face any issue, you can revert to the old VM using the `nova-resize-revert <server>` command. At this point, you can access the VM through SSH and verify whether the correct image is configured.

> ⚠ Ensure that you plan for a downtime as the OpenStack shutdowns the VM before resizing. Cisco recommends you not to resize a vdisk to a smaller value, as there is the risk of losing data.

VM Migration

Nova Migrate

The nova migrate command is used to move an instance from one compute host to another compute host. The scheduler chooses the destination compute host, based on the availability of the zone settings. This process does not assume that the instance has shared storage available on the target host.

To initiate the cold migration of the VM, you can execute the following command:

```
nova migrate [--poll] <server>
```

The VM migration can take a while, as the VM boots up with the new specifications. After the VM migration process, you can execute `nova resize-confirm <server> --` to overwrite the old VM image with the new one. If you encounter an problem, use the `nova-resize-revert <server>` command to revert to the old VM image. At this point, access the VM through SSH and verify the correct image is configured.

> ⚠ The OpenStack shutdown the VM before the migrate, so plan for a downtime.

Live Migrate

Live-migrating an instance means moving the virtual machine to a different OpenStack compute server while the instance is running. You can select the host to live migrate the instance. If the destination host is not selected, the nova scheduler chooses the destination compute based on the availability of the zone settings. You cannot use live-migration without shared storage except a booted from volume VM which does not have a local disk.

To initiate the live migration of the VM, you can execute the following command:

```
openstack server migrate <server>--live
```

The VM migration can take a while. The virtual machine status can be checked with the command:

```
openstack server show < server>
```

1. With NFV_HOST enabled, you must ensure that the vCPUs are available on the destination host to avoid collision. With cold migration, the vCPUs available on the destination host are automatically selected and assigned to the VM.
2. If you are trying to live-migrate a VM with config drive, it is always considered as cold-migration.
3. In VPP pod, live-migration is not supported as it uses huge pages by default.

Supported Integration

Supported Integration

NetApp Integration

NetApp Integration

Cisco VIM supports the integration of NetApp devices running ONTAP 9.X or higher. NetApp devices are used alternative to Ceph for block storage. Cisco VIM is integrated and tested with FAS2650 SKU of NetApp. Ensure that block storage information is not present while using NetApp devices.

> ⚠ NetApp is the backend for Nova, Cinder, and Glance services.

The integration of NetApp with Cisco VIM is based on the following assumptions:

- To avoid UUID collision, one-one mapping between a Cisco VIM pod and Storage Virtual Machine (SVM) is required.
- The installation and management of NetApp is outside the scope of Cisco VIM.
- The NetApp endpoint(s) defined in the *setup_data* must be reachable from the management network of Cisco VIM.
- As the Cinder volume, Nova VMs, and Glance images come from NetApp storage, create three distinct NFS volumes in NetApp.
- Create and set the respective export policies so that it is available to all clients.
- The volumes for Nova, Cinder, and Glance, must be created with user and group id of 2012, 2007, and 2008, respectively.
- The size of the volumes must be appropriate as per the usage.

To enable NetApp, update the *setup_data.yaml* file with the following code prior to the installation:

```
STORE_BACKEND: netapp   # for glance
VOLUME_DRIVER: netapp   # for cinder

######################################################
New NETAPP config section; no dedicated Ceph Allowed
######################################################

NETAPP:
  server_hostname: <ip of netapp management/API server>
  server_port: <port of netapp management/API server> 80 for HTTP 443 for https
  transport_type: http/https
  username: <username of netapp API server>
  password: <password of netapp API server>
  vserver: <SVM for cinder nfs volume>
  cinder_nfs_server: <data path ip of nfs server>
  cinder_nfs_path: <mount path>
  nova_nfs_server: <data path ip of nova nfs server>
  nova_nfs_path: <mount path nova nfs>
  glance_nfs_server: <data path of glance nfs server>
  glance_nfs_path: <mount path of glance nfs>
  netapp_cert_file: <root ca path for netapp cluster only if protocol is https>
```

For details on how to secure NetApp transport on Day 2, see NetApp from http to https.

Enabling SolidFire

Enabling SolidFire

Cisco VIM supports the automated integration with a customer-managed SolidFire cluster for a block-storage option. SolidFire supports Cinder service for backup of block-storage. The pre-deployed SolidFire cluster has two HA networks such as management network and storage network. The management network is on 1G interface with active/passive configuration for two ports, while the storage network is on 10G interface with active/active Link Aggregation Control Protocol (LACP) configuration.
It is recommended that the:

- Storage network of Cisco VIM is same as that of SolidFire.
- Management network of Solidfire is reachable from Cisco VIM control nodes.

SolidFire is available only as a Day 0 configuration.

To enable SolidFire, update the *setup_data.yaml* file with the following code prior to the installation.

```
SOLIDFIRE:
cluster_mvip: <management IP of SolidFire cluster> # must be reachable from the controller nodes
cluster_svip: <storage VIP on SolidFire cluster to be used by CVIM> # must be in Cisco VIM storage/management
network; recommended to have it in storage network for better performance
admin_username: <admin user on SolidFire cluster to be used by CVIM>
admin_password: <password for admin user defined above; password criteria is: "satisfy at least 3 of the
following conditions: " \ "at least 1 letter between a to z, " \ "at least 1 letter between A to Z, " \ "at
least 1 number between 0 to 9, " \  "at least 1 character from !$#@%^-_+=, " \
"AND password length is between 8 and 20 characters."
```

Enabling Zadara

Using Zadara

Overview

The Zadara Virtual Private Storage Array (VPSA) is a software-defined solution that is available as a Storage-as-a-Service with the storage servers residing in the customer premise and is also Layer 2 adjacent to the cloud. It is an elastic system that provides Enterprise-grade data protection and data management storage services.

Following are the key attributes:

- Enterprise quality, resilient, highly available, and consistent performance storage for the most demanding data center application workloads.
- Consumed as a Service - flexible, dynamic and billable.
- Scale out - to hundreds of storage nodes, thousands of drives, and multi-petabyte storage.
- True multi-tenancy - End-user controlled privacy and security. Separate workloads, resource allocation, and management per tenant such that each tenant truly experiences secure storage with no noisy neighbor.
- Universal storage - Supports all data services on one common infrastructure: Block, File, Object.

You can select Zadara as a backend for Cinder (block storage) and Glance (NFS), instead of Ceph. The use of Zadara helps in handling enterprise workloads, and provides a common infrastructure for all three storage types: Block, File, and Object.

Enabling Zadara in Cisco VIM is a Day 0 fresh Installation activity. In this case, the Cisco VIM cloud is a full-on cloud with Zadara as the backend for Glance and Cinder.

Prerequisites

- Zadara installation must be done ahead of time and is not the scope of Cisco VIM.
- Zadara pools for block storage and Glance images must be created ahead of time.
- For Glance image, a NAS volume must be pre-provisioned and a corresponding NFS export path must be provided in the *setup_data.yaml*
- The management network of Cisco VIM must reach the Zadara endpoint.
- The Fully Qualified Domain Name (FQDN) of the Virtual Private Storage Array (VPSA) *host_name* must be resolved to an IP address in the management network, but cannot be part of the management network pool.

Enabling Zadara

To enable Zadara in Cisco VIM:

1. Ensure that the block_storage section of Cisco VIM is absent.
2. Update the following in Cisco VIM setup_data:

```
ZADARA:
  access_key: <key to access vpsa end point in Zadara>
  vpsa_host: <fqdn of the vpsa host_name> # will resolve to an IP address in the management network;
cannot be part of the management network pool
  vpsa_poolname: <pool_name for vpsa>
  glance_nfs_name: <nfs name for glance>
  glance_nfs_path: <nfs path for glance>
```

> ⚠ Eliminates the need to configure a CA certificate in Cisco VIM, as the standard CA certificate bundle provided with the Linux distribution is sufficient and the matching certificate is pre-seeded to the Virtual Private Storage Array (VPSA).

> ⓘ Though Zadara needs to be enabled as a Day 0 option for security reason, you can change the Zadara *access_key* as a reconfigure option.

3. To update the *access_key,* the administrator must update the *setup_data.yaml* file with the commands listed below:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp/root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# cd /root/
```

```
[root@mgmt1 ~]# # update the setup_data with right access_key in the Zadara section
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

After the reconfiguration, you can see that the Zadara is back in use with the new *access_key.*

Enabling ACI

Enabling ACI

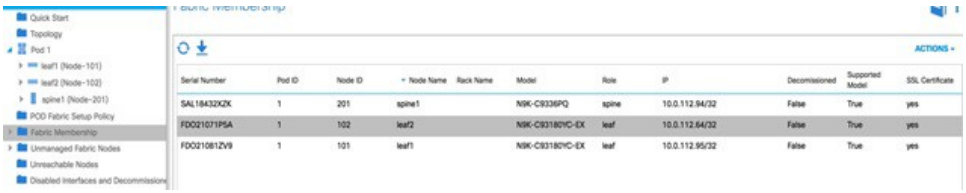
Overview

Cisco VIM integrates with ACI without the APIC plugin. Cisco VIM invokes the APIC APIs to pre-provision the right set of VLANs (along with the Day 0 aspects) on the corresponding server ports ahead of time, while supporting pod management operations

Assumptions

As Cisco VIM does the Day 0 configuration of the ACI, following are the assumptions that Cisco VIM makes for the integration to happen.

1. Before the Cisco VIM installation, the APIC 3.2 controllers running in a cluster of three must be installed and active.
2. All spine and leaf switches are booted in ACI mode and discovered under Fabric Inventory. The number of leaf switches cannot be changed after the initial installation.
3. The IP address should be assigned to each device from the TEP_ADDRESS_POOL.



4. Network must be designed such that the management node and controllers are reachable to APIC controllers.
5. Tunnel end point address pool (TEP_ADDRESS_POOL) is set to ACI default at 10.0.0.0/16. Ensure that this address space is not assigned in the cloud.
6. Multicast address pool is set to ACI default at 225.0.0.0/15. Ensure that this address space is not assigned anywhere in the cloud.
7. TEP_ADDRESS_POOL and multicast address pool are immutable for the lifecycle of the infrastructure.

> ⚠ Using Auto-ToR provisioning using APIC API, the port PV (port*VLAN) count in a given ACI Fabric domain is under the scale limits 10000 PV/ToR and 450000 PV/Fabric.

Additional Settings for Auto-ToR via ACI API on Day 0

When using the option of ToR automation via ACI API on Day 0 without the APIC plugin, FABRIC_INTERFACE_POLICIES (under SERVER_COMMON section) and vim_apic_network section are required. The FABRIC_INTERFACE_POLICIES include global fabric policies that are defined in APIC and to be applied to the relevant switch ports. Listed below is the definition of the same:

```
SERVER_COMMON:
...
FABRIC_INTERFACE_POLICIES:
#When configure_fabric is False
global:    # Global policies can be overridden per server role sriov_tor_info: # <only 1 policy for sriov
interface>
- <accportgrp-...>    # string, E.g. policy name starting with accportgrp-. Must be pre-provisioned and
mandatory.


#When configure_fabric is True
global:    # Global policies can be overridden per server role tor_info:    # <list of global fabric policies
for control plane>
1.     -<str>    # string, E.g. hintfpol-25G-On-RS-FEC. Must be pre-provisioned.
2.     -<str>    # string E.g cdpIfP-CdpDisable
dp_tor_info:    # <list of policies for data plane for Intel NIC>
3.     -<str>    # string, E.g. lacplagp-LacpActive. Must be pre-provisioned.
4.     -<str>    # string E.g lldpIfP-LldpEnable sriov_tor_info: # <list of policies for sriov interfaces>
5.    -<str>    # string, E.g. hintfpol-25G-On-RS-FEC. Must be pre-provisioned. control:    # Optional in case
needs to over-ridden. Must be one of the SERVER roles.
```

```
tor_info:    # <list of policies for control plane>
6.    -<str>    # string, E.g. hintfpol-25G-On-RS-FEC. Must be pre-provisioned. compute:    # Optional in case
needs to over-ridden. Must be one of the SERVER
roles.
dp_tor_info:    # <list of policies for data plane>
7.    -<str>    # string, E.g. hintfpol-25G-On-RS-FEC. Must be pre-provisioned.

# Pre-provision EPG/BD policies to be configured for management and tenant/provider EPGs (FHS policy)
EPG_POLICIES: # Goes by Network Segments and is entirely Optional
management:    # Optional, list of policy for management segment
       - <path_to_epg_policy>    # Must be pre-provisioned. tn-cvim-installer-tenant/trustctrlpol-Trust-DHCP-Sv.
provider:    # Optional, list of policy for provider segment
1.    - <path_to_epg_policy1>    # Must be pre-provisioned.
2.    - <path_to_epg_policy2>    # Must be pre-provisioned.
tenant:    # Optional, list of policy for tenant segment
3.    - <path_to_epg_policy1>    # Must be pre-provisioned.
4.    - <path_to_epg_policy2>    # Must be pre-provisioned.
In the vim_apic_networks section, the provider and tenant VLAN definitions are listed as below:

vim_apic_networks:
EPG_NAME: 'VL-%s-EPG' # required; pattern substituted with vlan_id

BD_NAME: 'VL-%s-BD'    # required; pattern substituted with vlan_id PROVIDER:
# Support static vlans with the following attributes defined (these vlans will only be referred to bind and
unbind Static Ports)
- app_profile: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core-AP'
EPG_NAME: <str>    # <optional string. Will prefix the pattern in the global EPG_NAME definition>
mode: <trunk|access>    # string, default trunk
tenant: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core' vlan_ids: '<3550>'    # Can be a
only a single id
config_type: pre-provisioned vlan_pools:
- <str-1>    # string E.g. 'Server-VlanPool'

# The "vlan_ids' can be a VLAN Range only for L2 networks provided they belong #to the same VLAN pool and EPGs
map to the same Phydom, App Profile, VRF
- vlan_ids: '<3550>'    # <Can be a single id or range and/or comma separated list>
EPG_NAME: <str>    # <optional string. Will prefix the pattern in the global EPG_NAME definition>
BD_NAME: <str>    # <optional string. Will prefix the pattern in the global BD_NAME definition>
vlan_pools:    # List of vlan pool names. Must be pre-provisioned in ACI POD
1.    <str-1>    # string E.g. 'Server-VlanPool'
2.    <str-2>    # string E.g. 'Ext-VlanPool'
phys_dom: <str>    # string. Must be pre-provisioned in ACI POD. E.g. Server-PhysDom
description: <str>    # optional; string. Must be pre-provisioned in ACI POD. E.g. 'provider net 3550'
tenant: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core' app_profile: <str>    # string, E.g.
Must be pre-provisioned in ACI POD. 'Core-AP' vrf: <str>    # string, E.g. Must be pre-provisioned in ACI POD.
'Core' subnets:    # List of subnets to be configured for the Bridge Domain
3.    scope: <str>    # string. Can be <'private'|'public'|'private,shared'>
4.    gateway_cidr:    # IPv4 or IPv6 network gateway with cidr E.g.
'240b:c010:101:2839::ffff/64'
      ctrl:  <no-default-gateway" or "nd" or "nd,no-default-gateway" or "no-default-gateway,nd" or "unspecified"
> # when gateway cidr is of type IPv6
        or
  ctrl:  <no-default-gateway" or "querier" or "querier,no-default-gateway" or "no-default-gateway,querier" or
"unspecified"> # when gateway cidr is of type IPv4

l3-out:    # optional, List of L3out External Routed Network Instances. Must be pre-provisioned
    -<External Routed Network/Instance Profile>    # E.g. Core-Ba-Ma-L3out/Core-Ba-Ma-ExtEPG
      -<External Routed Network/Instance Profile>    # E.g. ce1-epc-CP-L3out/ce1-epc-CP-ExtEPG mode:
trunk|access    # string, default trunk
       l2_unknown_unicast: <flood or proxy>
       limit_ip_learning: <true or false>
       preferred_group_member: <include or exclude>    # Optional, default is exclude
       arp_flood: <true or false>
       unicast_routing: <true or false>
       nd_policy: <true or false>      # When true, ensure that path/ndifpol is defined under SERVER_COMMON ->
EPG_POLICIES -> provider section

TENANT:
# Does not contain l3out
# Can be a VLAN Range only for L2 networks provided they belong to the # same VLAN pool and EPGs map to the
same Phydom, App Profile, VRF
```

```
- vlan_ids: '<2251:2260,2280,2290>'
EPG_NAME: <str>    # <optional string. Will prefix the pattern in the global EPG_NAME definition>
BD_NAME: <str>    # <optional string. Will prefix the pattern in the global BD_NAME definition>
vlan_pools:
5.    'Server-VlanPool' phys_dom: Server-PhysDom tenant: 'Core'
app_profile: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core-AP' vrf: Nokia-LI
mode: trunk
subnets:    # May contain a subnet in which case only valid value is a single vlan id
1.    scope: <str>    # string. Can be <'private'|'public'|'private,shared'> gateway_cidr:    # IPv4 or IPv6
network gateway with cidr E.g.
'240b:c010:101:2839::ffff/64'

    l2_unknown_unicast: <flood or proxy>
    limit_ip_learning: <true or false>
    preferred_group_member: <include or exclude>    # Optional, default is exclude
    arp_flood: <true or false>
    unicast_routing: <true or false>
    nd_policy: <true or false>  # When true, ensure that path/ndifpol is defined under SERVER_COMMON ->
EPG_POLICIES -> tenant section
```

In the vim_apic_networks section, the provider and tenant VLAN definitions are listed as below:

```
vim_apic_networks:
EPG_NAME: 'VL-%s-EPG' # required; pattern substituted with vlan_id

BD_NAME: 'VL-%s-BD'    # required; pattern substituted with vlan_id PROVIDER:
# Support static vlans with the following attributes defined (these vlans will only be referred to bind and
unbind Static Ports)
- app_profile: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core-AP'
EPG_NAME: <str>    # <optional string. Will prefix the pattern in the global EPG_NAME definition>
mode: <trunk|access>    # string, default trunk
tenant: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core' vlan_ids: '<3550>'    # Can be a
only a single id
config_type: pre-provisioned vlan_pools:
- <str-1>    # string E.g. 'Server-VlanPool'

# The "vlan_ids' can be a VLAN Range only for L2 networks provided they belong #to the same VLAN pool and EPGs
map to the same Phydom, App Profile, VRF
- vlan_ids: '<3550>'    # <Can be a single id or range and/or comma separated list>
EPG_NAME: <str>    # <optional string. Will prefix the pattern in the global EPG_NAME definition>
BD_NAME: <str>    # <optional string. Will prefix the pattern in the global BD_NAME definition>
vlan_pools:    # List of vlan pool names. Must be pre-provisioned in ACI POD
1.    <str-1>    # string E.g. 'Server-VlanPool'
2.    <str-2>    # string E.g. 'Ext-VlanPool'
phys_dom: <str>    # string. Must be pre-provisioned in ACI POD. E.g. Server-PhysDom
description: <str>    # optional; string. Must be pre-provisioned in ACI POD. E.g. 'provider net 3550'
tenant: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core' app_profile: <str>    # string, E.g.
Must be pre-provisioned in ACI POD. 'Core-AP' vrf: <str>    # string, E.g. Must be pre-provisioned in ACI POD.
'Core' subnets:    # List of subnets to be configured for the Bridge Domain
3.    scope: <str>    # string. Can be <'private'|'public'|'private,shared'>
4.    gateway_cidr:    # IPv4 or IPv6 network gateway with cidr E.g.
'240b:c010:101:2839::ffff/64'
      ctrl:  <no-default-gateway" or "nd" or "nd,no-default-gateway" or "no-default-gateway,nd" or "unspecified"
> # when gateway cidr is of type IPv6
        or
  ctrl:  <no-default-gateway" or "querier" or "querier,no-default-gateway" or "no-default-gateway,querier" or
"unspecified"> # when gateway cidr is of type IPv4

l3-out:    # optional, List of L3out External Routed Network Instances. Must be pre-provisioned
    -<External Routed Network/Instance Profile>    # E.g. Core-Ba-Ma-L3out/Core-Ba-Ma-ExtEPG
      -<External Routed Network/Instance Profile>    # E.g. ce1-epc-CP-L3out/ce1-epc-CP-ExtEPG mode:
trunk|access    # string, default trunk
       l2_unknown_unicast: <flood or proxy>
       limit_ip_learning: <true or false>
       preferred_group_member: <include or exclude>    # Optional, default is exclude
       arp_flood: <true or false>
       unicast_routing: <true or false>
       nd_policy: <true or false>      # When true, ensure that path/ndifpol is defined under SERVER_COMMON ->
EPG_POLICIES -> provider section
```

```
TENANT:
# Does not contain l3out
# Can be a VLAN Range only for L2 networks provided they belong to the # same VLAN pool and EPGs map to the
same Phydom, App Profile, VRF
- vlan_ids: '<2251:2260,2280,2290>'
EPG_NAME: <str>    # <optional string. Will prefix the pattern in the global EPG_NAME definition>
BD_NAME: <str>    # <optional string. Will prefix the pattern in the global BD_NAME definition>
vlan_pools:
5.    'Server-VlanPool' phys_dom: Server-PhysDom tenant: 'Core'
app_profile: <str>    # string, E.g. Must be pre-provisioned in ACI POD. 'Core-AP' vrf: Nokia-LI
mode: trunk
subnets:    # May contain a subnet in which case only valid value is a single vlan id
1.    scope: <str>    # string. Can be <'private'|'public'|'private,shared'> gateway_cidr:    # IPv4 or IPv6
network gateway with cidr E.g.
'240b:c010:101:2839::ffff/64'

    l2_unknown_unicast: <flood or proxy>
    limit_ip_learning: <true or false>
    preferred_group_member: <include or exclude>    # Optional, default is exclude
    arp_flood: <true or false>
    unicast_routing: <true or false>
    nd_policy: <true or false>  # When true, ensure that path/ndifpol is defined under SERVER_COMMON ->
EPG_POLICIES -> tenant section
```


Ensure that you update right VLAN information when using this option in context of APIC, during reconfiguration of VLANs.

Replacing ACI

Replacing ACI Controller

The Opflex ML2 plugin (in Unified mode) integrated with Cisco VIM manages the tenant VLANs dynamically, as VMs come and go in the cloud. In addition, we support an administrator driven automated workflow to provision the provider networks. This feature is supported on a C-series based Fullon or Micropod running with Cisco VIC 1227 and Intel NIC x710 with redundancy at NIC level. While the integration of ACI into Cisco VIM is a day-0 activity, Cisco VIM supports the replacement of the ACI controller in the ACI cluster and the expansion of the leaf switches to increase the fabric.

1. To update the setup_data, follow the below steps:

```
APICINFO:
apic_hosts: '<ip1|host1>:[port], <ip2|host2>:[port], <ip3|host3>:[port]'
# max of 3, min of 1, not 2; reconfigurable
Since the APIC manages the Leaf switches, its mandatory to define the new Leaf switches (in pairs)
in the following format:
TORSWITCHINFO: (mandatory)
SWITCHDETAILS:
::
-
hostname: <leaf-hostname-1>
vpc_peer_keepalive: <leaf-hostname-2>
vpc_domain: 1 # Must be unique across pairs
br_mgmt_port_info: 'eth1/27' # br_mgmt_* attributes must exist on at least one pair
br_mgmt_vlan_info: '3401'
node_id: <int> # unique across switches
-
hostname: <leaf-hostname-2>
vpc_peer_keepalive: <leaf-hostname-1>
vpc_domain: 1
br_mgmt_port_info: 'eth1/27' # br_mgmt_* attributes must exist on at least one pair
br_mgmt_vlan_info: '3401'
node_id: <int> # unique across switches
```

2. To initiate a change in ACI configuration on an existing pod, copy the setupdata into a local directory and update it manually with the relevant apic_hosts and/or new TORSWITCH information, and then run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/ [root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to include ACI info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

Updating APIC Parameters

Updating Cisco Application Policy Infrastructure Controller (APIC) Parameters

Updating APIC Hosts, Username, Password

With the ACI integration on Day 0, Cisco VIM supports the replacement of the APIC controller IP, username, and/or password of the APIC cluster. To initiate this change, update the relevant APIC attributes in *setup_data* as listed below:

```
APICINFO:
  apic_hosts: '<ip1|host1>:[port], <ip2|host2>:[port], <ip3|host3>:[port]' # max of 5, min of 1; reconfigurable
  apic_username: <apic_username>
  apic_password: <apic_password>
```

To update APIC configuration on an existing pod, copy the *setup_data* into a local directory and update it manually with the relevant apic_hosts IP, username, or password, and then run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to include new APIC info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

Updating Switch managed by APIC

With the ACI integration on Day 0, Cisco VIM supports the expansion of the leaf switches to increase the fabric in pairs. To initiate this change, update the relevant APIC attributes in *setup_data* as listed below:

```
Since the APIC manages the leaf switches, it is mandatory to define the new leaf switches (in pairs)
in the following format:
TORSWITCHINFO: (mandatory)
  SWITCHDETAILS:
  :         # Do not touch the existing ToR Pairs
  :
  :
  -
    hostname: <leaf-hostname-new1>
    vpc_peer_keepalive: <leaf-hostname-new2>
    vpc_domain: <int> # Must be unique across pairs
    node_id: <int> # unique across switches
  -
    hostname: <leaf-hostname-new2>
    vpc_peer_keepalive: <leaf-hostname-new1>
    vpc_domain: 1
    node_id: <int> # unique across switches
```

To add new ToR pairs in the TORSWITCH information section of an existing pod installed with ACI via Cisco VIM, copy the *setup_data* into a local directory, update it manually with the relevant SWITCHDETAILS in the TORSWITCHINFO section, and then run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to include new SWITCHDETAILS in pair)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

Red Hat IDM

Red Hat Identity Management System

Overview

Cisco VIM supports integration with RedHat Identity Management System (IDM) for Identity, Policy, Audit (IPA). The IPA solution helps in managing users and hosts and applying group-based policies using a centrally managed identity and authentication solution for linux hosts. You can enable this feature as a Day 0 or Day 1 activity. Multiple IPA servers with IPv4 and IPv6 endpoints are allowed for redundancy. When you enable IPA, you cannot enable the features of TTY_LOGGING and vim_ldap_admins.

For more information on IDM, see https://www.redhat.com/archives/rh-community-de-berlin/2012-November/pdfOlwXB8dm7U.pdf.

Assumptions

- IDM integration includes all hosts in a pod: management and cloud hosts in the cluster for any pod type.
- All operations are available only for an IPA client on the IPA client host.
- Any host management against the IPA server outside of enrollment and unenrollment from the IPA client is out of the scope of the automation.
- IPA client does not manage any users.
- Local root user access must not change.
- IPA servers can access all hosts through the management network.
- Certificates between the IPA server and hosts over the management network are not included.
- Hostname of all the servers (including the management node) in the pod are in FQDN with only lower cases (RFC4120).
- The servers' hostname including the management node must belong to the ipa_domain_name listed in the IPA_INFO section.

Integration of IPA for pods that use short hostnames (non-FQDN) is challenging when it is enabled as part of a reconfiguration operation. During the IPA registration of host clients, the IPA server updates the system hostname of the client to a hostname with FQDN. This breaks Cisco VIM operations such as cluster recovery where the hostnames defined in the *setup_data.yaml* file is used. Also, breakage exists in SRIOV mappings, and so on. Hence, it is recommended that the hostname of all servers in the pod, including the management node are in FQDN with only lower cases.

Enabling IDM on Day 0

To enable IDM, complete the following steps:

1. Add the following section with the configuration in the *setup_data.yaml* file and execute *ciscovim run:*

```
IPA_INFO:
  ipa_servers:
        - hostname: <fqdn_hostname in lower case belonging to ipa_domain_name>
        ipaddresses: # --- Optional
          - '<ipv4_address>'
          - '<ipv6_address>'
        - hostname: <fqdn hostname in lower case belonging to ipa_domain_name>
        ipaddresses: --- Optional
          - '<ipv4_address>'
          - '<ipv6_address>'
  enroller_user: <enroller_username>
  enroller_password: <enroller_password>
  ipa_domain_name: <ipa_domain_name>
```

2. To bring in this feature on Day 2, see Platform Security.

Supported Features

Supported Features

Platform Security

Platform Security

Enabling Custom Policy for VNF Manager Post Installation

During post-installation of a cloud, Cisco VIM helps to enable a VNF manager (such as ESC) to operate and manage tenant VMs in the OpenStack cloud, with additional privileged features.

Some of the VNF managers operate using specific OpenStack features that require the admin role.

Following are the steps to enable the custom policy for VNF Manager:

1. Take a backup of the setupdata file and update the file manually with the configuration below:

   ```
   ENABLE_ESC_PROV: True #Optional; By default, it is False.
   ```

2. Run the following reconfiguration commands:

   ```
   [root@mgmt1 ~]# cd /root/
   [root@mgmt1 ~]# mkdir MyDir
   [root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
   # update the setup_data to update the proxy info
   [root@mgmt1 ~]# cd /root/MyDir/
   [root@mgmt1 ~]# vi setup_data.yaml
   [root@mgmt1 ~]# cd ~/installer-xxxx
   [root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
   ```

Disabling Management Node Accessibility to Cloud API Network

Cisco VIM provides cloud connectivity verification from the data and control plane point of view using tools like cloud-sanity, VMTP, and NFVbench, which are typically run from the management node. For these tools to work, reachability to the Cloud API, external, and provider network is a must.

From release Cisco VIM 2.4.3 onwards, you can set the MGMTNODE_EXTAPI_REACH variable to True in the setup_data file to override the need to ensure reachability of management node from Cloud API, external, and provider network.

For example:

```
MGMTNODE_EXTAPI_REACH: True
```

By default, the MGMTNODE_EXTAPI_REACH variable is set to True. If you do not want to use the MGMTNODE_EXTAPI_REACH variable, you can set it to False as part of the Day 0 settings.

- The MGMTNODE_EXTAPI_REACH variable must be set during the initial installation, and cannot be changed later.
- You must ensure that the Cloud API, external, and provider network are properly routable, as Cisco VIM cannot automatically validate the same.

When MGMTNODE_EXTAPI_REACH is set to False, features such as VMTP and NFVbench are no longer accessible from the management node.

Horizon Hosting through NAT or DNS Aliases

From release Cisco VIM 3.0.0, you can deploy the Horizon portal through NAT or DNS alias. As a security measure, Horizon accepts a list of host addresses (IP or DNS) that are accessible. By default, this list includes the external_lib_vip_addr, the external_lb_vip_fqdn, and the ipv6 address (if applicable) only.

To host Horizon, perform the following steps:

1. Before launching the installation, update the setup_data.yaml file with the following information.

   ```
   HORIZON_ALLOWED_HOSTS:
   -  <NAT-IP>
   -  <NAT-IP>
   ```

   The parameter HORIZON_ALLOWED_HOSTS is optional and accepts the list of IP addresses and/or DNS names that you want to add as allowed hosts. Mostly, this IP address list match with the NAT address used for the deployment.
2. Run the following commands for reconfiguration:

   ```
   [root@mgmt1 ~]# cd /root/ [root@mgmt1 ~]# mkdir MyDir
   [root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
   # update/include the vim_ldap_admin in the setup_data
   [root@mgmt1 ~]# cd /root/MyDir/
   [root@mgmt1 ~]# vi setup_data.yaml [root@mgmt1 ~]# cd ~/installer-xxxx
   [root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
   ```

   The administrator can access the Horizon dashboard through aliases or NAT IPs.

Cinder Volume Encryption

Cisco VIM supports the configuration and creation of encrypted volumes managed by Cinder. The encryption is done natively using Linux Unified Key Setup (LUKS). From release Cisco VIM 3.0.0 onwards, this encryption is enabled by default and does not require any installation. Administrators can use the standard OpenStack APIs to create and mount the volumes. No configuration parameters are available in the setup data.

The following are the steps to create an encrypted volume:

1. From the management node, load the OpenStack authentication variables:

   ```
   [root@management-server-cisco~]# source ~/openstack-configs/openrc
   ```

2. Create a volume type that defines the desired encryption parameters using the below command:

   ```
   [root@management-server-cisco images]# openstack volume type create \
   --encryption-provider nova.volume.encryptors.luks.LuksEncryptor \
   --encryption-cipher aes-xts-plain64 \
   --encryption-key-size 256 \
   --encryption-control-location front-end LUKS
   ```

   Create an encrypted volume using the following command:

   ```
   [root@management-server-cisco images]# openstack volume create --size 1 --type LUKS encrypted_volume
   ```


   The overall storage Input Output Operations Per Second (IOPS) performance penalty is ~35% for Advanced Encryption Standard Cipher Block Chaining (AES-CBC) and ~60% for AES-XTS, when LUKS is enabled. Also, AES-CBC (keysize='128') encryption provides better performance as compared to AES-XTS (key_size='256') encryption mode.

Encryption of Secrets

Cisco VIM installation dynamically generates passwords for each Openstack service and for services running on the management node. By default, these passwords are system generated and are stored in the *secrets.yaml* file on the management node and then subsequently being read by various steps during the installation.

The *secrets.yaml* file is currently protected by Linux file permissions as well as SELinux mandatory access control. A clear text copy of this file is required during installation, reconfiguration, update, and upgrade. Therefore, the *secrets.yaml* file stores the passwords in cleartext, where a hashed version of these passwords is not sufficient.

From release Cisco VIM 3.4.0, Vault is used. Vault is a tool specifically designed to store and access the passwords securely. Vault encrypts the secrets prior to writing them to persistent storage. Hence, gaining access to the raw storage is not enough to access the secrets. To take advantage of this additional hardening option, you can optionally enable Vault in *setup_data.yaml* as a Day 0 option (reconfigure option will be available in the future). With vault enabled, all the passwords used by Cisco VIM services are stored in Vault with Consul as storage backend. To enable Vault, update the setup_data, with the following information as part of Day 0 installation.

```
VAULT: {enabled: True}
```

Once Vault is enabled, the contents of *secrets.yaml* are no longer visible.

To get the following user-relevant secrets, CLI and the corresponding Rest API are provided:

```
"CVIM_MON_PASSWORD", "CVIM_MON_READ_ONLY_PASSWORD", "CVIM_MON_SERVER_PASSWORD",
"ADMIN_USER_PASSWORD", "KIBANA_PASSWORD", "CVIM_MON_PROXY_PASSWORD".
```

Listed below is an example of how to fetch the secrets:

```
# ciscovim list-secrets --getpassword ADMIN_USER_PASSWORD

+---------------------+------------------+
| Secret Key          | Secret Value     |
+---------------------+------------------+
| ADMIN_USER_PASSWORD | D1g8O6Ws2Woav7Ye |
+---------------------+------------------+
```

The command ciscovim *list-secrets* can list all the secrets that are encrypted. TAC/services are trained on how to fetch any of the non-user facing secrets.

Customizing SSH Login Banner

From release Cisco VIM 3.0.0, you can provide a customized banner that will be displayed when an administrator attempts to login to the management node or Unified Management node. An optional parameter ssh_banner in the setup_data accepts a string or message to be displayed before the login prompt. This message indicates a warning consistent with a company's IT policies.

1. Before launching the installation, take a backup of the *setupdata.yaml* file and update the file manually with the configuration listed below:

   ```
   ssh_banner:
   <your Banner Text>

   WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing
   this system, you agree that your actions may be monitored if
   unauthorized usage is suspected.
   ```

2. Run the following commands for reconfiguration:

   ```
   [root@mgmt1 ~]# cd /root/
   [root@mgmt1 ~]# mkdir MyDir
   [root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
   # update/include the vim_ldap_admin in the setup_data
   [root@mgmt1 ~]# cd /root/MyDir/
   [root@mgmt1 ~]# vi setup_data.yaml
   [root@mgmt1 ~]# cd ~/installer-xxxx
   [root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
   ```

Enabling Red Hat Identify Management (IDM) System

Cisco VIM supports integration with Red Hat Identity Management System which is based on Identity, Policy, Audit (IPA) technology as a reconfigure option. Before you enable this feature, ensure that hostname of all servers including the management node are in lower case FQDN (RRFC4120), and belongs to ip_domain_name defined in IPA_INFO section. For assumptions associated to IDM, see Red Hat IDM. To enable this feature, follow the below steps:

1. Take a backup of the *setupdata* file and update the file manually with the configuration listed below:

   ```
   IPA_INFO:
   ipa_servers:
   ```

```
  - hostname: <hostname with fqdn belonging to the ipa_domain_name>
    ipaddresses: # --- Optional
      - '<ipv4_address>'
      - '<ipv6_address>'
  - hostname: <hostname with fqdn belonging to the ipa_domain_name>
    ipaddresses: --- Optional
      - '<ipv4_address>'
      - '<ipv6_address>'
enroller_user: <enroller_username>
enroller_password: <enroller_password>
ipa_domain_name: <ipa_domain_name>
```

2. Run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/  # update/include the IPA_INFO
in the setup_data
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```


You can change all the parameters other than *ipa_domain_name* via reconfiguration post installation. Also, you cannot reconfigure IPA in conjunction with any other reconfiguration operation.

Enabling Vault on Day 2 in Cisco VIM Pod

Cisco VIM supports Vault as a reconfiguration option.

1. To enable Vault on a pod running Cisco VIM 3.4.1 or later, update the *setup_data.yaml* file as follows:

```
#Vault:
enabled: True # optional, default if not defined is false
```

2. Take a backup of *setup_data* file and update it manually with the configuration details by running the following command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
# update the setup_data to enable vault
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Enabling Trusted Virtual Function on Day 2

For releases earlier to Cisco VIM 3.4.2, you must delete the existing VMs on the target compute to enable the trusted virtual function (VF) on a server after the initial installation of the cloud. To avoid the disruption caused to the existing VMs, a reconfigure option is introduced. You can enable trusted VF on the SRIOV ports as a reconfiguration option, on a per server basis using the below steps:

1. To enable trusted_vf on a pod running Cisco VIM 3.4.2 or later, update the SERVERS section for the target computes where trusted_vf is enabled in the *setup_data.yaml* file as given below:

```
SERVERS:
  <target_compute_name>:
    trusted_vf: True
```

2. Take a backup of *setupdata* file and update it manually with the configuration details by running the following command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# # update the setup_data to enable trusted_vf on the target computes
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

FQDN Support for Cisco VIM Management API

By default, Cisco VIM uses self-signed IP based TLS certificates for its management services that include REST API, Kibana, Prometheus, and CVIMMON. Optionally, the administrator can use third-party TLS certificates for Cisco VIM management services.

To enable FQDN support for Cisco VIM management API, follow the below steps:

> ⚠ FQDN must resolve to the management node IP address by configured DNS servers. For dual stack deployment, FQDN must resolve to both IPv4 & IPv6 address.

1. Copy the new key, CA root and certificate files into the *~/openstack-configs* folder under the following filenames:

```
# cp <new-ca-root-cert> /installer-xxx/openstack-configs/mercury-ca.crt

# cp <new-key-file> /installer-xxx/openstack-configs/mercury.key

# cp <new-cert-file> /installer-xxx/openstack-configs/mercury.crt
```

2. Obtain the FQDN name from the TLS certificate:

```
# openssl x509 -in /root/installer-xxx/openstack-configs/mercury-ca.crt -text -noout

Sample output:
. . .

Subject: C=US, ST=California, L=San Jose, O=IT, CN=cvim_management.domain.com
```

3. Once copied, run the following Rest API reconfiguration commands:

```
#  cd /root/installer-xxxx/tools

# ./restapi.py -a reconfigure-tls -d <FQDN>    # For example FQDN is cvim_management.domain.com
```

4. For Day 0 deployment, update the *setup_data* with the MGMTNODE_EXTAPI_FQDN set to <FQDN> value, which is used in Step 3 with *reconfigure-tls* option and run *ciscovim install:*

```
MGMTNODE_EXTAPI_FQDN: <FQDN>
```

5. For Day 2 deployment, update the *setup_data* with MGMTNODE_EXTAPI_FQDN set to <FQDN> and run *ciscovim* reconfigure command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# # update the setup_data with MGMTNODE_EXTAPI_FQDN: <FQDN>
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Enabling NFVBench

Enabling NFVBench Post Deployment

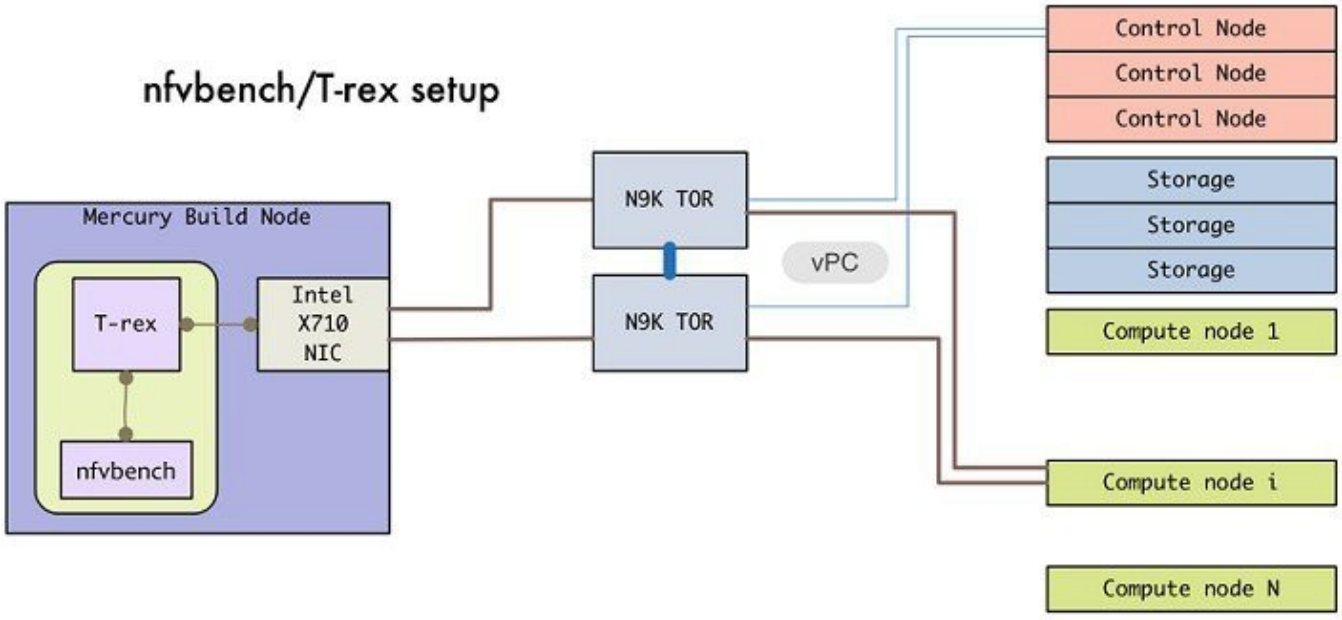
The NFVBench (performance benchmark) is an optional tool. You can deploy NFVBench after the installation of the pod. This section describes how to setup and use NFVbench with Cisco VIM.

Once the pre-requisites for the management node hardware (Intel NIC) are met, add the NFVbench configuration in the setup_data.yaml. By default, NFVbench configuration is not enabled in Cisco VIM as it needs additional hardware. NFVbench also works, when the mechanism driver is OVS or VPP.

Before you begin

- If you are using Quanta servers for the Day 0 BIOS setting of the management node, see Installing Management Node on Quanta Servers.
- An extra 10GE (Intel X710 NIC) or 40GE (Intel XL710) or 25G (Intel xxv710) must be installed on the management node.
- To interact with Intel NIC, the TRex traffic generator uses DPDK interface and uses hardware instead of just software to generate packets. This approach is more scalable and enables NFVbench to perform tests without software limitations.
- Wire two physical interfaces of the Intel NIC to the ToR switches (as shown in the following figure).

If your NIC has more than two ports, use the first two ports only. Connect the first port to the first ToR switch (order is given by setup_data.yaml) and the second port to the second TOR switch. If there is only one ToR switch, connect the first two ports to it as shown in the NFVbench topology figure.



1. Enable the NFVBench configuration in the *setup_data.yaml* file:

   Sample configuration for OVS/VLAN or VPP mechanism driver

```
NFVBENCH:
 enabled: True # True or False
# tor_info: {TORa: eth1/42, TORb: eth1/42} # Optional; Can only be defined when TORSWITCHINFO is defined
in the setup_data
# tor_info: {TOR: 'eth1/42,eth1/43'} # use if there is only one TOR switch
# nic_ports: 3,4 # Optional input, indicates which two of the four available ports of 10G Intel NIC are
used by NFVbench tool to send and receive traffic.
# Defaults to the first 2 ports of NIC (ports 1 and 2) if not specified.
# Port number must be between 1 and 4, one port cannot be used twice.
# nic_slot: <int> # Optional, defaults to first set of unbonded pair of NIC ports in an Intel 710 or 520
card the code finds; you can run NFVbench via XL710, 520
or X710 card
# Example:
# nic_ports: 1,4 # the first and the last port of Intel NIC are used
# nic_slot: 2 # # Optional, defaults to 1st set of unbonded pair of NIC ports in an Intel 710 or 520
card the code
finds; you can run NFVbench via XL710, 520 or X710 card
```

```
# nic_slot: Management node slot on which the NFVbench NIC card is anchored off
# For VTS/VXLAN
# vteps: "vtep_ip1,vtep_ip2" # Mandatory and needed only for VTS/VXLAN. Specify separated IP pairs in
tenant network and not in the tenant
pool, reconfigurable
##

For VXLAN over vxlan-tenant network
# vteps: "vtep_ip1,vtep_ip2" #Mandatory, specify separated IP pairs in vxlan-tenant network but not in
the vxlan-tenant pool, reconfigurable
# vnis: "vni_id1, vni_id2" # Mandatory, specify the VNI range to be used for all vxlan networks created
by NFVbench for benchmarking
```

Sample configuration for VTS mechanism driver

```
NFVBENCH:
 enabled: True # True or False
 tor_info: {TORa: eth1/42, TORb: eth1/42} # Optional, can only be defined when TORSWITCHINFO is defined
vtep: "ip1, ip2" # Mandatory and needed only for VTS/VXLAN.
# Specify any pair of unused VLAN ids for VLAN to VxLAN encapsulation in TOR switch.
# tor_info: {TOR: 'eth1/42,eth1/43'}
Use if there is only one TOR switch
# nic_ports: 3,4 # Optional input, indicates which two of the four available ports of 10G Intel NIC on
the management node are used by NFVbench tool to send and
 receive traffic.
# Defaults to the first 2 ports of NIC (ports 1 and 2) if not specified.
# Port number must be between 1 and 4, one port cannot be used twice.

# Example:

# nic_ports: 1,4 # the first and the last port of Intel NIC are used.
# nic_slot: 2 # # Optional, defaults to first set of unbonded pair of NIC ports in an Intel 710 or 520
card the code finds. You can run
# NFVbench via XL710 or X710 card

# Note: if nic_ports are defined, then nic_slot has to be defined and vice-versa
VTS_PARAMETERS:
...
VTS_DAY0: '<True|False>'# Required parameter when VTS enabled.
VTS_USERNAME: '<vts_username>'# Required parameter when VTS enabled.
VTS_PASSWORD: '<vts_password>'# Required parameter when VTS enabled.
VTS_NCS_IP: '11.11.11.111'# '<vts_ncs_ip>',mandatory when VTS enabled.
VTC_SSH_USERNAME: 'admin'# '<vtc_ssh_username>',mandatory for NFVbench.
VTC_SSH_PASSWORD: 'my_password'#'<vtc_ssh_password>', mandatory for NFVbench.
```


vtep_vlans field is required if VxLAN is used as encapsulation without VTS.

2. Configure minimal settings for NFVBench:

```
# Minimal settings required for NFVbench
TORSWITCHINFO:
CONFIGURE_TORS: <True or False> # True if
switches should be configured to support NFVbench
...
SWITCHDETAILS:
- hostname: 'TORa' # Hostname matching
'tor_info' switch name.
username: 'admin' # Login username for switch user.
password: 'my_password' # Login password for switch user.
ssh_ip: '172.31.230.123' # SSH IP for switch.
- hostname: 'TORb'
username: 'admin'
password: 'my_password'
ssh_ip: '172.31.230.124
```

The tor_info provides the information to configure the ToR switches. Two ports specified by interfaces are configured in trunk mode in the same port-channel **po**. NFVbench needs the login details to access ToR details and retrieve TX/RX counters. Manual configuration is required if the 'CONFIGURE_TORS' is set to 'False'.

With VTS as mechanism driver, additional settings are needed. NFVbench needs access to VTS NCS to perform cleanup after it detaches the traffic generator port from VTS. Also, a pair of VTEP VLANs is required for VLAN to VxLAN mapping. Value can be any pair of unused VLAN ID.

3. To do manual configuration on the ToRs, ensure that you perform the following configuration:

```
interface Ethernetx/y
switchport mode trunk
switchport trunk allowed vlan <3000-3049>
spanning-tree bpdufilter enable
```

4. Reconfigure Cisco VIM to start or restart the NFVBench container. To reconfigure, add necessary configuration to the *setup_data.yaml* file and run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp/root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# cd /root/
# update the setup_data to include NFVBENCH section
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

After the reconfiguration, you can see that the NFVBench container is up and ready for use.

Use the command *~/openstack-configs/openrc* to source the openrc *source* before using the nfvbench.

Customization of Edge

Customization of Edge

From release Cisco VIM 3.0.0 onwards, you need to specify a flavor metadata key *hw:vcpu0_pin_to_shared* to use the optional flavor in OpenStack, that can be set only at Day 0.

When a VM is spawned with the flavor that contains the above metadata set to **Yes**, NOVA allocates additional vCPU on top of the vCPU count specified in the flavor and pin vCPU0 to the pCPU that is reserved in the pool. The pinning of vCPU to pCPU is load-balanced, if hyper-threading is enabled in the host level.

To enable this configuration, set hw:cpu_policy to **dedicated**. And it is often used together with **hw:emulator_threads_policy** being set to **share**, so that the VM emulator threads are also pinned to the same dedicated pool to enable better real-time processing for latency and performance-sensitive VNFs.

To enable this feature, set the following command in the **setup_data.yaml** file on Day 0:

```
ENABLE_VM_EMULATOR_PIN:
<True or False> # optional, default is false
```

The number of cores reserved is determined by VM_EMULATOR_PCORES_PER_SOCKET, which is also pre-defined at the day-0 configuration.

```
VM_EMULATOR_PCORES_PER_SOCKET: < 1 to 4> # Optional,takes effect only when ENABLE_VM_EMULATOR_PIN is true.
If undefined, defaults to value of 1.
```

You can set the NOVA_OPT_LOW_LATENCY flag to enable further optimization on nova libvirt, to achieve lower latency for VM applications. To be specific, it will set **cpu_mode** to **host-passthrough** and **cpu_model_extra_flags** to **tsc-deadline** in nova.conf.

```
NOVA_OPT_FOR_LOW_LATENCY:
True or False # Optional, default to False
```

From release Cisco VIM 3.2.1 onwards, an option to enable Intel's Resource Director Technology (RDT) by Cache Allocation Technology (CAT) is available.

To enable CAT, you must enable NFV_HOSTS option. You can enable the CAT option only as a Day 0 option with the following option in the **setup_data.yaml** file:

```
INTEL_RDT:

ENABLE_CAT: false # Enable Intel CAT, optional and default to False
#Reserved cachelines per socket for sockets, allowed value of 1 to 32.
#Only valid when ENABLE_CAT is sets to True.
RESERVED_L3_CACHELINES_PER_SOCKET: 3
```

The cachelines reserved for hosts are not immediately applied. When first VM with the cacheline requirements lands on the any NUMA node of one compute node, Cisco VIM performs the cacheline partitioning on the host. If VM with no cacheline requirements are spawned (as defined via flavor) on one compute node, all VMs are allowed to use all cachelines available in the CPU. When the last VM with cacheline requirements is deleted from any NUMA node of one compute node, Cisco VIM resets the cacheline masks so that all new and existing VMs are allowed to use all available cachelines again.

To support extreme low latency (< 50 micro-seconds) requirements for vRAN workload, Cisco VIM integrates with Intel N3000 FPGA card for both hardware offload and I/Os. The option of N3000 Intel card is only allowed with Quanta servers, and the following item in the setup_data enables the cards on the servers. These configurations have effect only on computes where the N3000 cards are installed.

```
# Intel FPGA N3000 NIC (for QCT now)
# By default, FPGA VF is not enabled.
# To enable, define a value in the range from 1 to 8.
# INTEL_FPGA_VFS: <integer value from 1 to 8>
# By default, FPGA VF is not enabled.
# VFS support for Intel FPGA N3000 NIC (for QCT now) for SRIOV
# INTEL_VC_SRIOV_VFS: <integer value from 1 to 32>
```

You can enable the virtual function (VFS) values optionally at a per-server level, however, the global configuration is needed as listed below:

```
SERVERS:
compute-server-1:
INTEL_FPGA_VFS: <integer value from 1 to 8>
```

```
INTEL_SRIOV_VFS: <integer value from 1 to 32>
INTEL_VC_SRIOV_VFS: <integer value from 1 to 32>
```

⚠ You can enable single or multiple options listed above on a per server basis

Installation Mode

Installation Mode

You can deploy Cisco VIM in one of the following install modes:

- Connected: In this mode, the setup must be connected to Internet or Cisco VIM software hub to fetch artifacts and docker images.
- Disconnected: In this mode, Cisco VIM is not connected to Internet. The artifacts and docker images are loaded from USB device.

Based on the deployment type, select the install mode as connected or disconnected as given below:

```
# Install Mode: connected/disconnected
INSTALL_MODE: connected
```


You can switch from one mode to another via the reconfigure option.

NFVIMON

NFVIMON

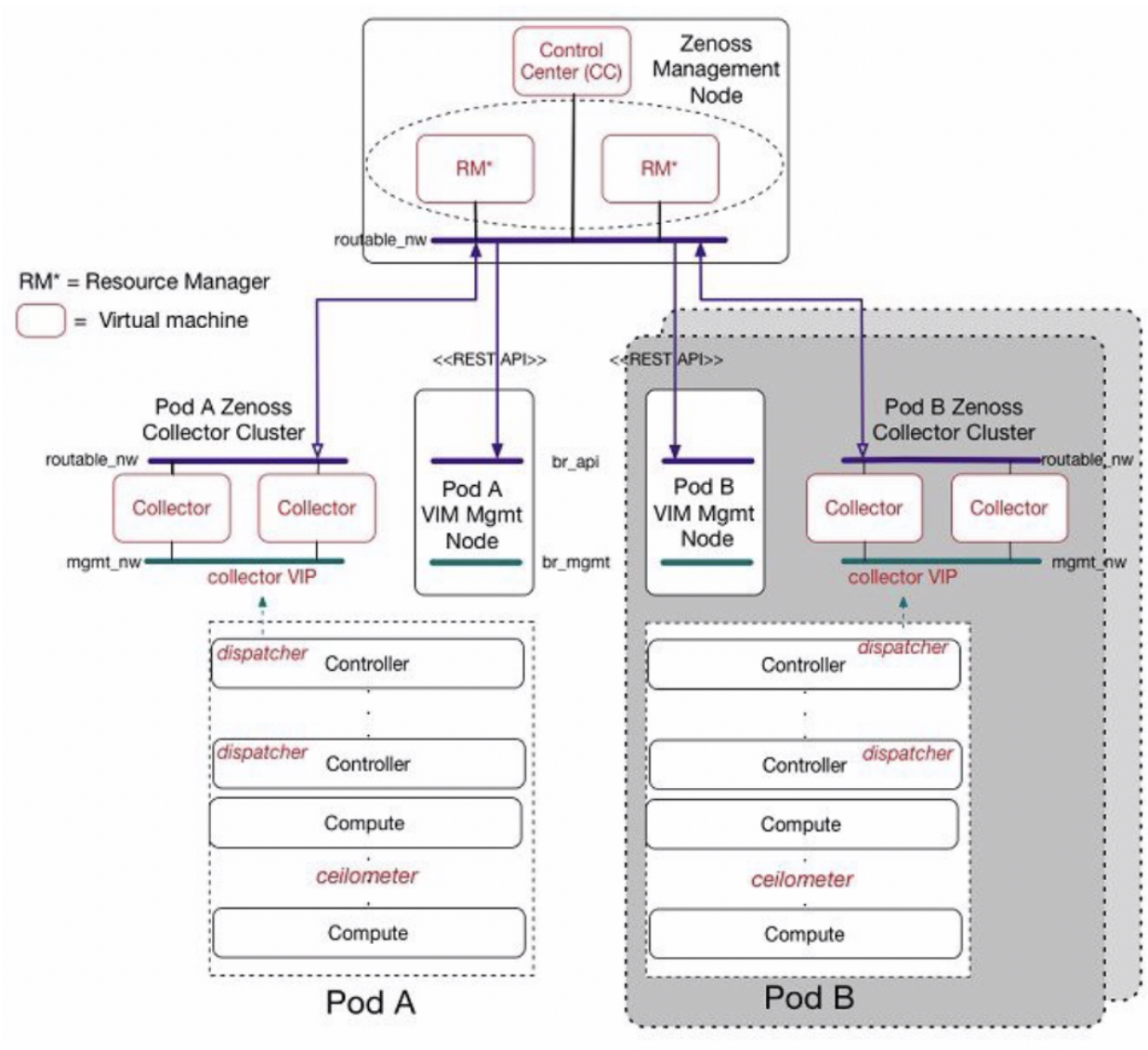
NFVIMON Overview

You can optionally install Cisco VIM with a third-party software known as NFVI Monitor (NFVIMON) to monitor the health and performance of the NFVI. This includes monitoring the physical and logical components of single or multiple NFVI pods. The NFVIMON feature is enabled by the Zenoss. NFVIMON provides extensive monitoring and collection of performance data for various components of the cloud infrastructure including Cisco UCS blade and rack servers, service profiles, Nexus top of rack switches, fabric connections, and OpenStack instances.

The monitoring system is designed to monitor single or multiple pods from a single management system.

You can enable NFVIMON on an existing pod, by extending the *setup_data.yaml* file with relevant information through the reconfigure option. After this configuration, add the pod as the VIM resource to be monitored in a Control Center.

NFVIMON Architecture



NFVIMON consists of four components:

- ceilometer service for data collection
- collector
- resource manager (RM)
- control-center with Cisco Zenpacks (CZ)

The NFVIMON architecture supports the monitoring of one or more Cisco VIM pods. There is no limit on the number of pods, but note that the setup supports up to ~ 25000 managed resources across pods, where a managed resource is a physical device, network device or virtual machine tracked from a monitoring perspective.

As NFVIMON is a third-party software, ensure that the integration of NFVIMON with Cisco VIM is loosely coupled and the VIM automation only deals with installation of the ceilometer service required to monitor the pod. The installation of other NFVIMON components like collector, resource manager (RM) and control-center with Cisco Zenpacks (CZ) are out of scope as they are part of Cisco advanced services.

Before you Begin

1. Ensure that you have engaged with the account team for services engagement on the planning and installation of the NFVIMON accessories along with its network requirements. The image information of collector, Resource Manager (RM) and control-center with Cisco Zenpacks (CZ) can be obtained only through Cisco Advance Services.
2. At a high level, you must have a designated node to host a pair of collector VMs for each pod, and a common node to host CC and RM VMs that can aggregate and display monitoring information from multiple pods.
3. The collector VMs must have two interfaces:
    - Interface with br_mgmt of the VIM.
    - Interface that is routable and reachable to the VIM Installer REST API and RM VMs.
4. As the collector VM is in an independent node, four IPs from the management network of the pod must be pre-planned and reserved. The installation steps of the collector, resource manager (RM) and control-center with Cisco Zenpacks (CZ) are part of Cisco advance service activities.

Start with one Cisco VIM pod (Pod A in the picture) and two external nodes (one to host 2 Collector VMs and one for remote management to host 1 control-center with Cisco Zenpacks and 2 RM VMs) of multiple pods.

Monitor the Cisco VIM pods at the time of installation if NFVIMON is enabled, or by adding NFVIMON after installation. Install the collectors manually in the external collector node, so that the pod is added for monitoring in the control center.

- From Cisco VIM 3.2.0, you can use non-root admin keys for monitoring purposes.
- From Cisco VIM 3.4.1, you can run NFVIMON along with CVIM MON. This capability eases the transition from NFVIMON to CVIM MON and allows operators to evaluate CVIM MON while using NFVIMON.

Enabling NFVIMON

The ceilometer service is the only component in NFVIMON that is managed by Cisco VIM orchestrator. While the ceilometer service collects the metrics to pass OpenStack information of the pod to the collectors, the Cisco NFVI Zenpack available in the controller node gathers the node level information.

1. To enable NFVIMON as part of the Cisco VIM installation, update the **setup_data.yaml** file with the following information:

```
#Define the PODNAME
PODNAME: <PODNAME with no space>; ensure that this is unique across all the pods
NFVIMON:
  MASTER:    # Master Section
    admin_ip: <IP address of Control Centre VM>
  COLLECTOR:    # Collector Section
        management_vip: <VIP for ceilometer/dispatcher to use> #Must be unique across the VIM pod and be
part of br_mgmt network.
        Collector_VM_Info:
-
                hostname: <hostname of Collector VM 1>
                password: <password_for_collector_vm1> # max length of 32
                ccuser_password: <password from master for 'ccuser' (to be used for self monitoring)> #
max length of 32
                admin_ip: <ssh_ip_collector_vm1> # Should be reachable from br_api network
                management_ip: <mgmt_ip_collector_vm1> # Should be part of br_mgmt network
                -
                hostname: <hostname of Collector VM 2>
                password: <password_for_collector_vm2> # max length of 32
                ccuser_password: <password from master for 'ccuser' (to be used for self monitoring)> #
```

```
max length of 32
                admin_ip: <ssh_ip_collector_vm2> # Must be reachable from br_api network
                management_ip: <mgmt_ip_collector_vm2> # Must be part of br_mgmt network
        COLLECTOR_TORCONNECTIONS: # Optional. Indicates the port where the collector is hanging off.
Recommended when Cisco NCS 5500 is used as ToR
          - tor_info: {po: <int>, switch_a_hostname: ethx/y, switch_b_hostname: ethx/y}

# Section of MASTER_2 and COLLECTOR_2 are optional and only needed to support NFVIMON in HA
  MASTER_2:    # Master Section
        admin_ip: <IP address of Control Centre VM>
  COLLECTOR_2:    # Collector Section
        management_vip: <VIP for ceilometer/dispatcher to use> #Should be unique across the VIM Pod;
Should be part of br_mgmt network
        Collector_VM_Info:
        -
                hostname: <hostname of Collector VM 1>
                password: <password_for_collector_vm1> # max length of 32
                ccuser_password: <password from master for 'ccuser' (to be used for self monitoring)> #
max length of 32
                admin_ip: <ssh_ip_collector_vm1> # Must be reachable from br_api network
                management_ip: <mgmt_ip_collector_vm1> # Must be part of br_mgmt network
                -
                hostname: <hostname of Collector VM 2>
                password: <password_for_collector_vm2> # max length of 32
                ccuser_password: <password from master for 'ccuser' (to be used for self monitoring)> #
max length of 32
                admin_ip: <ssh_ip_collector_vm2> # Should be reachable from br_api network
                management_ip: <mgmt_ip_collector_vm2> # Should be part of br_mgmt network
        COLLECTOR_TORCONNECTIONS: # Optional. Indicates the port where the collector is hanging off.
Recommended when Cisco NCS 5500 is used as ToR
          - tor_info: {po: <int>, switch_a_hostname: ethx/y, switch_b_hostname: ethx/y}

  DISPATCHER:
        rabbitmq_username: admin # Pod specific user for dispatcher module

  NFVIMON_ADMIN: admin_name # Optional, once enabled, you need to have only one admin that is
reconfigurable to add/update non-root user id.
```

⚠ If NFVIMON HA is enabled, ensure that all the admin IPs are on the same subnet for NFVIMON VMs and deployed servers.

2. To monitor ToR, ensure that the following TORSWITCHINFO sections are defined in the *setup_data.yaml* file:

```
TORSWITHCINFO:
SWITCHDETAILS:
-
hostname: <switch_a_hostname>:    # Mandatory for NFVIMON if switch monitoring is needed
username: <TOR switch username>    # Mandatory for NFVIMON if switch monitoring is needed
password: <TOR switch password>    # Mandatory for NFVBENCH; Mandatory for NFVIMON if switch monitoring
is needed
ssh_ip: <TOR switch ssh ip>    # Mandatory for NFVIMON if switch monitoring is needed
....
-
hostname: <switch_b_hostname>:    # Mandatory for NFVIMON if switch monitoring is needed
username: <TOR switch username>    # Mandatory for NFVIMON if switch monitoring is needed
password: <TOR switch password>    # Mandatory for NFVIMON if switch monitoring is needed
ssh_ip: <TOR switch ssh ip>    # Mandatory for NFVIMON if switch monitoring is needed
```

⚠ TORSWITCH monitoring is disabled, when running Cisco VIM with ACI plugin enabled.

3. To initiate the integration of NFVIMON on an existing pod, copy the setupdata into a local directory and update it manually with information listed above, and then run the reconfiguration command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
```

```
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to include NFVIMON related info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

4. To initiate the uninstallation of NFVIMON on an existing pod, copy the setupdata into a local directory and remove the entire NFVIMON section listed above, and then run the reconfiguration command as follows:

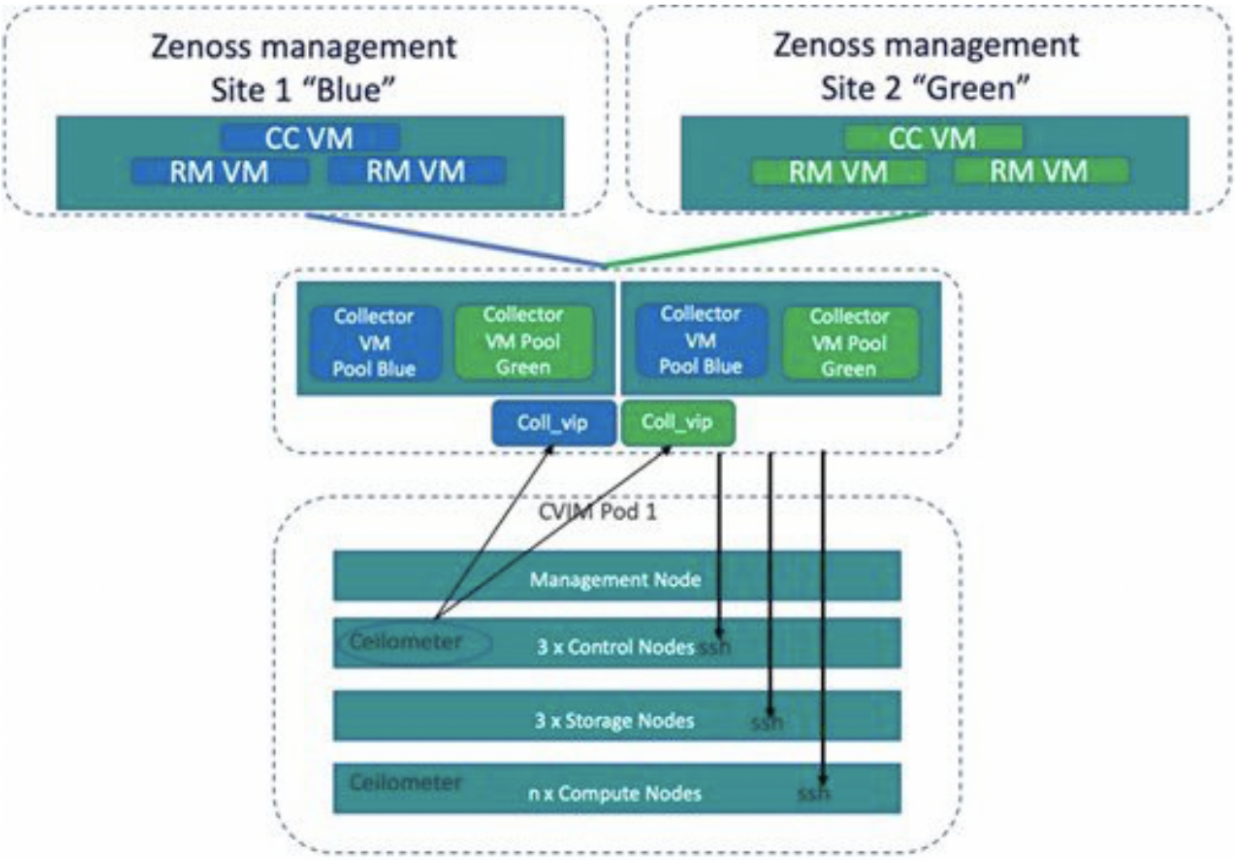
```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to exclude NFVIMON related info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim --setupfile ~/MyDir/<my_setup_data.yaml> reconfigure
```

- NFVIMON is supported only on a pod running with Keystone v3.
- NFVIMON can run with either root or non-root admin keys for monitoring.

Overview of NFVIMON High Availability

NFVIMON supports the functionality of high availability (HA). HA is achieved through dual polling of the redundant collectors over an active-active deployment. VM is deployed between the two physical collector servers with two sets of collectors. Two separate Zenoss CC-RMs are connected to one set of collectors each, to aid in simultaneous monitoring of the pod. Ceilometer is deployed in Cisco VIM pod such that it sends data to two separate collector VIPs simultaneously.

The NFVIMON HA architecture is depicted in the figure below:



You cannot move pods running with NFVIMON in standalone mode to HA mode through reconfiguration.

You can enable NFVIMON HA on Day 0 or Day 1 when the pod is not running with NFVIMON.

OpenStack Features

OpenStack Features

Memory/CPU Usage

Memory/CPU Usage

Memory Over-Subscription Ratio

Cloud allows you for over-subscription of resources such as CPU and memory. By default, the memory over-subscription value is set to 1.5. You can adjust the global memory over-subscription value in the range of 1.0 to 4.0.

> ⚠ You can change the default values only at the beginning of the installation

Run the following command to set the NOVA_RAM_ALLOCATION_RATIO, on fresh installation:

```
# cd installer-<tagid>/openstack-configs/
# update NOVA_RAM_ALLOCATION_RATIO value in openstack_config.yaml
```

Once the NOVA_RAM_ALLOCATION_RATIO is set, continue with the rest of the steps as planned for installation.

RAM Over-Subscription Ratio

Cloud allows you for over-subscription of CPU and memory. By default, the CPU over-subscription value is set to 16.0. You can adjust the global CPU over-subscription value in the range of 1.0 to 16.0.

> ⚠ You can change the default value before the installation begins.

Run the following command to set the NOVA_CPU_ALLOCATION_RATIO on fresh installation:

```
# cd installer-<tagid>/openstack-configs/
# update NOVA_CPU_ALLOCATION_RATIO value in openstack_config.yaml
```

Once the NOVA_CPU_ALLOCATION_RATIO is done, continue with the rest of the steps as planned for installation.

CPU and RAM Allocation Ratio

By default, OpenStack sets the CPU and RAM allocation ratio globally. Cisco VIM allows you to change the default CPU and RAM allocation ratio as a Day 0 or Day 1 operation. From Cisco VIM 3.4.1, you can set these parameters on a per compute basis via addition/removal of the target computes. From Cisco VIM 3.4.3, the CPU and RAM allocation ratio can be set on Day 2 via reconfigure option on a per compute basis.

> ⚠ Setting the parameters on a per compute basis via reconfigure option enforces the settings only for the new VMs that get launched on the target compute, but not for the existing VMs.

To enable CPU and RAM allocation ratio on a per compute basis, update each of the target compute nodes with the following configuration in the *setup_data.yaml* file, after taking a backup of the *setup_data.*

```
SERVERS:
   compute-server-1:
   NOVA_CPU_ALLOCATION_RATIO: 1.0 <float, range: 0.958-16.0>   # <== optional, override the
NOVA_CPU_ALLOCATION_RATIO configuration defined in openstack_config.yaml
   NOVA_RAM_ALLOCATION_RATIO: 1.0 <float, range: 1.0-4.0>      # <== optional, override the
NOVA_RAM_ALLOCATION_RATIO configuration defined in openstack_config.yaml
```

Run the following reconfiguration command after updating the target *setup_data:*

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/ # update the RAM and/or CPU Allocation
Ratio on a per compute basis
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```


For a given compute server, if NOVA_CPU_ALLOCATION_RATIO and/or NOVA_RAM_ALLOCATION_RATIO entries are added, you cannot drop it via reconfigure. To get to the global value, it is recommended to set the target compute's NOVA_CPU_ALLOCATION_RATIO and/or NOVA_RAM_ALLOCATION_RATIO value to that of global and run re-configure.

DHCP Reservations

DHCP Reservations for VM's MAC Addresses

From release Cisco VIM 3.2.0, you can have DHCP reservations for virtual machine MAC addresses, to get the same IP address always regardless of the host hypervisor or operating system they are running. To avail this optional feature, few restrictions exist.
If the MAC address ends with 00:00, then

- First entry of the first octect must be a Hex
- Second entry of the first octect must be 2, 6, a or e
- No entry can start with *fe*

For example, the MAC address entry can be [a-f][2,6,a,e]:yz:uv:ws:00:00, but not starting with *fe*

1. To enable this feature, take the backup of the of the setupdata file and update the file manually with the configuration listed below:

```
BASE_MACADDRESS: <[a-f][2,6,a,e]:yz:uv:ws:00:00>        # Entry not starting with "fe"
```

> ⚠ To avoid mac-address collision, ensure that a minimum of last three octects is 00. For example: BASE_MACADDRESS: <[a-f][2,6,a,e]:[a-f0-9][a-f0-9]:[a-f0-9][a-f0-9]:00:00:00>

2. Run the following commands for reconfiguration:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
# update/include the vim_ldap_admin in the setup_data
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Trusted Virtual Functions

Setting up Trusted Virtual Functions

The kernel feature allows the virtual functions (VF) to become trusted by the physical function and perform some privileged operations such as enabling VF promiscuous mode and changing VF MAC address within the guest. The inability to modify MAC addresses in the guest prevents the users from being able to easily setup up two VFs in a fail-over bond in a guest. To avail this feature, enable the following under each of the target compute nodes that are enabled with SRIOV:

```
SERVERS:
 compute-server-1:
 trusted_vf: <True or False> # <== optional, only applicable if its SRIOV node
```

You can avail this feature on Day 0, or enable in a compute on Day 2 by removing it and adding it back into the cloud after updating the setup_data with the configuration intent. From Cisco VIM 3.4.2, the trusted_vf can be set on Day 2 via reconfigure option on a per compute basis that are running with SRIOV. To enable trusted_vf on a per compute basis, update each of the target compute nodes with the following configuration in the *setup_data.yaml* file, after taking a backup of the *setup_data.* Then run the reconfiguration command after updating the target *setup_data:*

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/ # update the trusted_vf option on a per
compute basis which are running SRIOV
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Buffer Size Setup

Setting up Transmit and Receive Buffer Size

By default, the transmit and receive buffer for the interfaces on each of the servers is set to 1024. This feature allows you to set the rx_tz_queue_size to 512 on a per server basis, which is a requirement for some VNFs. To avail this feature, enable the following under each of the target compute nodes:

```
SERVERS:
 compute-server-1:
 rx_tx_queue_size: <512 or 1024> # optional, default if not defined is 1024
```

You can avail this feature on Day 0, or enable in a compute on Day 2 by removing it and adding it back into the cloud after updating the setup_data with the configuration intent.

VPP Port Mirroring Usage

VPP Port Mirroring Usage

Overview

The VPP port mirroring enables you to selectively create a mirror port to a VM. This mirror port detects all the packets sent and received by the VM without having access to the VM. The packets captured in this manner are saved as pcap files which are then used by tools like Wireshark and so on for further analysis.

The following CLIs are available in Cisco VIM:

- vpp-portmirror-create: Tool to create mirrored ports corresponding to Openstack ports.
- vpp-portmirror-delete: Tool to delete mirrored ports.
- vpp-portmirror-list: Tool to get a list of currently mirrored port.

The VPP port mirror tools perform the following:

- Checks if the specified port is a valid neutron port with valid UUID pattern.
- Checks if there is a corresponding Vhost interface in the VPP instance for the neutron port specified.
- Checks if the port has already mirrored.

Port Mirroring

1. Identify the VM that you want to monitor and the compute host on which it runs.

```
From the Management node, execute the following:
#cd /root/openstack-configs
# source openrc
# openstack server show vm-7
+--------------------------------------+------------------------------------------------------------+
| Field                                | Value                                                      |
+--------------------------------------+------------------------------------------------------------+
| OS-DCF:diskConfig                    | AUTO                                                       |
| OS-EXT-AZ:availability_zone          | nova                                                       |
| OS-EXT-SRV-ATTR:host                 | k07-compute-1                                              |
| OS-EXT-SRV-ATTR:hypervisor_hostname  | k07-compute-1                                              |
| OS-EXT-SRV-ATTR:instance_name        | instance-0000004d                                          |
| OS-EXT-STS:power_state               | Running                                                    |
| OS-EXT-STS:task_state                | None                                                       |
| OS-EXT-STS:vm_state                  | active                                                     |
| OS-SRV-USG:launched_at               | 2018-05-10T02:40:58.000000                                 |
| OS-SRV-USG:terminated_at             | None                                                       |
| accessIPv4                           |                                                            |
| accessIPv6                           |                                                            |
| addresses                            | net1=10.0.1.4                                              |
| config_drive                         |                                                            |
| created                              | 2018-05-10T02:40:37Z                                       |
| flavor                               | m1.medium (ac4bdd7f-ff05-4f0d-90a5-d7376e5e4c75)           |
| hostId                               | 8e7f752ab34153d99b17429857f86e30ecc24c830844e9348936bafc   |
| id                                   | 46e576c1-539b-419d-a7d3-9bdde3f58e35                       |
| image                                | cirros (e5e7e9d8-9585-46e3-90d5-4ead5c2a94c2)              |
| key_name                             | None                                                       |
| name                                 | vm-7                                                       |
| os-extended-volumes:volumes_attached | []                                                         |
| progress                             | 0                                                          |
| project_id                           | 434cf25d4b214398a7445b4fafa8956a                           |
| properties                           |                                                            |
| security_groups                      | [{u'name': u'my_sec_group'}]                               |
| status                               | ACTIVE                                                     |
| updated                              | 2018-05-10T02:40:58Z                                       |
| user_id                              | 57e3f11eaf2b4541b2371c83c70c2686                           |
+--------------------------------------+------------------------------------------------------------+
```

2. Identify the neutron port that corresponds to the interface that you want to mirror.

```
# openstack port list | grep 10.0.1.4
| ed8caee2-f56c-4156-8611-55dde24f742a | | fa:16:3e:6a:d3:e8 | ip_address='10.0.1.4',
subnet_id='6d780f2c-0eeb-4c6c-a26c-c03f47f37a45' |
```

3. SSH to the target compute node on which the VM is running and connect the VPP docker container.

```
# vpp
neutron_vpp_13881 [root@k07-compute-1 /]#
The syntax of the Port mirror create tool is as follows:
neutron_vpp_13881 [root@k07-compute-1 /]# vpp-portmirror-create
Option -p (--port) requires an argument
-p --port [arg] Port in openstack port uuid format. Required.
-d --debug Enables debug mode
-h --help This page
-n --no-color Disable color output
VPP port mirror utility.
```

4. Create a port mirror using the neutron port ID identified in Step 2. The CLI tool displays the mirrored interface name:

```
neutron_vpp_13881 [root@k07-compute-1 /]# vpp-portmirror-create -p ed8caee2-f56c-4156-8611-55dde24f742a
===============[ Port Mirroring ]=========================
2018-05-14 22:48:26 UTC [ info] Interface inside vpp is VirtualEthernet0/0/1 for Openstack port:
ed8caee2-f56c-4156-8611-
55dde24f742a
2018-05-14 22:48:26 UTC [ info] Port:ed8caee2-f56c-4156-8611-55dde24f742a is now mirrored at taped8caee2
2018-05-14 22:48:26 UTC [ notice] Note! Please ensure to delete the mirrored port when you are done
with debugging
```

.

> ⚠ Use the –debug flag to troubleshoot the Linux/VPP commands that are used to set up the port mirror.

5. Use the tap device as a standard Linux interface and use tools such as tcpdump to perform packet capture.

```
neutron_vpp_13881 [root@k07-compute-1 /]# tcpdump -leni taped8caee2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on taped8caee2, link-type EN10MB (Ethernet), capture size 262144 bytes
16:10:31.489392 fa:16:3e:6a:d3:e8 > fa:16:3e:0e:58:7b, ethertype IPv4 (0x0800), length 98: 10.0.1.4
> 10.0.1.10: ICMP echo
request, id 32513, seq 25752, length 64
16:10:31.489480 fa:16:3e:0e:58:7b > fa:16:3e:6a:d3:e8, ethertype IPv4 (0x0800), length 98: 10.0.1.10
> 10.0.1.4: ICMP echo
reply, id 32513, seq 25752, length 64
16:10:32.489560 fa:16:3e:6a:d3:e8 > fa:16:3e:0e:58:7b, ethertype IPv4 (0x0800), length 98: 10.0.1.4
> 10.0.1.10: ICMP echo
request, id 32513, seq 25753, length 64
16:10:32.489644 fa:16:3e:0e:58:7b > fa:16:3e:6a:d3:e8, ethertype IPv4 (0x0800), length 98: 10.0.1.10
> 10.0.1.4: ICMP echo
reply, id 32513, seq 25753, length 64
16:10:33.489685 fa:16:3e:6a:d3:e8 > fa:16:3e:0e:58:7b, ethertype IPv4 (0x0800), length 98: 10.0.1.4
> 10.0.1.10: ICMP echo
request, id 32513, seq 25754, length 64
16:10:33.489800 fa:16:3e:0e:58:7b > fa:16:3e:6a:d3:e8, ethertype IPv4 (0x0800), length 98: 10.0.1.10
> 10.0.1.4: ICMP echo
reply, id 32513, seq 25754, length 64
^C
```

6. Obtain a list of all the mirrored ports.

```
neutron_vpp_13881 [root@k07-compute-1 /]# vpp-portmirror-list
VPP interface VPP-side span port Kernel-side span port Neutron port
```

```
------------- ------------------ -------------------- ------------
VirtualEthernet0/0/0 tapcli-0 tap88b637e4 net-vpp.port:88b637e4-43cc-4ea2-8a86-2c9b940408ec
VirtualEthernet0/0/1 tapcli-1 taped8caee2 net-vpp.port:ed8caee2-f56c-4156-8611-55dde24f742a
```

7. Remove the mirrored port.

```
neutron_vpp_13881 [root@k07-compute-1 /]# vpp-portmirror-delete -p ed8caee2-f56c-4156-8611-55dde24f742a
===============[ Port Mirroring Operation]=========================
2018-05-14 23:18:49 UTC [ info] Interface inside vpp is VirtualEthernet0/0/1 for Openstack
port:ed8caee2-f56c-4156-8611-
55dde24f742a
Deleted.
2018-05-14 23:18:49 UTC [ info] Port:ed8caee2-f56c-4156-8611-55dde24f742a is now un-mirrored
```

VXLAN-EVPN Setup

VXLAN-EVPN Setup

Choose single VXLAN or multi-VXLAN (multi refers to 2) network terminating on the same box on day-0. Two vxlan segments such as vxlan-tenant and vxlan-ecn are defined.

For single VXLAN network, define only the vxlan-tenant. For two-VXLAN network, define vxlan-ecn segment along with vxlan-tenant network.

To enable VXLAN/EVPN in Cisco VIM, define the following in the setup-data file during the Day-0 deployment. Optionally, you can overload the configuration with that of head-end-replication for static VXLAN configuration.

1. In the **Networking** section, define the segment vxlan-tenant:

```
NETWORKING:
... networks:
.....
- # only needed when NETWORK_OPTIONS is vxlan, and TOR is Cisco NCS5500
vlan_id: <2003>
subnet: <191.168.11.0/25>
gateway: <191.168.11.1>
## 'pool' can be defined with single ip or a range of ip pool:
- <191.168.11.2,191.168.11.5>
- <191.168.11.7 to 191.168.11.12>
- <191.168.11.20>
segments:
  vxlan-tenant
   # only needed when NETWORK_OPTIONS is vxlan, and TOR is Cisco NCS5500, and second VXLAN segment is
required
vlan_id: <2005>
subnet: <191.165.11.0/25>
gateway: <191.165.11.1>
## 'pool' can be defined with single ip or a range of ip pool:
- <191.165.11.2,191.165.11.5>
- <191.165.11.7 to 191.165.11.12>
- <191.165.11.20>
segments:
vxlan-ecn
```

2. Define the vxlan section under NETWORK_OPTIONS, only allowed for Cisco NCS 5500 as ToR:

```
# Optional, only allowed for NCS-5500 as tor NETWORK_OPTIONS:
vxlan:

vxlan-tenant:

provider_network_name: <name of provider network>
bgp_as_num: <int value between 1 and 232-1>
bgp_peers: ['ip1', 'ip2'] ---> list of min length 1, Peer Route Reflector IPs
bgp_router_id: 'ip3' ---> Indicates the router ID to use for local GoBGP cluster, part of vxlan-tenant
network but not in the pool
head_end_replication: # Optional, can be brought in as reconfigure
-    vtep_ips: vni_id1:vni_id2, vni_id3, ... (upto as many Remote POD vteps, as required)

vxlan-ecn:

provider_network_name: <name of provider network> bgp_as_num: <int value between 1 and 232-1>
bgp_peers: ['ip1', 'ip2'] ---> list of min length 1, Peer Route Reflector IPs
bgp_router_id: 'ip3' ---> Indicates the router ID to use for local GoBGP cluster, part of vxlan-ecn
network but not in the pool
head_end_replication:    # Optional and reconfigurable
- vtep_ips: vni_id1:vni_id2, vni_id3, ... (upto as Remote POD many vteps, as required)
```

⚠ Following are the assumptions for the HER feature:

- VNIs can repeat across two or more remote POD VTEPs for HA.
- VNIs cannot repeat for the same remote POD VTEP.

- Within the same network segment, no remote POD VTEPs IP adddress can repeat.

3. In the **SERVERS** section, define vxlan_bgp_speaker_ip for each controller node.

> ⚠ The vxlan_bgp_speaker_ip belongs to the vxlan network, but not part of the IP pool defined in the vxlan segment.

```
control-server-1:
.....
# bgp_speaker_addresses: {vxlan-tenant: <ip address> # <== 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 as defined in the
network section

vxlan-ecn: <ip address>} # <== optional, only needed for multi-vxlan scenario and only when
NETWORK_OPTIONS is vxlan network,
for controller nodes only; IP belongs to the vxlan-ecn network, but not part of the pool as defined in
the network section
```

> ⚠ Setting up the BGP route-reflector and accessing it over the VXLAN network from the three controllers is outside the scope of Cisco VIM automation.

For head-end-replication option, define Local POD vtep_ips on all servers that act as compute nodes:

```
# vtep_ips:{vxlan-tenant: <ip address>, vxlan-ecn: <ip address>} #IPs must belong to the associated IP
pool of vxlan-tenant and vxlan-ecn
  networks
```

From release Cisco VIM 2.4.9, the BGP session between the controllers and route-reflector is set to be Layer 3 adjacent. By default, it is L2 adjacent. To support Layer 3 adjacency, define bgp_mgmt_address for each controller.

```
# bgp_mgmt_addresses: {vxlan-tenant: <ip address >, vxlan-ecn: <ip address>} # <== optional, only when
NETWORK_OPTIONS
is vxlan network, for contoller node only, needed when BGP peer is  over L3. IP addresses are unique and
are from management network,
but not part of pool.
```

Head-End Replication Option

Enabling Head-End Replication (HER) Option

For the releases Cisco VIM 2.4.9 and later, the multi-VXLAN EVPN based design optionally supports the static implementation of VXLAN technology using head-end replication. HER helps leverage the VXLAN technology, regardless of the hardware or software limitation of the VXLAN feature set at the remote end of the VTEP tunnel.

With the static information defined in the HER setup_data, VPP performs the head-end replication to all defined remote VTEPs and the Layer-2 Forwarding Information Base (L2FIB) MAC-IP table is populated based on flood and learn. When EVPN coexists with HER, Cisco VIM considers them as two different sets of BGP speakers each giving the information which ends up in the same etcd FIB table.

In Cisco VIM, the EVPN acts as the primary mechanism and HER as the fallback methodology. You can add or remove HER to or from an existing EVPN pod through Cisco VIM reconfigure option.

Following are the assumptions for the HER feature:

- VNIs can be allowed in the range of 1 to 65535.
- VNIs can be repeated across two or more remote POD VTEPs for HA.
- VNIs cannot be repeated for the same remote POD VTEP.
- Within the same network segment, no remote POD VTEPs IP address can be repeated.

To enable HER, follow the below steps:

1. Ensure that multi-VXLAN feature exists in day-0 configuration of the setup_data. Add a new section called head-end-replication under the NETWORK_OPTIONS -> vxlan -> vxlan-ecn and vxlan-tenant sections.

```
NETWORK_OPTIONS:
vxlan:
vxlan-tenant:
head_end_replication: # Optional and reconfigurable
- vtep_ips: vni_id1:vni_id2, vni_id3, ... (upto as many remote POD vteps as required)
vxlan-ecn:
head_end_replication: # Optional and reconfigurable
- vtep_ips: vni_id1:vni_id2, vni_id3, ... (upto as many remote POD vteps as required)

Update all compute nodes with vtep_ip information under the SERVERS section:
SERVERS:
Compute1:
...

For head-end-replication option, define vtep_ips on all servers that act as control and compute node

# vtep_ips: {vxlan-tenant: <ip address>, vxlan-ecn: <ip address>} # These IPs must belong to the
associated IP pool of
vxlan-tenant and vxlan-ecn networks, and must match the existing assigned vtep_ip for EVPN as they are
brought in as
part of reconfiguration.
```

2. To determine the respective vtep_ip on a per segment and server basis, run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# cd /root/installer-<x.y.z>/tools
[root@mgmt1 ~]#./vtep_ip_server_mapping.py
# Update the setup_data to include the HER section and vtep_ip corresponding to the network segment
for the respective servers
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Enabling BGP Adjacency

Enabling BGP Adjacency

From release Cisco VIM 2.4.9 onwards, the Layer 2 or Layer 3 BGP adjacency with the peering route-reflector is supported.

> ⚠ For releases prior to Cisco VIM 2.4.9, only Layer 2 BGP adjacency is supported.

Following are the assumptions made to move a pod from a Layer 2 BGP adjacency to that of Layer 3:

- The controllers with the bgp_speaker_addresses peer with the route-reflector over Layer 3.
- This option is only available when vxlan is enabled as NETWORK_OPTIONS.
- Every vxlan segment (vxlan-ecn and vxlan-tenant) will have its own IPs.
- IPs are picked up from management subnet, but they do not belong in the management pool.
- Switching from Layer 2 to Layer 3 peering is only supported, but not vice-versa.
- Once enabled, the only way to change the bgm_mgmt_address is through a replace controller.

To enable layer BGP adjacency between controllers and peering route reflector, follow the below steps:

1. Update all controller nodes with bgp_mgmt_address where the IPs reside in the management subnet, but not in the management IP pool:

   > ⚠
   > - VXLAN feature must exists in day-0 configuration of the setup_data.
   > - One unique IP must be available per VXLAN segment.

   ```
   SERVERS:
   Control1:
   ...
   # bgp_mgmt_address: {vxlan-tenant: <ip address>, vxlan-ecn: <ip address>} # These IPs must belong to
   the
   management segment, but not in the management IP pool.
   ```

2. Run the following reconfiguration commands:

   ```
   [root@mgmt1 ~]# cd /root/ [root@mgmt1 ~]# mkdir MyDir
   [root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
   # update the setup_data to include HER section and vtep_ips info
   [root@mgmt1 ~]# cd /root/MyDir/
   [root@mgmt1 ~]# vi setup_data.yaml [root@mgmt1 ~]# cd ~/installer-xxxx
   [root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
   ```

Re-binding of Neutron Port

Re-binding of Neutron Port to Another Network

Overview

In OpenStack implementation, once a Neutron port is created from a Neutron network, the ownership of the port cannot be changed. In some cases, the administration needs to dynamically change the VM port ownership even if it is already bound to a VM. This is particularly useful in case of VXLAN, where it is required to change the VNI associated with an existing port, to introduce a new VNF-VM in an existing service chain.

For example, you can start with:

Net1 – VM1 – Net2

And the goal is to change to:

Net1 – VM1 – Net3 – VM2 – Net2

Limitations

To meet specific customer use-case, the re-binding feature is developed within the following limitations:

1. The API is designed to have a short period of networking connectivity downtime, during the unbind/re-bind process. Essentially, it unbinds the port and rebinds it again from ML2 agent perspective.
2. This is only tested and supported in ML2/VPP context. The support for OVS may not work, and needs further development to have consistent behavior across ML2 drivers.

Prerequisites

1. The new network that will own the port must belong to the same project as the previous old network.
2. The MAC_address must be unique, so that no mac-address duplication exists in the newly migrated network.

> The Neutron server validates the above cases and throws errors if and when they are not satisfied.

Neutron Port Re-binding

Following are the steps to perform neutron re-binding :

1. Remove the fixed_ip on the port. This clears the IP allocation DBs in Neutron, and configures the DHCP agent to have the right information:

```
openstack port set --no-fixed-ip <PORT_ID>
```

2. Migrate the port to the new network:

```
openstack port set <PORT_ID> --network-id <NEW_NETWORK_ID>
```

3. Add the fixed_ip of the new subnet back to the port:

```
openstack port set <PORT_ID> --fixed-ip subnet=<NEW_SUBNET_ID>
```

Managing Provider/Tenant VLAN Ranges

Managing Provider/Tenant VLAN Ranges

You can increase or decrease the provider and tenant VLAN ranges post pod installation.

Increasing Provider and Tenant VLAN Ranges

Increasing provider/tenant VLAN ranges is applicable to C-series and B-series pod that is enabled with Cisco UCS Manager plugin. The B-series pod running without Cisco UCS Manager plugin cannot use this feature because of the inherent Day 0 networking configuration to be done in FI.

> ⚠ You should have the tenant and provider networks enabled on the pod from Day 0.

To increase provider and tenant VLAN ranges, enter the TENANT_VLAN_RANGES and/or PROVIDER_VLAN_RANGES in the *setup_data.yaml* file and run the reconfigure command through Ciscovimclient as follows:

```
TENANT_VLAN_RANGES: old_vlan_info, new_vlan_info
or/and
PROVIDER_VLAN_RANGES: old_vlan_info, new_vlan_info
```

Decreasing Provider and Tenant VLAN Ranges

To decrease provider and tenant VLAN ranges, update the TENANT_VLAN_RANGES and/or PROVIDER_VLAN_RANGES to be a subset of the original one in the setup_data.yaml file and run the reconfigure command through Ciscovimclient as follows:

```
TENANT_VLAN_RANGES: subset_old_vlan_info
PROVIDER_VLAN_RANGES: subset_old_vlan_info
```

> ⚠ You cannot remove and add new VLANs at the same time. Also if you remove VLAN, they cannot be reduced to less than 2 and 1 VLANs for tenant and provider network, respectively.

Changing the Pod

To change the pod, copy the setupdata into a local directory and update it manually by running the following command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
```

Update the setup_data, by running the following command:

```
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1~]# vi my_setup_data.yaml (update the setup_data with the right info)
```

Run the reconfiguration command as follows:

```
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ./ciscovimclient/ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

> ⚠ While using auto-ToR via ACI APIs without the APIC plugin, ensure that you update the vim_apic_networks section with the right VLAN information as part of the reconfiguration option.

Migrate SRIOV

Migrate SRIOV in VIC/NIC Pod

To use this feature, ensure that both the card types are available on the SRIOV compute nodes of the pod and with one of the card type participating in SRIOV as part of installation, and then execute the following steps:

You can redeploy the SRIOV ports between 2-X520 and 2-XL710 in a Cisco VIM pod where the control plane and data plane are running OFF Cisco VIC. This is driven through an optional parameter SRIOV_CARD_TYPE listed in the *setup_data.yaml*.

It is assumed that all computes participating in SRIOV has two sets of card types. Reconfiguration fails if the card type with a total of four ports is not available. Cisco recommends you to have two of each of the card type inserted on a per-compute basis, so that the correct network ports from the target network cards are picked by the orchestrator. However, if the SRIOV_CARD_TYPE is present during the fresh installation or during add compute operation, the SRIOV_CARD_TYPE parameter is given preference for the target/configured card type.

You can define the SRIOV_CARD_TYPE at a per-compute level, to override the global definition. This option allows some computes to run with XL-710 and other computes to run with X-520 for SRIOV ports. It should be noted that computes without SRIOV can co-exist in this pod.

1. Take a backup of the setupdata file and update the file manually with the configuration listed below:

```
SRIOV_CARD_TYPE: <X520 or XL710>
and/or update the hardware_info at a per compute level (see example below)
compute-xx:
hardware_info: {SRIOV_CARD_TYPE: <XL710 or X520>}
```

2. Run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
# update the setup_data to include the target SRIOV card type
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Augmenting VIC/NIC Pods

Augmenting VIC/NIC Pods

From release Cisco VIM 2.4.9 onwards, the augmentation of an existing M4 VIC/NIC based pod (some computes have X520, while others have XL710 for SRIOV), with the M5-based VIC/NIC (40G) computes is supported. To use this augmentation feature, you must define the SRIOV_CARD_TYPE at a per compute level (default is X520).

You can add M5-based 40G VIC/NIC computes into the pod in the following scenarios:

Use Case 1: If you run a pod with M4-based computes having only X520 cards, execute the reconfiguration operation and define the SRIOV_CARD_TYPE as XL710 under the hardware_info section of the target compute, to add the compute of M5 with 40G Cisco VIC and two XL710 cards,.

Use Case 2: If you run the pod with M4-based VIC/NIC computes having XL710 cards, execute the add compute operation and define the SRIOV_CARD_TYPE as XL710 for the target compute, to add M5-based compute nodes with XL710 cards.

The following steps 1 through 3 are not applicable for Use Case 2, and you can directly add/remove compute when required.

Identify if the pod has M4 computes running with two XL710 or not, that is, whether the pod is running with Use Case 1 or Use Case 2.

1. If the pod is running with Use Case 1, execute the following command:

```
# ciscovim reconfigure
```

2. Take a backup of the setupdata file and update the file manually with the configuration listed below:

```
Update the hardware_info at a per compute level (see example below)
compute-xx:
hardware_info: {SRIOV_CARD_TYPE: <XL710 or X520>}
```

3. Run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/ [root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/ # update the setup_data to
include the target SRIOV card type [root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml [root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim --setupfile /root/MyDir/setup_data.yaml add-computes <m5compute1, ...>
```

P-GPU

P-GPU Support

From Cisco VIM 3.4.1, GPU is supported in a passthrough mode. In this mode, the entire physical GPU card is available to the VM.

You can enable GPU in passthrough mode on a per UCS server basis. You can also enable GPU on a per-server basis (post install) through an add compute operation for the given server. As part of the validation, Cisco VIM checks for the presence of the right number of GPU cards. Hence, you must remove the GPU card from the server when you do not intend to use it, else the Cisco VIM hardware validation will fail.

Before you Begin

- The target server must have a minimum CIMC version of 4.0(2f).
- Only Tesla T4 GPU card is supported.
- To enable GPU on a compute node with Tesla T4 cards, you must include the following information about the target server in the *hardware_info* section of the *setup_data.yaml* file:

```
SERVERS:
  target_server_name:
    hardware_info: {NUM_GPU_CARDS: x} # where x is either 1 or 2 depending on if we have 1 or 2
Tesla T4 cards plugged in.
```

To use P-GPU in a given VM:

1. You must use a guest image with the right Nvidia drivers for the Tesla T4 card while spawning a VM with GPU, else the VM will crash on bootup.
2. Modify the OpenStack flavor to add the GPU alias:

   ```
   openstack flavor set gpuflavor –property "pci_passthrough:alias"="t4gpu:x"
   ```

   In the above example, x is 1 for one T4 card and 2 for two T4 cards. Depending on the value of x, the VM will pass through either one or two physical GPU cards.
3. Hide the KVM on the guest VM to bypass the Nvidia driver limitation with the KVM hypervisor.

   ```
   openstack image set gpuimage –property img_hide_hypervisor_id=true
   ```

4. Launch a VM with the above flavor to see the above card passthrough.

   After you perform the above steps, verify the card passthrough by using the *nvidia-smi* command inside the guest VM.

SR EVPN

Deploying Segment Routing EVPN

Before you Begin

- A pair of NCS 5500 acts as the ToR. As Cisco VIM supports only a single pair of NCS, you must properly scale your NCS and choose the right NCS-5500 SKU, so that all ports of all the nodes can be connected to this single pair of NCS. Ensure that you can increase the port count when selecting the NCS model.
- You cannot enable both SR EVPN and VXLAN EVPN on the same Cisco VIM pod. Only one forwarding mechanism can exist within a single pod.
- Cisco VIM administrators must provide the SR network and subnet information for overlays, and EVI or BD label. Cisco VIM does not manage the SR EVPN, it only attaches to an existing SR EVPN.
- You must provide the BGP configuration to the Cisco VIM installer during deployment.
- Cisco VIM 3.4.1 does not support traffic engineering policies for dynamic path selection through BGP SR extensions, or any explicit path selection through CLI or any interaction with an SDN controller.
- Only single homing L2 routes are supported. Only EVPN Type 2 and Type 3 are exchanged with the EVPN Route Reflectors (RR).
- You can enable this feature in Cisco VIM as a Day 0 option using either *setup_data.yaml* file or Unified Management when you install the pod.
- You cannot convert an existing pod to this SR-enabled forwarding mechanism, even if it is set up to use VPP for VLAN or VXLAN based forwarding.

Cisco VIM 3.4.1 does not support VMTP and NFVbench with SR EVPN.

For SR EVPN deployment, you must update the *setup_data.yaml* file as given below :

```
SERVERS:
  control-server-1:
    bgp_speaker_addresses: {sr-mpls-tenant: <ip address from sr-mpls-tenant network but not part of the pool>}
    bgp_mgmt_addresses: {sr-mpls-tenant: <ip address from management network but not part of the pool>}  # <==
optional, only when NETWORK_OPTIONS is sr-mpls network, for controller node only, needed when BGP peer is over
L3
    vtep_ips: sr-mpls-tenant: <ip address from sr-mpls-tenant network and part of the pool>}  # <== needed for
compute and control nodes
    sr_global_block: {prefix_sid_index: <int between 0 and 8000>, base: <int between 16000 and 1048576>}  # for
sr-mpls, unique and must exist for all controllers/computes, sum of prefix_sid_index and base has to be unique
across all servers
    dp_tor_info: {switch_a_hostname: ethx/y, switch_b_hostname: ethx/y} #For sr-mpls dp_tor_info is mandatory
and has no po info

sr_global_block will exist for all computes and controllers. These are the segment identifiers used to
associate with the Loopback IPs of the VPP nodes
tor_info will exist only for the control plane links.
dp_tor_info will not be port channel. SR being a Layer 3 feature will rely on ECMP links for data plane
redundancy.
vtep_ips is the loopback IP of the VPP which will be distributed by BGP LU for VPP reachability.
prefix sid is computed from sr_global_block section where base and index is defined.
NETWORK OPTIONS:
A new NETWORK OPTIONS section called sr-mpls has been introduced to support SR MPLS.
#  ######sr-mpls options #####
#  physnet_name: <unique_name> # Optional. Default is "physnet1"
#  enable_ecmp: <true or false>. # Optional (For SR, it is true. default is false), and only for vpp
#  ecmp_private_pool: <cidr> # Optional, Only if enable_ecmp is true.
#  sr-mpls:     # mutually exclusive to vxlan; will work with VPP and NCS-5500 only for now
#    sr-mpls-tenant:
#       physnet_name: <unique_name>
#       bgp_as_num: <int value between 1 and 4294967295> # unique across all AS
#       bgp_peers: ['ip1'] ---> list of length 1, Peer Route Reflector IPs
#       bgp_router_id: 'ip3' ---> The router ID to use for local GoBGP cluster

ecmp_private_pool is the range used to burn private IPs for the VPP uplinks to the aggregation layer.
enable_ecmp is used to enable ecmp links
sr-mpls-tenant is the key word to enable sr provider networking.
bgp_as_num is the bgp as number of the remote PE device
bgp_peer is the bgp speaker loopback address
```

```
bgp_router_id will be the router id address used by the gobgp speakers


NETWORKING:
A new networking section called sr-mpls-tenant has been introduced to support SR MPLS.
NETWORKING:
  Networks:
 -
    vlan_id: <vlan_id>
    subnet: <subnet in cidr>
    gateway: <gateway address>
    pool:
      - <a.b.c.d,e.f.g.h>
      - <i.j.k.l to m.n.o.p>
      - <q.r.s.t>

    segments:
      - sr-mpls-tenant

gateway is the BVI ip address to be used for the L3 gateway for CVIM control plane
pool is the address pool of the public addresses
segments will contain sr-mpls-tenant as a provider network
vlan_id is the id used to carve a sub interface for SR control plane from
```

Cinder Volume Multi-attach

Cinder Volume Multi-attach with Cisco VIM

Overview

Attaching a volume to multiple hosts or servers simultaneously is used for active/active or active/standby scenarios. This feature is available in Cisco VIM 3.4.1 because of upstream support.

For more information about this feature, see the OpenStack documentation at https://docs.openstack.org/cinder/latest/admin/blockstorage-volume-multiattach.html.

Assumptions and Caveats

1. Ensure that a multi-attach or clustered file system is used on the volumes, else there is a high probability of data corruption. If two VMs attach to the same volume, you must ensure that only one of the two VMs mounts the file system at a time.
2. By default, secondary volume attachments are made in read or write mode. This setup can cause problems for operations such as volume migration. This happens even if you create the volume with read-only permission.
3. Boot from volume is not supported with multi-attach volume.
4. Horizon does not work with volume attach to instance.
5. Use the nova client instead of OpenStack client for multi-attach volume.

Creating Multi-attach Volume

To attach a volume to multiple hosts or servers:

1. To attach a volume to multiple hosts or servers, you need to have the multi-attach flag set to true in the volume details.

   ```
   $ cinder type-create multiattach
   $ cinder type-key multiattach set multiattach="<is> True"
   ```

2. To create the volume you need to use the volume type you created earlier.

   ```
   $ cinder create <volume_size> --name <volume_name> --volume-type <volume_type_uuid>
   ```

   For example:

   ```
   $ cinder create 10 --name multi --volume-type bb5f35a1-bdfd-4744-b9f9-c0752598881d
   ```

3. Use the nova client to attach the volume to the instance.

   ```
   $ nova volume-attach INSTANCE_ID VOLUME_ID auto
   ```

   For example,

   ```
   $ nova volume-attach testvm3 785959c4-889d-421e-985e-074d488ec823
   ```

Configuring Multiple-storage Backends in Ceph

To configure multiple storage backends, enter the following commands:

```
cinder type-create cephssd
```

```
cinder type-key cephssd set volume_backend_name=ceph-ssd

cinder type-key cephssd set multiattach="<is> True"
```

Virtual GPU Support

Virtual GPU (vGPU) Support

Overview

From Cisco VIM 3.4.3, vGPU is supported in Tech-preview mode. In this mode, the NVIDIA virtual GPU software is installed at the virtualization layer along with the hypervisor. The NVIDIA virtual GPU software creates virtual GPUs that enable each virtual machine (VM) to share a physical GPU installed on the server or allocate multiple GPUs to a single VM to power the most demanding workloads. As the CPU workload is offloaded to GPU, better user experience and demanding engineering/creative applications are supported in a virtualized cloud environment.

You can also enable vGPU on a per-server basis via fresh installation or through an add compute operation for the given server. As part of the validation, Cisco VIM checks for the presence of the right number of GPU cards. You must remove the GPU card from the server when it is not required, as it can cause Cisco VIM hardware validation failure.

Enabling GPU

Before you begin

- The target server must have a minimum CIMC version of 4.0(2f).
- Only Tesla T4 GPU card is supported.
- Since Cisco does not have license to redistribute the NVIDIA rpm, obtain the *NVIDIA-vGPU-rhel-7.6_3.10.0_957.27.2-440.43.x86_64.rpm* from NVIDIA and copy it to */root/installer-xxx/openstack-configs* directory.
- Ensure that the sha1 checksum of the *NVIDIA-vGPU-rhel-7.6_3.10.0_957.27.2-440.43.x86_64.rpm* file is: `9a9c862547b153a32ec98ff092cc4a01a5ec7cc1`.
- All guest VGPU drivers need to be based on NVIDIA 10.X GRID software. This is a required as the compute host and guest major versions need to match up for NVIDIA support. For the guest image, obtain a valid license from NVIDIA and ensure that the version of NVIDIA GRID driver is 10.x.

To enable GPU on a compute node with Tesla T4 cards, you must include the following information about the target server in the *hardware_info* section of the *setup_data.yaml* file:

```
SERVERS:
  target_server_name:
    hardware_info: {NUM_GPU_CARDS: x, VGPU_TYPE: <vgpu_type>} # where x is either 1 or 2 depending on whether
the Tesla T4 cards plugged in is 1 or 2.

#Valid VGPU types: T4-1B, T4-2B, T4-2B4, T4-1Q, T4-2Q, T4-4Q, T4-8Q, T4-16Q, T4-1B4, T4-4C, T4-8C, T4-16C
```

After installation, create a flavor that supports VGPU via the following command:

```
# openstack flavor set vgpu_1 --property "resources:VGPU=1"
```

In OSP13 release, all hypervisors that support virtual GPUs accepts only a single virtual GPU per instance. Hence, ensure that you do not set more than one VGPU.

Forwarding ELK Logs

Forwarding ELK logs to External Syslog Server

Cisco VIM supports backup and recovery of the management node. To keep the process predictable and avoid loss of logs, the software supports the capability of forwarding the ELK logs to multiple external syslog server. It supports minimum of one and maximum of four external syslog servers. The capability is introduced to enable this feature after the pod is up and running with Cisco VIM through the reconfigure option.

The Syslog export reconfigure option supports the following options:

- Forwarding of ELK logs to external syslog server on a pod that is already up and running.
- Reconfiguration of the existing external syslog setting to point to a different syslog cluster.

1. Before launching the installation, update the *setup_data.yaml* file with the following:

```
###################################
SYSLOG EXPORT SETTINGS
###################################
SYSLOG_EXPORT_SETTINGS:
-
remote_host: <Syslog_ipv4_or_v6_addr> # required IP address of the remote syslog server
protocol : udp # defaults to udp
facility : <string> # required; possible values local[0-7] or user severity : <string; suggested value:
debug>
port : <int>; # defaults, port number to 514
clients : 'ELK' # defaults and restricted to ELK;

remote_host: <Syslog_ipv4_or_v6_addr> # IP address of the remote syslog #2 (optional)
server protocol : udp # defaults to udp
facility : <string> # required; possible values local[0-7]or user
severity : <string; suggested value: debug>
port : <int>; # defaults, port number to 514
clients : 'ELK' # defaults and restricted to ELK;
```

2. Take a backup of the *setupdata* file and update the file manually with the configuration listed in the preceding section. Then, run the reconfiguration command as follows:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# # update the setup_data to include Syslog Export info
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

With this configuration, you can export ELK logs to an external syslog server. On the remote host, verify if the logs are forwarded from the management node.

Most of the information other than the remote host information is not needed. Also, the client list is restricted to ELK only.

Network File System

Network File System (NFS) for ELK Snapshot

Cisco VIM optionally supports NFS for ELK snapshots. The remote location specified in the configuration must allow user elasticsearch (2020) and group mercury (500) to read from or write to the path specified in remote_path of the remote_host server.
Before launching the installation, update the *setup_data.yaml* file with the following:

```
###################################
 ## ES_REMOTE_BACKUP
###################################
#ES_REMOTE_BACKUP:    # Set if Elasticsearch backups uses a remote host.
# service: 'NFS'    # Only value supported is NFS.
# remote_host: <ip_addr>    # IP of the NFS server.
# remote_path: </root/es_remote> # Path to location of the backups in the remote server
```

With this configuration, the ELK snapshots are hosted at the remote NFS location. Thereby, ensuring that the management node does not run out of disk space. You can add this configuration to a pod that is already up and running.

TTY Logging

TTY Logging

Cisco VIM supports TTY logging on the management node and cluster hosts through the option in the *setup_data.yaml* file. By default, the TTY logging feature is not enabled, but available only during installation. If SYSLOG_EXPORT_SETTINGS is configured, the TTY audit messages are available in local syslog, Kibana dashboard, and remote syslog.

For the TTY logging to take effect in the management node, reboot the management node based on the customer downtime window.

At the end of the installation, a message **Management node needs to be rebooted for TTY logging to take effect** is displayed.

Before launching the installation, update the *setup_data.yaml* file with the following information:

```
# TTY Logging with pam.d and auditd. Events available in Kibana and remote syslog, if syslog export is enabled
ENABLE_TTY_LOGGING: <True or False>    # default value is False
```

Branding VM Workloads

Branding VM Workload

In Cisco VIM 3.4.3, you can check whether the VMs are running on Cisco VIM platform from the VM itself. You can execute the following within the VM and look for Cisco VIM under the product name:

```
$ sudo dmidecode -t system
# dmidecode 3.1
Getting SMBIOS data from sysfs.
SMBIOS 2.8 present.


Handle 0x0100, DMI type 1, 27 bytes
System Information
                Manufacturer: Cisco Systems, Inc.
                Product Name: Cisco VIM
                Version: 3.3.35
                Serial Number: 71e1c3cd-77c5-8742-ad3d-2cbf99f5d19e
                UUID: e5afbb33-9682-4986-bf53-108667ac796f
                Wake-up Type: Power Switch
                SKU Number: Not Specified
                Family: Virtual Machine


Handle 0x2000, DMI type 32, 11 bytes
System Boot Information
                Status: No errors detected
```


The branding feature introduces some implications to VNFs since Cisco VIM 3.4.3 release. As few VNFs depend on the output of dmidecode, this branding feature is reverted in Cisco VIM 3.4.4 and can be re-visited in future.

Administration

Administration

Managing Pods

Managing Cisco NFVI Pods

General Guidelines

General Guidelines

You can perform OpenStack management operations on Cisco NFVI pods including addition and removal of Cisco NFVI compute and Ceph nodes, and replacement of controller nodes. Each action is mutually exclusive. You can perform only one pod management action at a time. Before you perform a pod action, ensure that the following requirements are met:

- The node is part of an existing pod.
- The node information exists in the setup_data.yaml file, if the pod management task is removal or replacement of a node.
- The node information does not exist in the setup_data.yaml file, if the pod management task is to add a node.

For more information on operations that can be performed on pods, see Managing Hosts.

The setup_data.yaml file is the only user-generated configuration file that is used to install and manage the cloud. While many instances of pod management indicate that the setup_data.yaml file is modified, the administrator does not update the system generated setup_data.yaml file directly.

> ⚠ To avoid translation errors, ensure that you do not copy and paste the commands from the documents to the Linux CLI.

To update the *setup_data.yaml* file, follow the below steps:

1. Copy the setup data into a local directory:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
```

2. Update the setup data manually:

```
[root@mgmt1 ~]# vi my_setup_data.yaml (update the targeted fields for the setup_data)
```

   a. Run the reconfiguration command:

```
[root@mgmt1 ~]# ciscovim --setupfile ~/MyDir/<my_setup_data.yaml> reconfigure
```

   You can edit and enable a selected set of options in the *setup_data.yaml* file using the reconfigure option. After installation, you can change the values of the feature parameters. Unless specified, Cisco VIM does not allow you to undo the feature configuration. During reconfiguration, all other pod management activities are disabled. Post-update, the normal cloud management operations commence. If reconfigured OpenStack services fail, all the subsequent pod management operations are blocked. To resolve the situation through CLI, contact Cisco TAC:

   The following table shows the list of features that can be enabled or whose values can be changed post pod deployment:

Features Enabled Post Pod Deployment	**Comment (Repeated Redeployment Value)**
Optional OpenStack services	• Heat: OpenStack Orchestration Program (False) • LDAP: Works only with Keystone v3. Full or partial reconfiguration can be done. Except for domain, all attributes are reconfigurable. (Partial) • Ironic: Baremetal workload post installation (False) • Container: Cloud-native workload (False)
Pod monitoring	• CVIM-MON: monitoring host and service level with or without *ui_access* (False) • NFVIMON: Third-party monitoring from host to service level with aid of Cisco advance services. Supports un-configuration of the feature
Export of Elasticsearch, Fluentd, and Kibana (EFK) logs to external syslog server	Reduces single point of failure on management node and provides data aggregation (True)
NFS for Elasticsearch snapshot	NFS mount point for Elasticsearch snapshot is used, so that the disk on management node is not full (False)
Admin source networks	A list of allowed filters to access management node admin service over IPv4 or IPv6 (True)
NFVBench	

	Tool to help measure cloud performance. The management node needs a dedicated 10G/40G Intel NIC (4x10G 710 or 2x40G XL710 Intel NIC) (False)
EFK settings	Enables you to set EFK rotation frequency and size (True)
OpenStack service password	Implemented for security reasons, so that OpenStack passwords can be reset on-demand (True)
CIMC Password Reconfigure post installation	Implemented for security reasons, so that CIMC passwords for C-series pod can be reset on-demand (True)
TENANT_VLAN_RANGES and PROVIDER_VLAN_RANGES	You can increase or decrease the tenant and provider VLAN ranges on a pod that is up and running. It gives flexibility in network planning (True)
DHCP reservation for VM's MAC addresses	Allow DHCP reservation for virtual machine MAC addresses, to get the same IP address always regardless of the host hypervisor or operating system they are running (True)
Enable TRUSTED_VF on a per (SR-IOV) compute basis	Allows virtual functions to become trusted by the physical function and to perform some privileged operations such as enabling VF promiscuous mode and changing VF MAC address within the guest (True)
Support of multiple external syslog servers	Ability to offload the OpenStack logs to a maximum of four external syslog servers post-installation (True)
Replace of failed APIC hosts and add more leaf nodes	Ability to replace failed APIC hosts, and add more leaf nodes to increase the fabric influence (True)
Make Netapp block storage endpoint secure	Ability to move the Netapp block storage endpoint from clear to TLS post deployment (False)
Auto-backup of management Node	Ability to enable/disable auto-backup of management node. (True)
VIM Admins	• Ability to configure non-root Cisco VIM administrators (True) • Ability to configure Cisco VIM admins authenticated by LDAP (True)
EXTERNAL_LB_VIP_FQDN	Ability to enable TLS on external_vip through FQDN (False)
EXTERNAL_LB_VIP_TLS	Ability to enable TLS on external_vip through an IP address (False)
http_proxy and/or https_proxy	Ability to reconfigure http and/or https proxy servers (True)
Admin privileges for VNF Manager (ESC) from a tenant domain	Ability to enable admin privileges for VNF manager (ESC) from a tenant domain (False)
SRIOV_CARD_TYPE	Mechanism to switch between 2-X520 and 2-XL710 as an SRIOV option for Cisco VIC NIC settings at a global level and per compute level through reconfiguration. In the absence of per compute and global level, X520 card type is set by default (False)
Reset of KVM console passwords for servers	Aids to recover the KVM console passwords for servers (True)
Horizon behind NAT or with DNS alias(es)	Ability to host Horizon behind NAT or with DNS aliases (False)
Login banner for SSH sessions	Supports configurable login banner for SSH sessions (True)
Ability to add Layer-3 BGP session	Ability to switch BGP sessions from Layer 2 to Layer 3 in the presence of VXLAN configuration (False)
Add/remove of head-end-replication option	Ability to add or remove head-end-replication option, in the presence of VXLAN configuration (True)
Enabling Cloud Settings	Ability to set horizon and keystone settings as a reconfigurable options (True)
Vault	Ability to enable vault on Day 2 (False)
Identity, Policy and Audit (IPA) enablement	Ability to enable IPA as a Day 2 option (False)
Enable RAM and CPU Allocation Ratio	Ability to enable RAM and CPU allocation ratio on a per server basis as a Day 2 option (True)
NTP configuration change	NTP information update listed in NETWORKING section (maximum of 4 entries) (True)
DNS configuration change	Domain Name Server (DNS) information update listed in NETWORKING section (True)

All reconfiguration features contain repeated re-deployment option set to True or False. If repeated re-deployment is set to True, the values associated to the feature can be changed, otherwise, the feature can be deployed only once. Un-installation of the feature is only supported as an exception.

Identifying Installer Directory

Identifying Installer Directory

If you are an administrator and want to use CLI to manage the pods, you must know the location of the installer directory. To identify the installer directory of a pod, execute the following commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# ls -lrt | grep openstack-configs
lrwxrwxrwx. 1 root root 38 Mar 12 21:33 openstack-configs ->
/root/installer-<tagid>/openstack-configs
```

From the output, you can understand that the OpenStack-configs is a symbolic link to the installer directory. Verify if the REST API server is running from the same installer directory location, by executing the following commands:

```
# cd installer-<tagid>/tools
#./restapi.py -a status
Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h ago
REST API launch directory: /root/installer-<tagid>/
```

Managing Hosts

Managing Hosts

In Cisco VIM, a node can participate in multiple roles based on the pod type. The following rules apply for hardware management of a node:

1. If a node is a Micropod node that acts as controller, compute, and Ceph, the node can only go through the action of replace controller for its swap. You can perform this action on one node at a time.
2. If a node is a hyper-converged node (that is, acting as both compute and Ceph), the node is treated as a ceph node from hardware management point of view and the node can only go through the action of addition or removal of Ceph. This action can be done only on one node at a time.
3. If a node is a standalone compute node, the node can only go through the action of addition or removal of compute. You can add or remove multiple nodes at a time, but you cannot operate the pod with zero compute at any given time.
4. If a node is a dedicated controller node, the node can only go through the action of replace controller for its swap. This action can be done only on one node at a time.
5. If a node is a dedicated Ceph node, the node can only go through the action of addition or removal of Ceph. This action can be done only on one node at a time and you cannot have a pod with less than two node Ceph at a time.

For pod management actions, see the following table. If you log in as root, manually change the directory to */root/installer-xxx* to get to the correct working directory for these Cisco NFVI pod commands.

Action	Steps	Restrictions

Remove block_storage or compute node	1. Remove the node information from the ROLES and SERVERS section of the setup_data.yaml file for the specific node.
	2. Enter one of the following commands:
	For compute nodes:
	`ciscovim remove-computes --setupfile ~/MyDir/my_setup_data.yaml <"compute-1,compute-2"> [--force]`
	For storage nodes:
	`ciscovim remove-storage --setupfile ~/MyDir/my_setup_data.yaml <"storage-1"> [--force]`
		• You can remove multiple compute nodes, but only one storage at a time.
		• The pod must have a minimum of one compute and two storage nodes after the removal action.
		• In Cisco VIM, the number of Ceph OSD nodes vary from 3 to 20. You can remove one OSD node at a time as part of the pod management.
		⚠
		1. On a Micropod or edge pod expanded with standalone computes, only the standalone compute nodes can be removed. Pod management operation for storage node is not supported for Micro or edge pod.
		2. Compute management operations are not supported for hyper-converged nodes.
		3. In UMHC or NGENAHC pod, if a VM is running on the storage node, remove-storage operation fails in pre-validation and gives a warning to you about the running VM's. Use force option to forcefully remove the storage node.
		4. In Ceph pod, pod management operations for compute is not supported. Removal of storage node is only allowed for servers that are exclusively available with cephosd roles.

Add block_storage or compute node	1. Add the node information from the ROLES and SERVERS section of the setup_data.yaml file for the specific node.
	2. Enter one of the following commands:
	For compute nodes:
	`ciscovim add-computes --setupfile ~/MyDir/my_setup_data.yaml <"compute-1,compute-2"> [--skip_vmtp]`
	For storage nodes:
	`ciscovim add-storage --setupfile ~/MyDir/my_setup_data.yaml <"storage-1"> [--skip_vmtp]`
		• You can add multiple compute nodes and only one storage node at a time.
		• The pod must have a minimum of one compute and two storage nodes before the addition action.
		• The number of ceph OSD nodes can vary from 3 to 20. You can add one OSD node at a time as part of the pod management.
		⚠
		1. On a Micro or edge pod expanded with standalone computes, you can add only the standalone compute nodes. Pod management operation for storage node is not supported.
		2. In hyper-converged mode, compute management operations are not supported for hyper-converged nodes.

Replace		

controller node	1. If the controller node is in a rack based deployment (UCS C-Series or Quanta based pod), update the CIMC info node in the SERVERS section of the setup_data.yaml file for the specific nod. 2. For B-series, update only the blade and chassis information. 3. Enter the following commands: `ciscovim replace-controller --setupfile ~/MyDir/my_setup_data.yaml <"control-1"> [--force] [--skip_vmtp]`	• You can replace only one controller node at a time. The pod can have a maximum of three controller nodes. • The replace controller node operation is supported in Micropod. ⚠ 1. While replacing the controller node, the IP address and hostname are reused. So, do not update any other controller information other than CIMC access and hardware information for C-series, and blade and chassis information for B-series. 2. For Micro, edge and Ceph pod, this operation is supported on the AIO (all in one), compute-control, and cephcontrol nodes, respectively. In a Micro or edge pod, If a VM is running on the controller node, the replace controller operation fails during pre-validation and gives a warning to the user about running VM's. Use force option to forcefully replace the controller.

⚠ For remove-compute, remove-storage, and replace-controller operations, Cisco VIM attempts to change the host OS boot mode to single user and power-off those server(s) to avoid the creation of duplicate IP address on the management and storage networks, and to prevent the remove/replace server from connecting back to the deployment.

If the remove/replace server is powered-off before triggering Cisco VIM remove/replace operation, then the server must not be brought back on the network as it may create duplicate IP address when connected to deployment with valid credentials.

To power up those removed/replaced server(s):
- isolate the server on the network (shutdown of corresponding ToR switchports or unplug the network cables)
- power up the server
- delete the virtual drive from CIMC
- power-cycle the server
- bring the server on the network (no shutdown of corresponding ToR switchports or plug back the network cables)

When you add a compute or storage node to a rack based pod (UCS C-Series or Quanta), you can increase the management/provision address pool. Similarly, for a UCS B-series pod, you can increase the Cisco IMC pool to provide routing space flexibility for pod networking. Along with server information, these are the only items you can change in the *setup_data.yaml* file after the pod is deployed.

To make changes to the management or provisioning sections and/or CIMC (for UCS B-Series pods) network section, you must not change the existing address block as defined on Day 0. You can add only to the existing information by adding new address pool block(s) of address pool as shown in the following example:

```
NETWORKING:
::
networks:
-
vlan_id: 99
subnet: 172.31.231.0/25
gateway: 172.31.231.1
## 'pool' can be defined with single ip or a range of ip pool:
- 172.31.231.2, 172.31.231.5 - IP address pool on Day-0
- 172.31.231.7 to 172.31.231.12 - IP address pool ext. on Day-n
- 172.31.231.20
segments:
## CIMC IP allocation. Needs to be an external routable network
- cimc
-
vlan_id: 2001
subnet: 192.168.11.0/25
gateway: 192.168.11.1
rt_prefix: < Local to POD > #optional, only for segment management/provision, storage,
tenant and ToR-type NCS-5500
rt_suffix: < Region>:< pod_region_number > #optional, only for segement
management/provision, storage, tenant and ToR-type NCS-5500
## 'pool' can be defined with single ip or a range of ip
pool:
- 192.168.11.2 to 192.168.11.5 - IP address pool on Day-0
- 192.168.11.7 to 192.168.11.12  IP address pool on day-n
- 192.168.11.20  IP address pool on day-n
segments:
## management and provision goes together
- management
- provision
```

The IP address pool is the only change allowed in the networking space of the specified networks management/provision and/or CIMC (for B-series). The overall network must have enough address space to accommodate for future enhancement on day-0. After making the changes to servers, roles, and the corresponding address pool, you can execute the add compute/storage CLI shown above to add new nodes to the pod.

For C-series M5 pods, with Cisco NCS 5500 as ToR with splitter cable connection onto the server, you have to adjust the entry for the splitter_opt_4_10 in respective SWITCHDETAILS for the Cisco NCS 5500 ToR pairs with the server (cimc_ip), and connection (tor_info, dp_tor_info, sriov_tor_info) details.

For example, to add compute or storage with Cisco NCS 5500 as ToR with splitter cable, add the following entry to the respective Cisco NCS 5500:

```
TORSWITCHINFO:
  CONFIGURE_TORS: true # Mandatory
  TOR_TYPE: NCS-5500 # Mandatory
  ESI_PREFIX:91.<Pod_number>.<podregion_number>.00.00.00.00 #optional - only for NCS-5500
  SWITCHDETAILS:
  -
    hostname: <NCS-5500-1> # hostname of NCS-5500-1
    username: admin
    password: <ssh_password of NCS-5500-1>
    ...
    splitter_opt_4_10: 'FortyGigE<C/D/X/Y>,HundredGigE<E/F/A/B>, ...' # Optional for NCS-5500, only when
splitter is needed on per switch basis (i.e. the peer switch may or may not have the entry)
```

To remove a compute or a storage, delete the respective information. To replace the controller, swap the relevant port information from which the splitter cables originate.

For replace controller, you can change only a subset of the server information. For C-series, you can change the server information such as CIMC IP, CIMC Username, CIMC password, rack_id, and tor_info. For B-series, you can change the rack_id, chassis_id, and blade_id, but not the server hostname and management IP during the operation of replace controller.

Pod Recovery

Pod Recovery

This section describes the recovery processes for Cisco NFVI control node and the pod that is installed through Cisco VIM. For recovery to succeed, a full Cisco VIM installation must be done in the past. The recovery is caused by a failure of one or more controller services such as Rabbit MQ, MariaDB, and other services. The management node must be up and running, and all the nodes must be accessible through SSH without passwords from the management node. You can also use this procedure to recover from a planned shutdown or accidental power outage.

For control node recovery, use the following command:

```
ciscovim cluster-recovery
```

The control node recovers after the network partition is resolved.

> ⚠ The database sync between controller nodes might take time, which can result in cluster recovery failure. In that case, wait for sometime for the database sync to complete and then rerun the cluster-recovery.

To make sure that Nova services are good across compute nodes, execute the following command:

```
# source /root/openstack-configs/openrc
# nova service-list
```

To check the overall cloud status, execute the following command:

```
# ciscovim cloud-sanity create test all
```

To view the results of cloud-sanity, use the following command:

```
#ciscovim cloud-sanity show result all -id <uid of the test >
```

In case of a complete pod outage, you must follow a sequence of steps to bring the pod back. The first step is to bring up the management node, and check if the management node containers are up and running using the *docker ps –a* command. After you bring up the management node, bring up all the other pod nodes. Ensure that each node is reachable through *password-less SSH* from the management node. Verify that no network IP changes have occurred. You can get the node SSH IP access information from */root/openstack-config/mercury_servers_info*.

Execute the following command sequence:

1. Check the *setup_data.yaml* file and runtime consistency on the management node:

   ```
   # cd /root/installer-<tagid>/tools
   # ciscovim run --perform 1,3 -y
   ```

2. Execute the cloud-sanity using *ciscovim* command:

   ```
   #ciscovim cloud-sanity create test all
   ```

3. To view the results of cloud-sanity, use the command:

   ```
   #ciscovim cloud-sanity show result all -id
   <uid of the test >
   ```

4. Check the status of the REST API server and the corresponding directory where it is running:

   ```
   # cd/root/installer-<tagid>/tools
   #./restapi.py -a status
   Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h
   ago
   REST API launch directory: /root/installer-<tagid>/
   ```

5. If the REST API server is not running from the right installer directory, execute the following to get it running from the correct directory:

```
cd/root/installer-<tagid>/tools
#./restapi.py -a setup
Check if the REST API server is running from the correct target directory
#./restapi.py -a status
Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h ago
REST API launch directory: /root/new-installer-<tagid>/
```

6. Verify Nova services are good across the compute nodes by executing the following command:

```
# source /root/openstack-configs/openrc
# nova service-list
```

7. If cloud-sanity fails, execute cluster-recovery (ciscovim cluster-recovery), and then re-execute the cloud-sanity and nova service-list steps as listed above. Recovery of compute and OSD nodes requires network connectivity and reboot, so that they can be accessed using SSH without password from the management node.

8. To shut down, bring down the pod in the following sequence:

    a. Shut down all VMs, then all the compute nodes. It should be noted that graceful shut down of VMs is important. Check the VM status from the output of *openstack server list --all-projects*, which must show that all VMs are in SHUTOFF state before you proceed.
    b. Shut down all compute node (s).
    c. Shut down all storage nodes serially. Before proceeding to next step, ensure that you wait until the storage node shutdown is completed.
    d. Shut down all controllers, but one at a time. Before proceeding to next step, wait for the controller node shutdown to complete.
    e. Shut down the management node.
    f. Shut down the networking gears.

    ⚠ To shut down a node, SSH to the node or connect to CIMC KVM console and issue the shutdown command *#shutdown -h now*

9. Bring the nodes up in reverse order, that is,

    a. Bring up the networking gears.
    b. Bring up or power ON the management node via CIMC/BMC/ILO as part of the vendor type.
    c. Bring up or power ON the control nodes via CIMC/BMC/ILO as part of the vendor type.
    d. Bring up or power ON the storage nodes and control nodes via CIMC/BMC/ILO as part of the vendor type.
    e. Wait until the Ceph health reports are fine and then proceed to next step.
    f. Bring up or power ON the compute nodes via CIMC/BMC/ILO as part of the vendor type.

    ⚠ Ensure that each node type is completely booted up, before you move on to the next node type.

10. Run the cluster recovery command, to bring up the pod, post power-outage:

```
# ciscovim cluster-recovery
```

11. Run the cloud sanity using the command:

```
# ciscovim cloud-sanity
```

12. Execute docker cloudpulse check, to ensure that all containers are up:

```
cloudpulse run --name docker_check
```

13. Validate the Cisco API server by running the following command:

```
# ciscovim run --perform 1,3 -y
```

14. Bring up all VMs and validate if they are all up (not in shutdown state). If any of the VMs are in down state, bring them up using the Horizon dashboard.

Management Storage IP

Management Storage IP Support

From release Cisco VIM 3.2.2 onwards, along with server management IP (v4 and v6), you can also statically define the server storage IP during pod installation. To help in the transition, Cisco created a tool that helps to update the setup_data with the server storage IP information of a pod that is already up and running.
To run the utility, ensure that the pod is up and running Cisco VIM 3.2.2 or later:

```
#cd installer-xxx/tools/
#./update_static_addrs.sh
```

On success, a message *Static Address updates in setup_data.yaml complet*e is displayed at the end of the run.

NUMA Pinning

NUMA Pinning

From release Cisco VIM 3.4.0, NUMA pinning of VMs is supported. To make use of this feature, you must add *hw:pin_to_numa* in their VM's flavor, and set its value to 0 or 1. When you spawn VM with that flavor, the VM uses only the host CPUs from the NUMA that is specified in the flavor.

Managing Scheduler Filters

Managing Scheduler Filters and User Data

OpenStack Nova is an OpenStack component that provides on-demand access to compute resources by provisioning large networks of virtual machines (VMs). In addition to the standard Nova filters, Cisco VIM supports the following additional scheduler filters:

- ServerGroupAffinity Filter—Ensures that an instance is scheduled onto a host from a set of group hosts. To use this filter, you must create a server group with an affinity policy and pass a scheduler hint using group as the key and the server group UUID as the value. Use the **nova** comm and-line tool and the **--hint** flag. For example:

  ```
  $ nova server-group-create --policy affinity group-1
  $ nova boot --image IMAGE_ID --flavor 1 --hint group=SERVER_GROUP_UUID server-1
  ```

- ServerGroupAntiAffinityFilter—Ensures that each group instance is on a different host. To use this filter, you must create a server group with an anti-affinity policy and pass a scheduler hint, using group as the key and the server group UUID as the value. Use the **nova** command-line tool and the **--hint** flag. For example:

  ```
  $ nova server-group-create --policy anti-affinity group-1
  $ nova boot --image IMAGE_ID --flavor 1 --hint group=SERVER_GROUP_UUID server-1
  ```

- SameHostFilter—Within an instance set, it schedules one instance on the same host as another instance. To use this filter, pass a scheduler hint using **same_host** as the key and a list of instance UUIDs as the value. Use the **nova** command-line tool and the **--hint** flag. For example:

  ```
  $ nova boot --image IMAGE_ID --flavor 1 --hint same_host=INSTANCE_ID server-1
  ```

- DifferentHostFilter—Within an instance set, schedules one instance on a different host than another instance. To use this filter, pass a scheduler hint using **different_host** as the key and a list of instance UUIDs as the value. The filter is the opposite of SameHostFilter. Use the **nova**comman d-line tool and the **--hint** flag. For example:

  ```
  $ nova boot --image IMAGE_ID --flavor 1 --hint different_host=INSTANCE_ID server-1
  ```

In addition to scheduler filters, you can set up user data files for cloud application initialization. A user data file is a special key in the metadata service that holds a file that cloud-aware applications in the guest instance can access. For example, one application that uses user data is the cloud-init system which is an open-source package that is available on various Linux distributions to handle early cloud instance initialization. The typical use case is to pass a shell script or a configuration file as the user data during the Nova boot, for example:

```
$ nova boot --image IMAGE_ID --flavor 1 --hint user-data FILE_LOC server-1
```

Monitoring Cisco NFVI Health

Monitoring Cisco NFVI Health with CloudPulse

You can query the state of various Cisco NFVI OpenStack endpoints using an OpenStack health-checking tool called CloudPulse. By default, the tool automatically polls OpenStack Cinder, Glance, Nova, Neutron, Keystone, Rabbit, Mariadb, and Ceph every four minutes. However, you can use a CLI REST API call from the management node to get the status of these services in real time. You can integrate the CloudPulse API into your applications and get the health of the OpenStack services on demand. You can find additional information about using CloudPulse in the following OpenStack sites:

- https://wiki.openstack.org/wiki/Cloudpulse
- https://wiki.openstack.org/wiki/Cloudpulseclient
- https://wiki.openstack.org/wiki/Cloudpulse/DeveloperNotes
- https://wiki.openstack.org/wiki/Cloudpulse/OperatorTests
- https://wiki.openstack.org/wiki/Cloudpulse/APIDocs

CloudPulse supports two set of tests: endpoint based test (runs as a cron or manually) and operator test (run manually).

The endpoint based test group include:

- nova_endpoint
- neutron_endpoint
- keystone_endpoint
- glance_endpoint
- cinder_endpoint

Operator tests include:

- ceph_check: Executes the command *ceph -f json status* on the Ceph-mon nodes and parses the output. If the output is not HEALTH_OK, the ceph_check reports an error.
- docker_check: Finds out if all the Docker containers are in the running state in all the nodes. It reports an error, if any container is in the exited state. It runs the command

  ```
  docker ps -aq --filter 'status=exited'
  ```

- galera_check: Executes the command *mysql SHOW STATUS* on the controller nodes and displays the status.
- node_check: Checks if all the nodes in the system are up and online. It also compares the results of nova hypervisor list and finds out if all the computes are available.
- rabbitmq_check: Runs the command *rabbitmqctl cluster_status* on the controller nodes and finds out if the rabbitmq cluster is in quorum. If nodes are offline in the cluster rabbitmq_check, the report is considered as failed.

CloudPulse servers are installed in containers on all control nodes. The CloudPulse client is installed on the management node by the Cisco VIM installer. To execute CloudPulse, source the openrc file in the openstack-configs directory and execute the following:

```
[root@MercRegTB1 openstack-configs]# cloudpulse --help
usage: cloudpulse [--version] [--debug] [--os-cache]
[--os-region-name <region-name>]
[--os-tenant-id <auth-tenant-id>]
[--service-type <service-type>]
[--endpoint-type <endpoint-type>]
[--cloudpulse-api-version <cloudpulse-api-ver>]
[--os-cacert <ca-certificate>] [--insecure]
[--bypass-url <bypass-url>] [--os-auth-system <auth-system>]
[--os-username <username>] [--os-password <password>]
[--os-tenant-name <tenant-name>] [--os-token <token>]
[--os-auth-url <auth-url>]
<subcommand> ..
```

To check the results of periodic CloudPulse, enter the following command:

```
[root@MercRegTB1 openstack-configs]# cloudpulse result
+--------------------------------------+------+-------------------+----------+---------+
| uuid                                 | id   | name              | testtype
| state   |
+--------------------------------------+------+-------------------+----------+---------+
| 4f4c619a-1ba1-44a7-b6f8-3a06b5903260 | 7394 | ceph_check                | periodic | success |
| 68b984fa-2edb-4d66-9d9b-7c1b77d2322e | 7397 | keystone_endpoint | periodic | success |
| c53d5f0f-a710-4612-866d-caa896e2d135 | 7400 | docker_check      | periodic | success |
| 988d387c-1160-4601-b2ff-9dbb98a3cd08 | 7403 | cinder_endpoint   | periodic | success |
| 5d702219-eacc-47b7-ae35-582bb8e9b970 | 7406 | glance_endpoint   | periodic | success |
| 033ca2fc-41c9-40d6-b007-16e06dda812c | 7409 | rabbitmq_check    | periodic | success |
```

```
| 8476b21e-7111-4b1a-8343-afd634010b07 | 7412 | galera_check      | periodic | success |
| a06f8d6e-7b68-4e14-9b03-bc4408b55b48 | 7415 | neutron_endpoint  | periodic | success |
| ef56b26e-234d-4c33-aee1-ffc99de079a8 | 7418 | nova_endpoint     | periodic | success |
| f60021c7-f70a-44fb-b6bd-03804e5b7bf3 | 7421 | node_check        | periodic | success |
+--------------------------------------+------+-------------------+----------+---------+
```

By default, 25 results are displayed. Use –number argument to get desired number (up to 240) of results. For example,

```
[root@MercRegTB1 openstack-configs]# cloudpulse result -number 100
```

To view all CloudPulse tests, use the following command:

```
# cd /root/openstack-configs
# source openrc
# cloudpulse test-list
```

To run a CloudPulse test on demand:

```
# cd /root/openstack-configs
# source openrc
# cloudpulse run --name <test_name>
# cloudpulse run --all-tests
# cloudpulse run --all-endpoint-tests
# cloudpulse run --all-operator-tests
```

To run a specific CloudPulse test on demand:

```
# cloudpulse run --name neutron_endpoint
+------------+--------------------------------------+
| Property   | Value                                |
+------------+--------------------------------------+
| name       | neutron_endpoint                     |
| created_at | 2016-03-29T02:20:16.840581+00:00     |
| updated_at | None                                 |
| state      | scheduled                            |
| result     | NotYetRun                            |
| testtype   | manual                               |
| id         | 3827                                 |
| uuid       | 5cc39fa8-826c-4a91-9514-6c6de050e503 |
+------------+--------------------------------------+
```

To show detailed results of a specific CloudPulse run:

```
#cloudpulse show 5cc39fa8-826c-4a91-9514-6c6de050e503
+------------+--------------------------------------+
| Property   | Value                                |
+------------+--------------------------------------+
| name       | neutron_endpoint                     |
| created_at | 2016-03-29T02:20:16+00:00            |
| updated_at | 2016-03-29T02:20:41+00:00            |
| state      | success                              |
| result     | success                              |
| testtype   | manual                               |
| id         | 3827                                 |
| uuid       | 5cc39fa8-826c-4a91-9514-6c6de050e503 |
+------------+--------------------------------------+
```

To see the CloudPulse options, source the openrc file in openstack-configs directory and execute:

```
#cloudpulse --help
```

The CloudPulse uses a RESTful http service called the Openstack Health API to allow you to list the CloudPulse tests, create new CloudPulse tests and see the CloudPulse results.
The API calls require keystone authentication. From release Cisco VIM 3.0.0 onwards, only keystone v3 is supported.
The identity service generates authentication tokens that permit access to the CloudPulse REST APIs. Clients obtain this token and the URL endpoints for other service APIs, by supplying their valid credentials to the authentication service. Whenever you make a REST API request to CloudPulse, you must provide your authentication token in the X-Auth-Token request header.

CloudPulse is not applicable for Ceph pod.

Assessing Cisco NFVI Status

Assessing Cisco NFVI Status with Cloud-Sanity

The cloud-sanity tool is designed to give you a quick overall status of the pod health. Cloud-sanity can run tests on all node types in the pod: management, control, compute, and ceph storage.
The following are test areas supported in cloud-sanity:

1. RAID Disk health checks.
2. Basic network connectivity between the management node and all other nodes in the pod.
3. Mariadb cluster size.
4. RabbitMQ operation and status.
5. Nova service and hypervisor list.
6. CEPHMON operation and status.
7. CEPHOSD operation and status.

To run the cloud-sanity tool, login to the management node and run the ciscovim command with the cloud-sanity option.

Cloud-sanity user workflow:

1. Use "ciscovim cloud-sanity create …" command to initiate a test.
2. Use "ciscovim cloud-sanity list …" command to view summary/status of current test jobs.
3. Use "ciscovim cloud-sanity show … --id <ID>" command to view detail test results.
4. Use "ciscovim cloud-sanity delete … --id <ID>" to delete test results no longer needed.

The results are maintained so that you can view them any time.

> ⚠ Delete the results which are no longer needed.

Following are the steps to assess the pod status:

1. To run the cloud sanity, complete the following steps:

```
# ciscovim help cloud-sanity
usage: ciscovim cloud-sanity [--id <id>] [--skip-disk-checks] [-y]
create|delete|list|show test|result
all|control|compute|cephmon|cephosd|management
Run cloud-sanity test suite
Positional arguments:
create|delete|list|show The control command to perform
test|result The identity of the task/action
all|control|compute|cephmon|cephosd|management
The sanity check
Optional arguments:
--id <id> ID used to identify specific item to
show/delete.
--skip-disk-checks Flag to skip running disk-checks during
cloud-sanity test
-y, --yes Yes option to perform the action
```

2. To run the cloud sanity test, you need to create a test job. Once the test job is created, the system displays a message with the time and the ID when the test job is created.

   Run the following command to create a test job:

```
# ciscovim cloud-sanity create test all
+------------+--------------------------------------+
| Field          | Value                                                    |
+------------+--------------------------------------+
| command          | create                                |
| created_at | 2018-03-07T15:37:41.727739           |
| id                 | c000ca20-34f0-4579-a997-975535d51dda |
| result         |                                                                                  |
| status         | not_run                                                          |
| test_name  | all                                                                |
| updated_at | None                                                             |
+------------+--------------------------------------+
The user can create different test suites based on target roles. All, management, control, compute,
cephmon and cephosd. Only one test will be run at any time.
```

```
Example test create commands:
• ciscovim cloud-sanity create test control
o Runs control node tests only
• ciscovim cloud-sanity create test compute
o Runs compute nodes tests only
• ciscovim cloud-sanity create test management
o Runs management node tests only
• ciscovim cloud-sanity create test cephmon
o Runs cephmon tests only
• ciscovim cloud-sanity create test cephosd
o Runs cephosd tests only
```

The cloud-sanity tests use the disk-maintenance and osd-maintenance tools, to assess overall health and status of the RAID disks and OSD status.

> ⚠ Failures detected in RAID disk health and CEPHOSD operational status can be evaluated with the disk-maintenance and osd-maintenance tools.

3. Use the ciscovim cloud-sanity list command to monitor a currently running test or just view all the tests that have been run/completed in the past:

```
# ciscovim cloud-sanity list test all
+--------------------------------------+--------------+----------+---------------------+
| ID                                                              | Sanity Check | Status   |
Created                          |
+--------------------------------------+--------------+----------+---------------------+
| c000ca20-34f0-4579-a997-975535d51dda | all                  | Complete | 2018-03-07 15:37:41 |
| 83405cf0-e75a-4ce2-a438-0790cf0a196a | cephmon      | Complete | 2018-03-07 15:52:27 |
| 6beceb00-4029-423b-87d6-5aaf0ce087ff | cephmon          | Complete | 2018-03-07 15:55:01 |
| 2707a2e1-d1b5-4176-8715-8664a86bbf7d | cephosd          | Complete | 2018-03-07 16:11:07 |
| b30e1f49-a9aa-4f90-978a-88ba1f0b5629 | control      | Complete | 2018-03-07 16:14:29 |
| f024ff94-ac3e-4745-ba57-626b58ca766b | compute      | Running  | 2018-03-07 16:16:44 |
+--------------------------------------+--------------+----------+---------------------+
We can filter on cephmon if needed
# ciscovim cloud-sanity list test cephmon
+--------------------------------------+--------------+----------+---------------------+
| ID                                                              | Sanity Check | Status   |
Created            |
+--------------------------------------+--------------+----------+---------------------+
| 83405cf0-e75a-4ce2-a438-0790cf0a196a | cephmon          | Complete | 2018-03-07 15:52:27 |
| 6beceb00-4029-423b-87d6-5aaf0ce087ff | cephmon      | Complete | 2018-03-07 15:55:01 |
+--------------------------------------+--------------+----------+---------------------+
Example cloud-sanity list commands:
• ciscovim cloud-sanity list control
• ciscovim cloud-sanity list compute
• ciscovim cloud-sanity list management
• ciscovim cloud-sanity list cephmon
• ciscovim cloud-sanity list cephosd
```

4. Use the following commands to view the test-sanity results. Cloud-sanity test results can be passed, failed, or skipped. A skipped test is one that is not supported on this particular POD (for example, RAID test is only supported with Hardware RAID.) A skipped test does not count to the overall pass/fail status.

```
# ciscovim cloud-sanity show test all --id c000ca20-34f0-4579-a997-975535d51dda
Cloud sanity Results
+------------+-----------------------------------------------------------------+---------+
| Role               |
Task
| Result  |
+------------+-----------------------------------------------------------------+---------+
| Management | Management - Disk Maintenance RAID Health ***************** | PASSED  |
|                         |                                                                 |         |
| Management | Management - Container Version Check ********************* | PASSED  |
|                         |                                                                 |         |
| Management | Management - Disk Maintenance VD Health ****************** | PASSED  |
|            |                                                                 |         |
| Control    | Control - Check RabbitMQ is Running ********************** | PASSED  |
|                         |                                                                 |         |
| Control    | Control - Check RabbitMQ Cluster Status ****************** | PASSED  |
```

```
| Control    | Control - Container Version Check ********************** | PASSED  |
| Control    | Control - Check MariaDB Cluster Size ******************** | PASSED  |
| Control    | Control - Ping All Controller Nodes ********************* | PASSED  |
| Control    | Control - Check Nova Service List *********************** | PASSED  |
| Control    | Control - Ping Internal VIP ***************************** | PASSED  |
| Control    | Control - Disk Maintenance RAID Health ****************** | PASSED  |
| Control    | Control - Disk Maintenance VD Health ******************** | PASSED  |
| Compute    | Compute - Check Nova Hypervisor List ******************** | PASSED  |
| Compute    | Compute - Disk Maintenance RAID Health ****************** | PASSED  |
| Compute    | Compute - Ping All Compute Nodes ************************ | PASSED  |
| Compute    | Compute - Container Version Check *********************** | PASSED  |
| Compute    | Compute - Disk Maintenance VD Health ******************** | PASSED  |
| CephOSD    | CephOSD - Ping All Storage Nodes ************************ | PASSED  |
| CephOSD    | CephOSD - Check OSD Result Without OSDinfo *************** | PASSED  |
| CephOSD    | CephOSD - OSD Overall Status **************************** | PASSED  |
| CephOSD    | CephOSD - Check OSD Result With OSDinfo ***************** | PASSED  |
| CephMon    | CephMon - Check Cephmon Status ************************** | PASSED  |
| CephMon    | CephMon - Ceph Cluster Check **************************** | PASSED  |
| CephMon    | CephMon - Check Cephmon Results ************************* | PASSED  |
| CephMon    | CephMon - Check Cephmon is Running ********************** | PASSED  |
+------------+-------------------------------------------------------------+---------+
[PASSED] Cloud Sanity All Checks Passed
```

5. To delete the cloud sanity test results, run the following command:

```
# ciscovim cloud-sanity delete test all --id c000ca20-34f0-4579-a997-975535d51dda
Perform the action. Continue (Y/N)Y
Delete of UUID c000ca20-34f0-4579-a997-975535d51dda Successful
# ciscovim cloud-sanity list test all
+--------------------------------------+--------------+----------+---------------------+
| ID                                   | Sanity Check | Status   |
Created                          |
+--------------------------------------+--------------+----------+---------------------+
| 83405cf0-e75a-4ce2-a438-0790cf0a196a | cephmon          | Complete | 2018-03-07 15:52:27 |
| 6beceb00-4029-423b-87d6-5aaf0ce087ff | cephmon           | Complete | 2018-03-07 15:55:01 |
| 2707a2e1-d1b5-4176-8715-8664a86bbf7d | cephosd      | Complete | 2018-03-07 16:11:07 |
| b30e1f49-a9aa-4f90-978a-88ba1f0b5629 | control      | Complete | 2018-03-07 16:14:29 |
| f024ff94-ac3e-4745-ba57-626b58ca766b | compute      | Complete | 2018-03-07 16:16:44 |
+--------------------------------------+--------------+----------+---------------------+
```

The cloud-sanity tests use the disk-maintenance and osd-maintenance tools to assess overall health and status of RAID disks and OSD status.

> ⚠ Failures detected in RAID disk health and CEPHOSD operational status can be evaluated with the disk-maintenance and osd-maintenance tools.

Service Catalog URL

Service Catalog URL

The OpenStack Keystone service catalog allows API clients to dynamically discover and navigate to cloud services. CloudPulse has its own service URL which is added to the Keystone service catalog. You need to send a token request to Keystone, to find the service URL of CloudPulse. The token request lists the catalog of available services.

Get Token from Keystone

To get the token from keystone, run the following commands:

Resource URI

Verb	URI
POST	http://<controller_lb_ip>:5000/v2.0/tokens

Example

```
JSON Request
POST / v2.0/tokens
Accept: application/json
{
        "auth": {
        "passwordCredentials":{
                "username": "admin",
                "password": "iVP1YciVKoMGId1O"}
                        }
}
JSON Response
200 OK
Content-Type: application/json
{
"access": {
        "token": {
        "issued_at": "2017-03-29T09:54:01.000000Z",
        "expires": "2017-03-29T10:54:01Z",
        "id":"gAAAAABY24Q5TDIqizuGmhOXakV2rIzSvSPQpMAmC7SA2UzUXZQXSH-ME98d3Fp4Fsj16G561a420B4BK0fylcykL22EcO9",
............
........}
}
```

Get Service Catalog URL for CloudPulse

Resource URI

Verb	URI
GET	http://<controller_ip>:35357/v2.0/endpoints

Example:

```
JSON Request
GET /v2.0/endpoints
Accept: application/json
JSON Response
```

```
200 OK
Content-Type: application/json
{"endpoints": [
{"internalurl": "http://<controller>:9999",
"adminurl": "http://<controller>:9999",
"publicurl":"http://<controller>:9999"
}]}
}
```

CloudPulse APIs

The following is the list of APIs and their corresponding functions. The CloudPulse API is accessed with the X-Auth-token which is received from the Keystone token generation API .

List of CloudPulse Tests

To get the list of cloudpulse tests:

Resource URI

Verb	URI
GET	http://<controller_ip>:9999/cpulse

Get Detailed Test Result

To get detailed test result:

Resource URI

Verb	URI
GET	http://<controller_ip>:9999/cpulse/<uuid>

Uuid : uuid of the test

Example

```
JSON Request
 GET /cpulse/e6d4de91-8311-4343-973b-c507d8806e94
 Accept: application/json
 JSON Response
 200 OK
 Content-Type: application/json
 {
         "name": "galera_check", "state": "success",
         "result":"ActiveNodes:16.0.0.37,16.0.0.17,16.0.0.27",
         "testtype": "periodic", "id": 4122,
         "uuid": " e6d4de91-8311-4343-973b-c507d8806e94"
 }
```

Get List of Tests Available

To get a list of available cloudpulse tests:

Resource URI

Verb	URI
GET	http://<controller_ip>:9999/cpulse/list_tests

Example

```
JSON Request
 GET /cpulse/list_tests
 Accept: application/json
 JSON Response
```

```
 200 OK
 Content-Type: application/json
 {
         "endpoint_scenario":

"all_endpoint_tests\ncinder_endpoint\nglance_endpoint\nkeystone_endpoint\nneutron_endpoint\nnova_endpoint",
        "operator_scenario":
"all_operator_tests\nceph_check\ndocker_check\ngalera_check\nnode_check\nrabbitmq_check"
 }
```

Schedule a manual CloudPulse test:

To schedule a manual test of CloudPulse, run the following commands:

Resource URI

Verb	URI
POST	http://<controller_ip>:9999/cpulse

Example

```
JSON Request POST /cpulse
 Accept: application/json
 {
 "name": "galera_check"
 }
 JSON Response
 200 OK
 Content-Type: application/json
 {
 "name": "galera_check",
 "state": "scheduled",
 "result":"NotYetRun",
 "testtype": "manual",
 "id": 4122,
 "uuid": " e6d4de91-8311-4343-973b-c507d8806e94"
 }
```

Remove Test Results

To remove the test results:

Resource URI

Verb	URI
DELETE	http://<controller_ip>:9999/cpulse/<uuid>

Uuid : uuid of the test

Example

```
JSON Request
 DELETE /cpulse/68ffaae3-9274-46fd-b52f-ba2d039c8654
 Accept: application/json
 JSON Response
 204 No Content
```

Checking Network Connections

Checking Network Connections

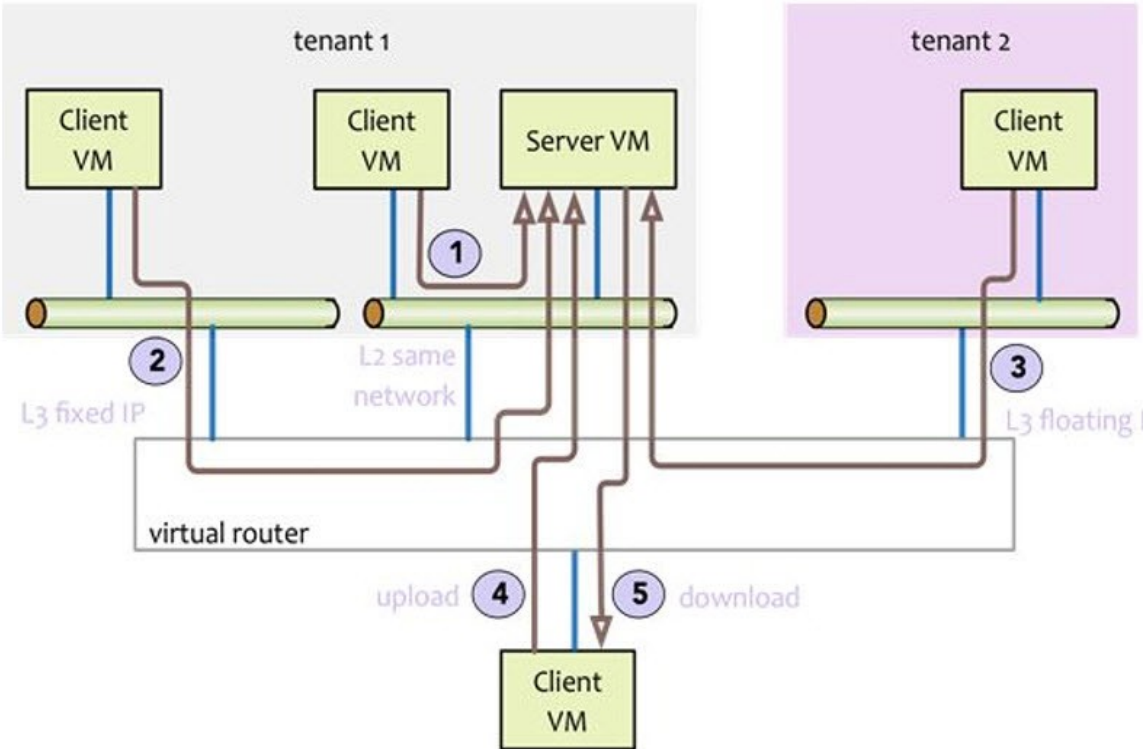
You can use Virtual Machine Through Put (VMTP) to check Layer-2 and Layer-3 data plane traffic between Cisco NFVI compute nodes. VMTP performs ping connectivity, round trip time measurement (latency), and TCP/UDP throughput measurement for the following Cisco NFVI east to west VM-to-VM flows:

- Same network (private fixed IP, flow number 1).
- Different network using fixed IP (same as intra-tenant L3 fixed IP, flow number 2).
- Different network using floating IP and NAT (same as floating IP inter-tenant L3, flow number 3).
- When an external Linux host is available for testing north to south flows, external host to VM download and upload throughput and latency (L3 /floating IP, flow numbers 4 and 5).

The following figure shows the traffic flows VMTP measures. Cloud traffic flows are checked during Cisco VIM installation and can be checked at any later time by entering the following command:

```
$ ciscovim run --perform 8 -y
```

The following figure depicts the VMTP cloud traffic monitoring.



General Scheme of Enabling Optional Services

General Scheme of Enabling Optional Services Post Cisco VIM Deployment

Before running the reconfigure option, it is recommended to run the cloud sanity to ensure that the NFVI is up and running and no faults exists. After the successful execution of cloud sanity, take a backup of the setup_data file and update it manually with the configuration details by running the following command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml/root/MyDir/ # update the setup_data to for the
targeted change
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Managing VIM Administrators

Managing VIM Administrators

Additional VIM Administrators

The VIM administrator can login to the management through SSH or the console using the configured password. Administrators have their own accounts. After the VIM administrator account creation, the administrator can manage their own password using the Linux *passwd* command. You can change the *vim_admins* parameter to add and remove VIM administrators during reconfiguration, while the passwords for existing accounts remain unchanged.

1. Before launching the installation, take a backup of the setup_data.yaml file and update the file manually with the configurations listed below:

```
vim_admins:
- vim_admin_username: <username>
  vim_admin_password_hash: <sha512-password-hash>

- vim_admin_username: <username>
  vim_admin_password_hash: <sha512-password-hash>

- vim_admin_username: <username>
  vim_admin_password_hash: <sha512-password-hash>
  The value of password hash must be in the standard sha512 format.

# To generate the hash admin_password_hash should be the output from on the management node

# python -c "import crypt; print crypt.crypt('<plaintext password>')"
```

2. Run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
# update the setup_data to include vim_admin info
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Enabling VIM Administrator with LDAP Authentication

Cisco VIM supports management of the VIM administrators whose access to the management node can be authenticated through an external LDAP server. It can be added as a Day 0 or Day 1 activity. Multiple LDAP entries are allowed, as only the domain_name and ldap_uri in each entry are mandatory. Ensure that the ldap_uris is secured over LDAPs, and the TLS is enabled for the external api (external_lb_vip_tls: True).

To obtain sudo access to the management node and execute ciscovim commands, you must manually add the user with root privileges to the wheel group in the corresponding LDAP domain, for example, usermode -aG wheel user1. Also, you must enable the pod with external TLS. For LDAP certificate management, copy over the CA root certificate file of the LDAP server onto the management node and append it to the */root/openstack-configs/haproxy-ca.crt* chain.

To enable VIM administrators with LDAP authentication, perform the following steps:

1. Take a backup of the *setup_data* file and update the file manually with the configuration listed below during installation:

```
vim_ldap_admins:
- domain_name: corp_ldap1
  ldap_uri: "ldaps://<ip_address_1:[port_1]>,ldaps://<ip_address_2:[port_2]>"
  ldap_search_base: "dc=cisco,dc=com"
  ldap_schema: rfc2307 # Optional
  ldap_user_object_class: posixAccount # Optional
  ldap_user_uid_number: uidNumber # Optional
  ldap_user_gid_number: gidNumber # Optional
```

```
  ldap_group_member: memberUid # Optional

- domain_name: corp_ldap2
  ldap_uri: "ldaps:///<ip_address_3:[port_3]"
  ldap_search_base: "dc=cisco,dc=com"
  ldap_schema: rfc2307                  # Optional, supported possible values 'rfc2307'
  ldap_user_object_class: posixAccount  # Optional
  ldap_user_uid_number: uidNumber       # Optional
  ldap_user_gid_number: uidNumber       # Optional
  ldap_group_member: memberUid          # Optional
  ldap_default_bind_dn: "<string>"      # Optional
  ldap_default_authtok: "<string>"      # Optional
  ldap_default_authtok_type: "<string>" # Optional (password|obfuscated_password)
  ldap_group_search_base: "<string>"    # Optional
  ldap_user_search_base: "<string>"     # Optional
  access_provider: "<string>"           # Optional
  simple_allow_groups: "<string>"       # Optional
  ldap_id_use_start_tls: <boolean>      # Optional
  ldap_tls_reqcert: "<string>"          # Optional (never|allow|try|demand)
  chpass_provider: "<string>"           # Optional (ldap|none)
```


- ldap_default_authtok is mandatory, if the LDAP server does not support anonymous bindings.
- Multiple entries of the LDAP domain are allowed. For each entry, only *domain_name* and *ldap_uri* info are mandatory. Ensure that the ldap_uri is secured over ldaps. As part of reconfiguration, you can add new domain_name, but cannot change the domain_name once it is configured.

2. To reconfigure the VIM administrator, run the following commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
# update/include the vim_ldap_admin in the setup_data
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Enabling Root Login Post Cisco VIM Installation

Cisco VIM supports an option to enable/disable root access at login. By default, this option is set to True. You can optionally disable this facility through reconfiguration.

Following are the steps to enable the root login:

1. Take a backup of the *setup_data* file and update the file manually with the configuration listed below:

```
permit_root_login: <True or False> # if set to false, one has to use su to drop down to root and execute
administrator functionalities.
```

2. Run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/ [root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
# update the setup_data to include vim_admin info
[root@mgmt1 ~]# cd /root/MyDir
[root@mgmt1 ~]# vi setup_data.yaml [root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim --setupfile /root/MyDir/setup_data.yaml reconfigure
```

Disabling Root Login

Cisco VIM offers the option of disabling root login.

Listed below are the available options:

```
# Permit Root Login (optional, default True)

# True: admin can ssh to management node with root userid and password

# False: admin cannot use root userid for ssh;  must use vim_admin_username # At least one vim_admin must be
configured if it is False
  permit_root_login: True
```

Read-only OpenStack Role

Read-only OpenStack Role

By default, Cisco VIM deployment of OpenStack supports two user roles: admin and user. Admin can view and change all OpenStack resources including system and project resources. Users can view and change only project resources.
Optionally, Cisco VIM provides OpenStack user role which is read-only administrator or readonly. Use the optional parameter ENABLE_READONLY_ROLE to enable this feature.

The OpenStack read-only user can:

- Access the project and identity dashboards, but not the admin dashboard.
- View all the project resources, but cannot make any changes to them.

The admin can only assign the readonly role using the Horizon dashboard or OpenStack CLI, to the target user for accessing each project. A user can be given the readonly role to multiple projects.

> ⚠ Ensure that the admin role is not given for the user having only readonly access, as the conflict of access will not constrain the user to read-only operations.

Enabling this feature provides the following enhancements to the Cisco VIM pod.

- *readonly* role is added to the OpenStack deployment.
- OpenStack service policies are adjusted to grant read permissions such as *list* and *show*, but not *create, update*, or *delete.*
- **AllProjects** tab is added to the Horizon interface. This allows the readonly user to see all instances for which the user have access. Under the **Project** tab, you can see the resources for a single project. You can change the projects using the Project pulldown in the header.

To enable read-only OpenStack role and create read-only OpenStack administrator, perform the following steps:

1. Before launching the installation, take a backup of the setupdata file and update the setup_data.yaml file with the following information:

```
ENABLE_READONLY_ROLE: True
```

2. If the OpenStack user role is not enabled on the Day 0, you can enable it by executing the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
# update the setup_data to include ENABLE_READONLY_ROLE: True
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

3. When the feature is enabled, an OpenStack administrator can create new user accounts that will have the special privileges of a Read-Only user. From the management node, load the OpenStack authentication variables:

```
[root@management-server-cisco ~]# source ~/openstack-configs/openrc
```

4. Create a new user account with a strong password:

```
[root@management-server-cisco images]# openstack user create --password-prompt reader
User Password:
Repeat User Password:
+----------+----------------------------------+
| Field    | Value                            |
+----------+----------------------------------+
| email    | None                             |
| enabled  | True                             |
| id       | e2f484de1e7d4faa9c9de2446ba8c3de |
| name     | reader                           |
| username | reader                           |
+----------+----------------------------------+
```

5. Assign the project and role to that user account:

```
[root@management-server-cisco images]# openstack role add --project admin --user reader
readonly
+-----------+----------------------------------+
| Field     | Value                            |
+-----------+----------------------------------+
| domain_id | None                             |
| id            | ed2fb5b2c88e4241918573624090174b |
| name              | readonly                                  |
+-----------+----------------------------------+
```

Alternatively, the OpenStack admin logged into the Horizon dashboard can perform the above steps. You can perform the actions corresponding to the CLI commands on the Identity/Users panel in the dashboard.

After deployment, the administrators can create new users assigned with this role.

If the ENABLE_READONLY_ROLE is False (by default), the readonly role will not have special permissions or restrictions, but have the create, update, and delete permissions to project resources similar to that of project member. You need to assign the users with readonly role, when ENABLE_READONLY_ROLE is set to True.

Managing Power and Reboot

Managing Power and Reboot

Power Management of C-series Computes

The power management function of computes optimize the overall power consumption of the data center. Powering down the server through an API/CLI helps you to have a power backup. This procedure is applicable to standalone computes only and no VM must be running on that node before power down is initiated.

1. To power off one or more compute nodes, run the following commands:

```
Run ciscovim power-off help command
# ciscovim help power-off
usage: ciscovim power-off --setupfile SETUPFILE [-y] <node1,node2,...>
Power Off compute-nodes
Positional arguments:
<node1,node2,...> Power off Compute Nodes
Optional arguments:
--setupfile SETUPFILE <setupdata_file>. Mandatory for any POD management
operation.
-y, --yes Yes option to perform the action
```

2. To list all the nodes in the Openstack Cloud, run the following command:

```
# ciscovim list-nodes
```

3. Choose one or more active compute node to be powered off.
4. Run the following command:

```
# ciscovim power-off <compute-server-1, compute-server-2, .... > --setupfile <path_setup_data.yaml>
```

5. Run the following command to verify that the computes are power off:

```
#ciscovim list-nodes
```

- The status of the compute nodes that are powered off must be *InActive*.
- To prevent cloud destabilization, you must ensure that at least one compute node is in *Active* state.
- You cannot perform the pod management operations such as update, reconfigure, and so on, to the entire pod, if one or more compute nodes are powered off.
- You cannot turn OFF the power of computes which run VMs or which provide other roles such as All-in-one (AIO) nodes in a Micropod, using this API. Power error-handling methods are added to handle such cases.
- As part of the power-off action, cloud-sanity is run internally. If the cloud sanity fails, the power-off action is aborted.

Power-on Compute Nodes

Following are the steps to power on the compute nodes:

1. Run the following command to power-on one or more compute nodes:

```
Run ciscovim power-on help command
# ciscovim help power-on
```

```
usage: ciscovim power-on --setupfile SETUPFILE [-y] <node1,node2,...>
Power On compute-nodes
Positional arguments:
<node1,node2,...> Power on Compute Nodes
Optional arguments:
--setupfile SETUPFILE <setupdata_file>. Mandatory for any POD management
operation.
-y, --yes Yes option to perform the action
```

2. To list all the nodes in the OpenStack cloud, enter the following command:

```
# ciscovim list-nodes
```

3. Choose one or more active compute nodes to be powered on.
4. Run the following command:

```
# ciscovim power-on <compute-server-1, compute-server-2, .... > --setupfile <path_setup_data.yaml>
```

5. Run the following command to verify if the compute(s) are powered on:

```
# ciscovim list-nodes
```


The status of the compute nodes that are powered ON must be *Active*.

Managing Reboot of Cisco VIM Compute Nodes

Use *ciscovim* CLI to reboot the Cisco VIM nodes. During software update, core libraries like *kernel, glibc, systemd* and so on require rebooting of the system to run the latest version. Cisco VIM has the functionality to reboot nodes (if needed) during an update, but Cisco defers the update of compute nodes which are running application VMs.

Reboot the nodes using the CLI before migrating the VM's on another computes as shown in the following steps:

1. Run the following command to Reboot one or more compute nodes:

```
Run ciscovim reboot help command
# ciscovim help reboot
usage: ciscovim reboot [-y] <node1,node2,...>
Reboot compute-nodes
Positional arguments:
<node1,node2,...> Reboot Compute Nodes
Optional arguments:
-y, --yes Yes option to perform the action
```

2. Run the following command to select one or more compute nodes:

```
# ciscovim reboot <compute-server-1, compute-server-2, .... >
```


- You cannot reboot all the compute nodes simultaneously. Ensure that at least one node is Active to prevent the cloud destabilization.
- You cannot reboot the computes on which VMs are running. The nodes which are associated with multiple roles, for example, All-in-one (AIO) nodes in a Micropod or Hyper-converged can be rebooted one at a time.

Cisco VIM Client Reboot and Remove Compute Using Force Option

When VMs are running on a particular compute node, you cannot reboot or remove that compute node. Cisco VIM installer internally checks for the presence of VMs and aborts the operation, if VM is running on the target compute node.
To execute remove-compute operation without any failure, migrate or terminate the VMs running on compute nodes and then execute remove or reboot operations using the below option in Cisco VIM client:

```
-f/--force
```


Before executing reboot or remove compute operations with force option:

- If a remove compute operation is executed with a *force* option, the VMs running on that compute node are deleted.
- If a reboot compute operation is executed with a *force* option, the VMs are restored to last running status post successful reboot of that compute node.

Example of Remove Compute

```
# ciscovim help remove-computes
usage: ciscovim remove-computes --setupfile SETUPFILE [-y] [-f] <node1,node2,...>
Remove compute-nodes from the Openstack cloud
Positional arguments:
<node1,node2,...> Remove compute nodes
Optional arguments:
--setupfile SETUPFILE <setupdata_file>. Mandatory for any POD management
operation.
-y, --yes Yes option to perform the action
-f, --force Force option to remove or reboot
# ciscovim remove-computes --setupfile /tmp/remove_computes_setup_data.yaml gg34-4 -y --force
monitoring remove_compute (gg34-4) operation
.........................
Cisco VIM Runner logs
.........................
```

Example of removing multiple computes

```
# ciscovim remove-computes --setupfile /tmp/remove_computes_setup_data.yaml gg34-1, gg34-2
-y -force
```


For remove-compute operation, Cisco VIM attempts to change the host OS boot mode to single user and power-off those compute node(s) to avoid the creation of duplicate IP address on the management and storage networks, and to prevent the compute node(s) from connecting back to the deployment.

If the compute node(s) to be removed are powered-off before triggering Cisco VIM remove-compute operation, then the server must not be brought back on the network as it may create duplicate IP address when connected to deployment with valid credentials.

To power up the removed compute node(s):
- network isolate the compute node(s) (shutdown of corresponding ToR switchports or unplug the network cables)
- power up the server from CIMC
- delete the virtual drive from CIMC
- power-cycle the server from CIMC
- bring the compute node on the network (no shutdown of corresponding ToR switchports or plug back the network cables)

If ToR_TYPE is Cisco NCS 5500, you must manually remove all the sub-interfaces that are manually configured on the NCS switch, as the Cisco VIM automation does not unconfigure/configure the sub-interfaces for which the VLANs are not defined in the setup_data.yaml. If sub-interfaces are not removed, it results in remove-compute operation.

Example of reboot compute

```
# ciscovim help reboot
usage: ciscovim reboot [-y] [-f] <node1,node2,...>
Reboot compute-nodes
Positional arguments:
<node1,node2,...> Reboot Compute Nodes
Optional arguments:
-y, --yes Yes option to perform the action
-f, --force Force option to perform the action
# ciscovim reboot gg34-4 -y --force
monitoring reboot (gg34-4) operation
.........................
Cisco VIM Runner logs
.........................
```

Example of rebooting multiple computes

```
# ciscovim reboot compute-server-hostname1,compute-server-hostname2 -y --force
```

Managing Reboot Status of Cisco VIM Nodes

You can find which Cisco VIM nodes require a reboot after an update, using the CLI. Reboot the nodes after an update, so that the cloud is running the latest host packages.

> ⚠ It is mandatory for the operator to reboot nodes to be able to perform next update or pod management operation.

Run the following command to check the reboot pending status for nodes in the pod, post update.

```
Run ciscovim reboot-status help command
# ciscovim help reboot-status
usage: ciscovim reboot-status
List of Openstack Nodes that require a reboot
Sample command execution:
# ciscovim reboot-status
Fetching Nodes that require a Reboot
+--------------------------+-----------------+
| Node Name                | Reboot Required |
+--------------------------+-----------------+
| compute-server-hostname1 | No              |
| compute-server-hostname2 | No              |
| compute-server-hostname3 | No              |
+--------------------------+-----------------+
```

Managing Reboot of Cisco VIM Management Node and Standalone Control and Ceph Nodes

You must reboot the nodes that constitute the control plane of Cisco VIM with utmost care, only during a maintenance window. Execute the *ciscovim cluster recovery,* if any of the controllers are rebooted. Check the ceph status post reboot of the Ceph nodes and wait until Ceph reaches HEALTH_OK state.

To reboot the nodes one at a time, execute the following command:

```
# shutdown -r now
```

> ⚠ Any power down of nodes must be done gracefully and not via CIMC/BMC/ILO to avoid potential disk corruption.

Security

Security

The following topics describe Cisco NFVI network and application security and best practices.

Verification

Verification

Verifying Management Node Network Permissions

The Cisco NFVI management node stores sensitive information related to Cisco NFVI operations. Access to the management node can be restricted to requests coming from IP addresses known to be used by administrators. The administrator source networks is configured in the setup file, under **[NETWORKING]** using the **admin_source_networks** parameter.

To verify this host based firewall setting, log into the management node as an admin user and list the rules currently enforces by iptables. Verify that the source networks match the values configured. If no source networks have been configured, then all source traffic is allowed. However, note that only traffic destined to ports with known admin services is allowed to pass. The **admin_source_networks** value can be set at install time or changed through reconfiguration.

```
[root@control-server-1 ~]# iptables -list
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT icmp -- anywhere anywhere
ACCEPT tcp -- 10.0.0.0/8 anywhere tcp dpt:ssh
ACCEPT tcp -- 172.16.0.0/12 anywhere tcp dpt:ssh
ACCEPT tcp -- 10.0.0.0/8 anywhere tcp dpt:https
ACCEPT tcp -- 172.16.0.0/12 anywhere tcp dpt:https
ACCEPT tcp -- 10.0.0.0/8 anywhere tcp dpt:4979
ACCEPT tcp -- 172.16.0.0/12 anywhere tcp dpt:4979
ACCEPT tcp -- 10.0.0.0/8 anywhere tcp dpt:esmagent
ACCEPT tcp -- 172.16.0.0/12 anywhere tcp dpt:esmagent
ACCEPT tcp -- 10.0.0.0/8 anywhere tcp dpt:8008
ACCEPT tcp -- 172.16.0.0/12 anywhere tcp dpt:8008
ACCEPT tcp -- 10.0.0.0/8 anywhere tcp dpt:copy
ACCEPT tcp -- 172.16.0.0/12 anywhere tcp dpt:copy
ACCEPT tcp -- 10.0.0.0/8 anywhere tcp dpt:22250
ACCEPT tcp -- 172.16.0.0/12 anywhere tcp dpt:22250
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
DROP   all -- anywhere anywhere
```

Verifying Management Node File Permissions

The Cisco NFVI management node stores sensitive information related to Cisco NFVI operations. These files are secured by strict file permissions. Sensitive files include secrets.yaml, openrc, *.key, and *.pem. To verify the file permissions, log into the management node as an admin user and list all of the files in the *~/openstack-configs/* directory. Verify that only the owner has read and write access to these files. For example:

```
[root@control-server-1 ~]# ls -l ~/openstack-configs
total 172
-rw-------. 1 root root 3272 Jun 21 17:57 haproxy.key
-rw-------. 1 root root 5167 Jun 21 17:57 haproxy.pem
-rw-------. 1 root root 223 Aug 8 18:09 openrc
-rw-------. 1 root root 942 Jul 6 19:44 secrets.yaml
[...]
```

Viewing Administrator Access Attempts

As the UCS servers are part of the critical Cisco NFVI infrastructure, Cisco recommends monitoring administrator login access periodically.

To view the access attempts, use the *journalctl* command to view the log created by ssh. For example:

```
[root@control-server-1 ~]# journalctl -u sshd
-- Logs begin at Tue 2016-06-21 17:39:35 UTC, end at Mon 2016-08-08 17:25:06 UTC. --
Jun 21 17:40:03 hh23-12 systemd[1]: Started OpenSSH server daemon.
Jun 21 17:40:03 hh23-12 systemd[1]: Starting OpenSSH server daemon...
Jun 21 17:40:03 hh23-12 sshd[2393]: Server listening on 0.0.0.0 port 22.
Jun 21 17:40:03 hh23-12 sshd[2393]: Server listening on :: port 22.
Jun 21 17:40:43 hh23-12 sshd[12657]: Connection closed by 171.70.163.201 [preauth]
Jun 21 17:41:13 hh23-12 sshd[12659]: Accepted password for root from 171.70.163.201 port 40499
Jun 21 17:46:41 hh23-12 systemd[1]: Stopping OpenSSH server daemon...
Jun 21 17:46:41 hh23-12 sshd[2393]: Received signal 15; terminating.
Jun 21 17:46:41 hh23-12 systemd[1]: Started OpenSSH server daemon.
Jun 21 17:46:41 hh23-12 systemd[1]: Starting OpenSSH server daemon...
Jun 21 17:46:41 hh23-12 sshd[13930]: Server listening on 0.0.0.0 port 22.
Jun 21 17:46:41 hh23-12 sshd[13930]: Server listening on :: port 22.
Jun 21 17:50:45 hh23-12 sshd[33964]: Accepted password for root from 171.70.163.201 port 40545
Jun 21 17:56:36 hh23-12 sshd[34028]: Connection closed by 192.168.212.20 [preauth]
Jun 21 17:57:08 hh23-12 sshd[34030]: Accepted publickey for root from 10.117.212.20 port 62819
Jun 22 16:42:40 hh23-12 sshd[8485]: Invalid user user1 from 10.117.212.20
Jun 22 16:42:40 hh23-12 sshd[8485]: input_userauth_request: invalid user user1 [preauth]
```

Verifying SELinux

To minimize the impact of a security breach on a Cisco NFVI server, the Cisco VM enables SELinux (Security Enhanced Linux) to protect the server resources. To validate that SELinux is configured and running in enforcing mode, use the sestatus command to view the status of SELinux and verify that its status is enabled and in enforcing mode. For example:

```
[root@mgmt1 ~]# /usr/sbin/sestatus -v
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: permissive
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28
```

Validating Port Listening Services

To prevent access by unauthorized users and processes, Cisco NFVI has no extra services listening on network ports. To verify this, use the netstat -plnt command to get a list of all services listening on the node and verif that no unauthorized services are listening. For example:

```
[root@-control-server-1 ~]# netstat -plnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program
name
tcp 0 0 23.23.4.101:8776 0.0.0.0:* LISTEN 24468/python2
tcp 0 0 23.23.4.101:5000 0.0.0.0:* LISTEN 19874/httpd
tcp 0 0 23.23.4.101:5672 0.0.0.0:* LISTEN 18878/beam.smp
tcp 0 0 23.23.4.101:3306 0.0.0.0:* LISTEN 18337/mysqld
tcp 0 0 127.0.0.1:11211 0.0.0.0:* LISTEN 16563/memcached
tcp 0 0 23.23.4.101:11211 0.0.0.0:* LISTEN 16563/memcached
tcp 0 0 23.23.4.101:9292 0.0.0.0:* LISTEN 21175/python2
tcp 0 0 23.23.4.101:9999 0.0.0.0:* LISTEN 28555/python
tcp 0 0 23.23.4.101:80 0.0.0.0:* LISTEN 28943/httpd
tcp 0 0 0.0.0.0:4369 0.0.0.0:* LISTEN 18897/epmd
tcp 0 0 127.0.0.1:4243 0.0.0.0:* LISTEN 14673/docker
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 2909/sshd
tcp 0 0 23.23.4.101:4567 0.0.0.0:* LISTEN 18337/mysqld
tcp 0 0 23.23.4.101:15672 0.0.0.0:* LISTEN 18878/beam.smp
tcp 0 0 0.0.0.0:35672 0.0.0.0:* LISTEN 18878/beam.smp
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 4531/master
tcp 0 0 23.23.4.101:35357 0.0.0.0:* LISTEN 19874/httpd
tcp 0 0 23.23.4.101:8000 0.0.0.0:* LISTEN 30505/python
tcp 0 0 23.23.4.101:6080 0.0.0.0:* LISTEN 27996/python2
tcp 0 0 23.23.4.101:9696 0.0.0.0:* LISTEN 22396/python2
tcp 0 0 23.23.4.101:8004 0.0.0.0:* LISTEN 30134/python
```

```
tcp 0 0 23.23.4.101:8773 0.0.0.0:* LISTEN 27194/python2
tcp 0 0 23.23.4.101:8774 0.0.0.0:* LISTEN 27194/python2
tcp 0 0 23.23.4.101:8775 0.0.0.0:* LISTEN 27194/python2
tcp 0 0 23.23.4.101:9191 0.0.0.0:* LISTEN 20752/python2
tcp6 0 0 :::9200 :::* LISTEN 18439/xinetd
tcp6 0 0 :::4369 :::* LISTEN 18897/epmd
tcp6 0 0 :::22 :::* LISTEN 2909/sshd
tcp6 0 0 ::1:25 :::* LISTEN 4531/master
```

Validating Non-Root Users for OpenStack Services

To prevent unauthorized access, Cisco NFVI runs OpenStack processes as a non-root user. To verify OpenStack processes are not running as root, use the ps command to get a list of all node processes. In the following example the user is 162:

```
[root@control-server-1 ~]# ps -aux | grep nova-api
162 27194 0.6 0.0 360924 132996 ? S Aug08 76:58 /usr/bin/python2
/usr/bin/nova-api
162 27231 0.0 0.0 332192 98988 ? S Aug08 0:01 /usr/bin/python2
/usr/bin/nova-api
162 27232 0.0 0.0 332192 98988 ? S Aug08 0:01 /usr/bin/python2
/usr/bin/nova-api
162 27233 0.0 0.0 332192 98988 ? S Aug08 0:01 /usr/bin/python2
/usr/bin/nova-api
```

Verifying Password Strength

Cisco NFVI passwords can be generated in two ways during installation:

- The Cisco NFVI installer generates unique passwords automatically for each protected service.
- You can provide an input file containing the passwords you prefer.

Cisco-generated passwords are unique, long, and contain a mixture of uppercase, lowercase, and numbers. If you provide the passwords, password strength is your responsibility.

You can view the passwords by displaying the secrets.yaml file. For example

```
[root@mgmt1 ~]# cat ~/openstack-configs/secrets.yaml
ADMIN_USER_PASSWORD: QOZGSjVQzgu7ejv1
CINDER_DB_PASSWORD: TP2h7OAfa0VHZBb2
CINDER_KEYSTONE_PASSWORD: 0jko2Vc76h005eP9
CLOUDPULSE_KEYSTONE_PASSWORD: Vuov6wdPe5jc5kGp
COBBLER_PASSWORD: 8bhVOeciqw5jUyY5
CPULSE_DB_PASSWORD: 2DwLE0IsavQWEfMn
CVIM_MON_PASSWORD: t4qf4ORVRTtce4E0
CVIM_MON_READ_ONLY_PASSWORD: UTicXzdxn0krFplS
CVIM_MON_SERVER_PASSWORD: 1qcASpt2bRuDWbi7
DB_ROOT_PASSWORD: 5a4pQjTpCZDO1sE5
ETCD_ROOT_PASSWORD: 43yluJNsNBhv8kTp
GLANCE_DB_PASSWORD: U1HdRc7lkZslW2nD
GLANCE_KEYSTONE_PASSWORD: FpQfFnqg0AtcJbVa
HAPROXY_PASSWORD: dQzIKoi9WbCxwHGz
```

When Vault is used, it provides information about the following password only:

"CVIM_MON_PASSWORD", "CVIM_MON_READ_ONLY_PASSWORD",

"CVIM_MON_SERVER_PASSWORD", "ADMIN_USER_PASSWORD", "KIBANA_PASSWORD",

“CVIM_MON_PROXY_PASSWORD

```
# ciscovim list-secrets --getpassword <PASSWORD_KEY>
For example,
ciscovim list-secrets --getpassword ADMIN_USER_PASSWORD
+---------------------+-----------------------------+
|Secret Key           | Secret Value                |
+---------------------+-----------------------------+
```

```
| ADMIN_USER_PASSWORD| D1g8O6Ws2Woav7Ye             |
|+-------------------+-----------------------------+
```

Reconfiguration

Reconfiguration

Reconfiguring Passwords and OpenStack Configurations

> ⚠ This section is not applicable, if you have installed the optional Cisco Virtual Topology System. For information about use of passwords when VTS is installed, see *Installing Cisco VTS*

You can reset some configurations after installation including the OpenStack service password and debugs, TLS certificates, and log rotation configurations. Two files, secrets.yaml and openstack_config.yaml which are located in : */root/installer-{tag id}/openstack-configs/* contain the passwords, debugs, TLS file location, and ELK configurations. Also, Elasticsearch uses disk space for the data that is sent to it. These files can grow in size, and Cisco VIM has configuration variables that establishes the frequency and file size under which they are rotated.

Cisco VIM installer generates the OpenStack service and database passwords with 16 alphanumeric characters and stores those in /root/openstack-configs /secrets.yaml. You can change the OpenStack service and database passwords using the password reconfigure command on the deployed cloud. The command identifies the containers affected by the password change and restarts them so the new password can take effect.

> ⚠ Always schedule the password reconfiguration in a maintenance window as the container restart might disrupt the control plane.

Run the following command to view the list of passwords and configurations:

```
[root@mgmt1 installer-xxxx]# ciscovim help reconfigure
usage: ciscovim reconfigure [--regenerate_secrets] [--setpassword <secretkey>]
[--setopenstackconfig <option>]
Reconfigure the openstack cloud
Optional arguments:
--regenerate_secrets Regenerate All Secrets
--setpassword <secretkey> Set of secret keys to be changed.
--setopenstackconfig <option> Set of Openstack config to be changed.
[root@mgmt1 ~]# ciscovim list-openstack-configs
+----------------------------
+-------------------------------------------------------------------------------------------------------------------------
--+
| Name                                                  |
Option
|
+----------------------------
+-------------------------------------------------------------------------------------------------------------------------
--+
| IRONIC_DEBUG_LOGGING                  |
True
|
|
|
| OPFLEX_DEBUG_LOGGING       |
True
|
|
|
| GNOCCHI_VERBOSE_LOGGING    |
True
|
|
|
| AIM_DEBUG_LOGGING                  |
True
|
|
|
```

```
| CINDER_DEBUG_LOGGING       |
False
|
|
|
| KEYSTONE_DEBUG_LOGGING     |
False
|
|
|
| log_rotation_size                 |
100M
|
|
|
| CLOUDPULSE_VERBOSE_LOGGING |
True
|
|
|
| OCTAVIA_VERVOSE_LOGGING    |
True
|
|
|                               | MAGNUM_VERBOSE_LOGGING         |
True
|
|
|
| NOVA_DEBUG_LOGGING                |
True
|
|
|
| NEUTRON_VERBOSE_LOGGING          |
True
|
|
|
| external_lb_vip_cert                 | /root/openstack-configs/haproxy.
pem                                                                  |
|
|
| GLANCE_VERBOSE_LOGGING          |
True
|
|
|
| elk_rotation_frequency     |
weekly
|
|
|
| CEILOMETER_VERBOSE_LOGGING |
True
|
|
|
| NOVA_CPU_ALLOCATION_RATIO  |
16.0
|
|
|
| CLOUDPULSE_DEBUG_LOGGING   |
False
|
|
|
| log_rotation_frequency     |
weekly
|
```

```
|
|
| HEAT_DEBUG_LOGGING         |
False
|
|
|
| KEYSTONE_VERBOSE_LOGGING   |
True
|
|
|
| external_lb_vip_cacert     | /root/openstack-configs/haproxy-ca.
crt                                                                  |
|
|
| GNOCCHI_DEBUG_LOGGING          |
False
|
|
|
| MAGNUM_DEBUG_LOGGING                 |
True
|
|
|
| OCTAVIA_DEBUG_LOGGING      |
False
|
|
|
| log_rotation_del_older          |
8
|
|
|                                                                                                                                  |
CINDER_VERBOSE_LOGGING     |
True
|
|
|
| elk_rotation_size                |
2
|
|
|
| IRONIC_VERBOSE_LOGGING         |
True
|
|
|
| elk_rotation_del_older          |
8
|
|
|
| NEUTRON_DEBUG_LOGGING          |
True
|
|
|
| HEAT_VERBOSE_LOGGING                 |
True
|
|
|
| CEILOMETER_DEBUG_LOGGING          |
False
|
|
|
```

```
| ES_SNAPSHOT_AUTODELETE     | {u'threshold_warning': 60, u'enabled': True, u'period': 'hourly',
u'threshold_high': 80, u'threshold_low': 50}  |
|
|

| GLANCE_DEBUG_LOGGING       |
False
|
|
|
| NOVA_VERBOSE_LOGGING                  |
True
|
|
|
| NOVA_RAM_ALLOCATION_RATIO  |
1.5
|
|
|
+----------------------------
+-----------------------------------------------------------------------------------------------------------------------
--+
The command in to get the list of all passwords:
[root@mgmt1 installer-xxxx]# ciscovim list-secrets
+----------------------------------+--------------------------+--------------------------+
| Secret Key                       | Created At               | Updated At               |
+----------------------------------+--------------------------+--------------------------+
| ADMIN_USER_PASSWORD              | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| CEILOMETER_DB_PASSWORD           | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| CEILOMETER_KEYSTONE_PASSWORD     | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| CINDER_DB_PASSWORD               | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| CINDER_KEYSTONE_PASSWORD         | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| CLOUDPULSE_KEYSTONE_PASSWORD     | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| COBBLER_PASSWORD                 | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| CPULSE_DB_PASSWORD               | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| CVIM_MON_SERVER_PASSWORD         | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| DB_ROOT_PASSWORD                 | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| ETCD_ROOT_PASSWORD               | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| GLANCE_DB_PASSWORD               | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| GLANCE_KEYSTONE_PASSWORD         | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| HAPROXY_PASSWORD                 | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| GNOCCHI_DB_PASSWORD              | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| GNOCCHI_KEYSTONE_PASSWORD        | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| HEAT_DB_PASSWORD                 | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| HEAT_KEYSTONE_PASSWORD           | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| HEAT_STACK_DOMAIN_ADMIN_PASSWORD | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| HORIZON_SECRET_KEY               | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| IRONIC_DB_PASSWORD               | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| IRONIC_KEYSTONE_PASSWORD         | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| KEYSTONE_DB_PASSWORD             | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| KIBANA_PASSWORD                  | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| METADATA_PROXY_SHARED_SECRET     | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| NEUTRON_DB_PASSWORD              | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| NEUTRON_KEYSTONE_PASSWORD        | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| NOVA_DB_PASSWORD                 | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| NOVA_KEYSTONE_PASSWORD           | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| RABBITMQ_ERLANG_COOKIE           | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| RABBITMQ_PASSWORD                | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| VOLUME_ENCRYPTION_KEY            | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| VPP_ETCD_PASSWORD                | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
| WSREP_PASSWORD                   | 2020-04-19 00:52:22+00:00 | 2020-04-19 00:52:22+00:00 |
+----------------------------------+--------------------------+--------------------------+

[root@mgmt1 installer-xxxx]#
When using Vault, you can fetch information about the following user facing password only:
"CVIM_MON_PASSWORD", "CVIM_MON_READ_ONLY_PASSWORD",
"CVIM_MON_SERVER_PASSWORD", "ADMIN_USER_PASSWORD", "KIBANA_PASSWORD",
"CVIM_MON_PROXY_PASSWORD".
```

You can change specific password and configuration identified from the available list.
Run the reconfiguration command as follows:

```
# ciscovim help reconfigure
usage: ciscovim reconfigure [--regenerate_secrets]
[--setupfile <setupdata_file>]
[--alertmanager_config <alertmanager_config_file>]
[--alerting_rules_config <alerting_rules_config_file>]
[--setpassword <secretkey>]
[--setopenstackconfig <option>]
[--setopenstackconfig_file <config_file>]
[--cimc_password] [--rma_tors <tor1,tor3,...>]
[--regenerate_ceph_keyring] [-y]
Reconfigure the Openstack cloud
Optional arguments:
--regenerate_secrets Regenerate All Secrets
--setupfile <setupdata_file> User setup_data.yaml
--alertmanager_config <alertmanager_config_file>
User alertmanager_config.yaml
--alerting_rules_config <alerting_rules_config_file>
User alerting_rules_config.yaml
--setpassword <secretkey> Set of secret keys to be changed.
--setopenstackconfig <option> Set of Openstack config to be changed.
--setopenstackconfig_file <config_file>
Set of Openstack configs to be changed from
file.
--cimc_password Reconfigure CIMC password
--rma_tors <tor1,tor3,...> Comma separated list of ToRs
--regenerate_ceph_keyring Regenerate Ceph Keyring
-y, --yes Yes option to perform the action to reconfigure the Openstack cloud
[root@mgmt1 ~]# ciscovim reconfigure --setpassword ADMIN_USER_PASSWORD,NOVA_DB_PASSWORD
--setopenstackconfig HEAT_DEBUG_LOGGING,HEAT_VERBOSE_LOGGING Password for ADMIN_USER_PASSWORD:
Password for NOVA_DB_PASSWORD:
Enter T/F for option HEAT_DEBUG_LOGGING:T Enter T/F for option HEAT_VERBOSE_LOGGING:T
```

The password must be alphanumeric and can be maximum 32 characters in length.

Following are the configuration parameters for OpenStack:

Configuration Parameter	**Allowed Values**
AIM_DEBUG_LOGGING	T/F (True or False)
CEILOMETER_DEBUG_LOGGING	T/F (True or False)
CEILOMETER_VERBOSE_LOGGING	T/F (True or False)
CINDER_DEBUG_LOGGING	T/F (True or False)
CINDER_VERBOSE_LOGGING	T/F (True or False)
CLOUDPULSE_DEBUG_LOGGING	T/F (True or False)
CLOUDPULSE_VERBOSE_LOGGING	T/F (True or False)
GLANCE_DEBUG_LOGGING	T/F (True or False)
GLANCE_VERBOSE_LOGGING	T/F (True or False)
GNOCCHI_DEBUG_LOGGING	T/F (True or False)
GNOCCHI_VERBOSE_LOGGING	T/F (True or False)

HEAT_DEBUG_LOGGING	T/F (True or False)
HEAT_VERBOSE_LOGGING	T/F (True or False)
IRONIC_DEBUG_LOGGING	T/F (True or False)
IRONIC_VERBOSE_LOGGING	T/F (True or False)
KEYSTONE_DEBUG_LOGGING	T/F (True or False)
KEYSTONE_VERBOSE_LOGGING	T/F (True or False)
MAGNUM_DEBUG_LOGGING	T/F (True or False)
MAGNUM_VERBOSE_LOGGING	T/F (True or False)
NEUTRON_DEBUG_LOGGING	T/F (True or False)
NEUTRON_VERBOSE_LOGGING	T/F (True or False)
NOVA_DEBUG_LOGGING	T/F (True or False)
NOVA_VERBOSE_LOGGING	T/F (True or False)
OPFLEX_DEBUG_LOGGING	T/F (True or False)
elk_rotation_del_older	Days after which older logs are purged
elk_rotation_frequency	Available options: daily, weekly, fortnightly, monthly
elk_rotation_size	Gigabytes (entry of type float/int is allowed)
log_rotation_frequency	Frequency to rotate the logs on all the servers. Available options: daily, weekly, monthly, yearly
log_rotation_size	Indicates the maximum file size to start the rotation of the log files. Value is a float number + the unit (available options: k, M, G) Examples: 100M indicates that rotation happens when the log file size exceeds 100 Megabytes. 5.1G indicates that rotation happens when the log file size exceeds 5.1 Gigabytes.
log_rotation_del_older	Number of files (already rotated) to keep before deleting the old files
external_lb_vip_cacert	Location of the HAProxy CA certificate
external_lb_vip_cert	Location of the HAProxy certificate
NOVA_RAM_ALLOCATION_RATIO	Mem oversubscription ratio (from 1.0 to 4.0)
NOVA_CPU_ALLOCATION_RATIO	CPU allocation ratio (from 1.0 to 16.0)
ES_SNAPSHOT_AUTODELETE	The auto-deletion of the old snapshots done to to the elasticsearch database can be managed by the following parameters: enabled: [True|False] # Enable/Disable the cronjob in the management node. If the cronjob is disabled, disk space in the management can be consumed by the periodic snapshots made by Curator period: [hourly, daily, weekly, monthly] # Frequency of cron job to check for disk space consumed by the Elasticsearch snapshots threshold_warning: <1-99> # % of disk space occupied to start displaying a warning message. threshold_low: <1-99> # % of disk space occupied after cleaning up snapshots. threshold_high: <1-99> # % of disk space when starting to delete snapshots.

Alternatively, you can regenerate all passwords using regenerate_secrets command option as follows:

```
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --regenerate_secrets
```

In addition to the services passwords, you can change the debug and verbose options for Heat, Glance, Cinder, Nova, Neutron, Keystone and Cloudpulse in */root/openstack-configs/openstack_config.yaml*. You can modify the other configurations including the ELK configuration parameters, API and Horizon TLS certificates, Root CA, NOVA_RAM ALLOCATION_RATIO, NOVA_CPU_ALLOCATION_RATIO, and ES_SNAPSHOT_AUTODELETE. When reconfiguring these options (For Example API and TLS), some control plane downtime will occur, so plan the changes during maintenance windows.

The command to reconfigure these elements are:

```
ciscovim reconfigure
```

The command includes a built-in validation to ensure that you do not enter typos in the secrets.yaml or openstack_config.yaml files.

When reconfiguration of password or enabling of openstack-services fails, all subsequent pod management operations are blocked. In such case, you can contact Cisco TAC to resolve the situation.

From Cisco VIM 3.4.1, you can enable NOVA_RAM_ALLOCATION_RATIO and NOVA_CPU_ALLOCATION_RATIO on a per server basis during day-0 installation or day-2 as part of pod management.

- For pod operations, OpenStack uses the service accounts such as admin, cinder, glance, heat, heat_domain_admin, neutron, nova, placement, and cloudpulse. These accounts use passwords to authenticate each other for standard operations. You must not change the password used by these accounts, other than using the ciscovim reconfigure operation. To enforce this behavior, starting Cisco VIM 2.4.5, the "change password" panel is disabled on the Horizon dashboard for these accounts.
- You should create personal OpenStack user accounts for those who need OpenStack admin or member access. You can change the passwords for these accounts through the Horizon dashboard, OpenStack CLI, or OpenStack client interface.

Reconfiguring Glance Client Key for Central Ceph Cluster

From release Cisco VIM 3.0.0, the installation of a central ceph cluster is automated to serve the images to edge pods through Glance service. No local ceph cluster for edge pods as they have constraints on power and space. The edge pods do not need any persistent storage and provide services via a central ceph cluster for glance. For the edge pods to communicate with central ceph cluster using a cluster id, a GLANCE_CLIENT_KEY is required.

Follow the below steps to reset the GLANCE_CLIENT_KEY:

1. Regenerate the client keyring for glance.
    a. On the central ceph cluster, ssh to the management node and execute the following:

    ```
    # ciscovim reconfigure --regenerate_ceph_keyring --setupfile /root/Save<setup_data.yaml> -y
    ```

    Alternatively, you can regenerate the key via the corresponding RestAPI call:

    ```
    # curl -u <user>:<password> -X POST https://<ip|host>:8445/v1/misc --header "Content-Type:
    application/json" -d '{"action": {"reconfigure": "true", "regenerate_ceph_keyring": true}}'
    ```

2. Retrieve the generated client keyring for glance. From the management node, execute the following command to get the cluster UUID:

    ```
    # cat /root/openstack-configs/ceph/fetch/ceph_cluster_uuid.conf
    <cluster_uuid>
    # cat /root/openstack-configs/ceph/fetch/<cluster_uuid>/etc/ceph/ceph.client.glance.keyring
    [client.glance]
    key = <GLANCE_CLIENT_KEY>
    caps mon = "allow r"
    caps osd = "allow class-read object_prefix rbd_children, allow rwx pool=images"
    ```

3. Reconfigure the edge pod to use the new keyring generated on central ceph. SSH to the management node of each edge pod and execute the following:

    ```
    [root@mgmt1 ~]# cd /root/ [root@mgmt1 ~]# mkdir MyDir [root@mgmt1 ~]# cd MyDir
    [root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
    ```

```
[root@mgmt1 ~]# cp<my_setup_data.yaml> <my_setup_data_original.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the GLANCE_CLIENT_KEY with the new info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

4 Optional, but recommended to do it on a handful of pods. Once reconfiguration is done, test if the keyring works by creating and deleting glance images.

Reconfiguring CIMC/BMC Password on Existing Installation

Cisco VIM allows you to reconfigure the CIMC/BMC password on an existing installation along with OpenStack services.

> ⚠ You must have a Cisco C-series or Quanta-based pod up and running with Cisco to reconfigure the CIMC password.

1. Update the cimc_password in the CIMC-COMMON section, and/or the individual cimc_password for each server and then run the reconfigure option provided by Ciscovimclient.

```
CIMC-COMMON:
cimc_username: "admin"
cimc_password: <"new password">
::
SERVERS:
:
control-server-2:
cimc_info: {'cimc_ip': '<ip_addr>',
'cimc_username': 'admin',
'cimc_password': <'update with new passowrd'>} # only needed if each server has specific
password
```

2. To change the CIMC password for the pod, copy the setupdata into a local location and update it manually with the CIMC password as shown in the snippet above. The new password must satisfy atleast three of the following conditions:

    - 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.

    > ⚠ Do not change CIMC password directly into the exiting /root/openstack-configs/setup_data.yaml file.

3. Run the vim reconfiguration command, to post update the setup_data as follows:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# cp <my_setup_data.yaml> <my_setup_data_original.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the relevant CIMC setup_data to include LDAP info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~1]# ciscovim reconfigure --cimc_password --setupfile /root/MyDir/<my_setup_data.yaml>
```

> ⚠ After successful completion of the CIMC Password, reconfigure operation triggers an auto-back when the management node auto-back recovery feature is enabled. If the CIMC Password reconfigure fails, contact Cisco TAC to recover from the failure.

Reconfiguring Administrator Source Networks

To access the administrator services, Cisco VIM provides source IP based filtering of network requests on the management node. These services include SSH and Kibana dashboard access. When the services are configured, all admin network requests made to the management node are dropped, except the allowed list of addresses in the configuration.
Reconfiguration of administrator source network supports the following options:

- Set administrator source network list: You can add or delete the network addresses from the configuration. The entire list is replaced during reconfiguration.

- Remove administrator source network list: If the **admin_source_networks** option is removed, the source address does not filter the incoming admin service requests.

1. Configure the following commands in the setup_data.yaml file:

```
admin_source_networks: # optional, host based firewall to include the allowed list of admin's source IP
- 10.0.0.0/8
- 172.16.0.0/12
```

> ⚠ Care must be taken while updating the source networks. If the list is misconfigured, operators are locked out of access to the management node through SSH. If it is locked, the operator must log into the management node through the console port to repair the configuration.

2. To initiate the integration, copy the setupdata into a local directory by running the following command:

```
[root@mgmt1 ~]# cd /root/ [root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
```

3. Update the setupdata by running the following command:

```
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to include Admin Source Network information
```

4. Run the reconfiguration command as follows:

```
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

Password Reset for Cisco VIM Management Node

Run the following command to reset the root password of Cisco VIM management node **RHEL-7 / systemd**

1. Boot your system and wait until the **GRUB2** menu appears.
2. In the **boot loader** menu, highlight any entry and press **e**.
3. Find the line beginning with linux. At the end of this line, append the following:

```
init=/bin/sh
```

Or if you face any alarm, instead of **ro** change **rw** to **sysroot** as shown in the following example:

```
rw init=/sysroot/bin/sh
```

4. Press **Ctrl+X** to boot the system using the options you edited. Once the system boots, you can see the shell prompt without having to enter any user name or password:

```
sh-4.2#
```

5. Load the installed SELinux policy by running the following command:

```
sh-4.2# /usr/sbin/load_policy -i
```

6. Execute the following command to remount your root partition:

```
sh4.2#
mount -o remount,rw /
```

7. Reset the root password by running the following command:

```
sh4.2# passwd root
```

When prompted, enter your new root password and click **Enter** key to confirm. Enter the password for the second time to ensure that you typed it correctly and confirm with **Enter** again. If both the passwords match, a confirmation message appears.

8. Execute the following command to remount the root partition again, this time as read-only:

```
sh4.2#
 mount -o remount,ro /
```

9. Reboot the system. Now you can login as the root user using the new password set up during this procedure. To reboot the system, enter **exit** and **exit** again to leave the environment and reboot the system. For more details on changing root password, see https://access.redhat.com/solutions/918283.

Cloud Settings

Cloud Settings

You can enable specific cloud security hardening settings as a Day 0 or Day n option via reconfiguration. Listed below are the settings that are allowed in Cisco VIM.

```
cloud_settings:

  # Optional, number of incorrect password attempts before the user is locked out.
  # Default is 0 for no lockout.
  # Type: Integer, Allowed range: 0 to 100
  keystone_lockout_failure_attempts: 6

  # Optional, number of seconds for which a user is locked out after exceeding
  # keystone_lockout_failure_attempts.
  # Default is 1800 (30 minutes).
  # Type: Integer, Allowed range: 300 (5 minutes) to 86400 (24 hours).
  keystone_lockout_duration: 1800

  # Optional, number of last passwords to compare with the new one.
  # Default is 0 for no history check.
  # Type: Integer, Allowed range: 0 to 10
  keystone_unique_last_password_count: 5

  # Optional, minimum number of days allowed between password changes.
  # Default is 0 for no limit.
  # Type: Integer, Allowed range: 0 to 2
  keystone_minimum_password_age: 1

  # Optional, number of seconds of inactivity before the Horizon dashboard session
  # is logged out.
  # Default is 1800 (30 minutes).
  # Type: Integer, Allowed range: 300 (5 minutes) to 86400 (24 hours).
  horizon_session_timeout: 1800
```

Open source documentation of cloud settings is available at: https://docs.openstack.org/keystone/latest/admin/configuration.html#security-compliance-and-pci-dss

To initiate the integration of cloud settings on an existing pod, copy the setup data into a local directory and update it manually with the information listed above, and then run the *reconfigure* command as follows:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to include cloud_settings related info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

Fernet Key Operations

Fernet Key Operations

Keystone fernet token format is based on the cryptographic authentication method - Fernet. Fernet is an implementation of Symmetric Key Encryption. Symmetric key encryption is a cryptographic mechanism that uses the same cryptographic key to encrypt plaintext and the same cryptographic key to decrypt ciphertext. Fernet authentication method also supports multiple keys where it takes a list of symmetric keys, performs all encryption using the first key in a list and attempts to decrypt using all the keys from that list.

The Cisco NFVI pods uses fernet keys by default. The following operations can be carried out in Cisco NFVI pods.

To check if the fernet keys are successfully synchronized across the keystone nodes.

```
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim help check-fernet-keys
usage: ciscovim check-fernet-keys
Check whether the fernet keys are successfully synchronized across keystone nodes.
```

To forcefully rotate the fernet keys:

```
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim help rotate-fernet-keys
usage: ciscovim rotate-fernet-keys
Trigger rotation of the fernet keys on keystone
```

To resync the fernet keys across the keystone nodes:

```
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim help resync-fernet-keys
usage: ciscovim resync-fernet-keys
Resynchronize the fernet keys across all the keystone nodes
```

Certificates

Certificates

Managing Certificates

When TLS protection is configured for the OpenStack APIs, the two certificate files namely *haproxy.pem* and *haproxy-ca.crt,* are stored in the */root /openstack-configs/* directory. To verify cloud authenticity, the clients running on servers outside of the deployed cloud need a copy of the root certificate *(h aproxy-ca.crt).* If the installed certificate is signed by a well-known certificate authority , no additional configuration is needed on client servers. However, if a self-signed or local CA is used, copy the haproxy-ca.crt to each client. Following instructions are specific to the client operating system or browser, to install the certificate as a trusted certificate.

Alternatively, you can explicitly reference the certificate using the environment variable OS_CACERT or command line parameter –cacert, if OpenStack CLI is used.
While Cisco NFVI is operational, a daily check is made to monitor the expiration dates of the installed certificates. If certificates are not nearing expiration, an informational message is logged. As the certificate approaches expiration, an appropriate warning or critical message is logged.

```
2017-04-24T13:56:01 INFO Certificate for OpenStack Endpoints at 192.168.0.2:5000 expires in 500 day
```

Reconfiguring TLS Certificates

Cisco VIM provides a way to configure TLS certificates on-demand for any reason. For example, certificate expiration policies governing certificate management.
Reconfiguration of certificates in general is supported in the following components:

Cisco VIM Rest API endpoints

To reconfigure certificate files, follow the below steps:

1. Copy the new key, CA root, and certificate files into the /root*/openstack-configs* folder under the following filenames:

   ⚠ Cisco VIM RestAPI endpoint supports IP based CN (common name) TLS certificate.

   ```
   cp <new-ca-root-cert> /root/openstack-configs/mercury-ca.crt
   cp <new-key-file> /root/openstack-configs/mercury.key
   cp <new-cert-file> /root/openstack-configs/mercury.crt
   ```

   mercury-ca.crt must contain entire trust chain including RootCA and any intermediate CA. *mercury.pem* must contain the TLS certificate and the private key. The private key must not have any passphrase (non-encrypted key).

2. Once copied, run the below reconfiguration steps:

   ```
   cd /root/installer-xxxx/tools/
   ./restapi.py -a reconfigure-tls
   ```

3. If the copied certificate in Step 1 is FQDN based, use following option to reconfigure:

   ```
   cd /root/installer-xxxx/tools/
   ./restapi.py -a reconfigure-tls -d <FQDN>
   For e.g.
   ./restapi.py -a reconfigure-tls -d gg34-bn.cisco.com
   ```

4. To get the FQDN name from certificate, use following command:

```
# openssl x509 -in /root/openstack-configs/mercury-ca.crt -text -noout
. . .
Subject: C=US, ST=California, L=San Jose, O=IT, CN=gg34-bn.cisco.com
```

5. Execute ciscovim reconfigure to deploy TLS certificate to other services like Kibana, and so on.

OpenStack API Endpoints (haproxy)

It is important to replace the certificates before they expire. After Cisco NFVI is installed, you can update the certificates by replacing the *haproxy.pem* and *haproxy-ca.crt* files and running the reconfigure command. To reconfigure certificate files, follow the below steps:

1. Copy the new key, CA root, and certificate files into the *~/openstack-configs* folder under the following filenames:
   haproxy-ca.crt must contain entire trust chain including RootCA and any intermediate CA. If LDAP certificate for keystone authentication is issued by a different authority than that of haproxy certificate, the entire trust chain (RootCA and any intermediate CA) for LDAP certificate must be appended to the file.
   haproxy.pem must contain the TLS certificate and the private key. The private key must not have any passphrase (non-encrypted key).

```
cp <new-ca-root-cert> /root/openstack-configs/haproxy-ca.crt
cp <new-cert-file> /root/openstack-configs/haproxy.pem
```

2. Once copied, run the below reconfiguration steps:

```
mv /root/openstack-configs/openrc /root/<your_dir>/      # workaround as listed in CSCvt33521
cd /root/installer-xxxx
ciscovim reconfigure
```

3. For generating third-party certificates, follow the below:

   a. If *external_lb_vip_fqdn* is defined in the *setup_data,* generate the certificate using the *external_lb_vip_fqdn* as DNS.
   b. If *external_lb_vip_ipv6_address* is defined but not *external_lb_vip_fqdn*, generate the certificate using the *external_lb_vip_ipv6_address* as IP Address.
   c. If the *setup_data* contains only *external_lb_vip_address*, but neither *external_lb_vip_ipv6_address* nor *external_lb_vip_fqdn*, generate the certificate using the *external_lb_vip_address* as IP Address.

Verifying TLS Certificates

Cisco VIM provides a tool to check the expiration date of the installed certificates. If a certificate is expired, you may not be able to access the HTTPS endpoints. Checks are run daily and a syslog message is created if a certificate is nearing expiration.
In addition, a tool is provided to check certificate expiration on demand. The tool's command line support can be shown as follows:

```
# cd ~/installer-xxxx/tools
# python certificate-check.py -help
```

To check all certificates, run the following commands:

```
#cd ~/installer-xxxx/tools
# python certificate-check.py
```

To check a single certificate, run the following commands:

```
cd ~/installer-xxxx/tools
# python certificate-check.py -s openstack
```

LDAP AD Support with Keystone v3

LDAP AD Support with Keystone v3

With the introduction of KeystoneV3, the openstack service authentication can be delegated to an external LDAP/AD server. In Cisco VIM, this feature has been introduced optionally if the authorization is done by Keystone v3. Just like Keystonev3, this feature can be enabled on an existing pod running Cisco VIM. To avail this feature post pod deployment, the setup_data needs to be augmented with the following information during the pod installation.

An important pre-requisite for enabling AD/LDAP integration is that the AD/LDAP endpoint MUST be reachable from all the Controller nodes that run OpenStack Keystone Identity Service.

```
LDAP:
domain: <Domain specific name>
user_objectclass: <objectClass for Users> # e.g organizationalPerson
group_objectclass: <objectClass for Groups> # e.g. groupOfNames
user_tree_dn: '<DN tree for Users>' # e.g. 'ou=Users,dc=cisco,dc=com'
group_tree_dn: '<DN tree for Groups>' # e.g. 'ou=Groups,dc=cisco,dc=com'
suffix: '<suffix for DN>' # e.g. 'dc=cisco,dc=com'
url: '<ldap:// host:port>' # e.g. 'ldap://172.26.233.104:389'
or
url: '<ldaps|ldap>://[<ip6-address>]:[port]'
e.g.ldap://[2001:420:293:2487:d1ca:67dc:94b1:7e6c]:389 ---> note the mandatory "[.. ]"
around the ipv6 address
user: '<DN of bind user>' # e.g. 'dc=admin,dc=cisco,dc=com', Optional but need to added
along with password.
password: <password> # e.g. password of bind user, Optional but need to be added along
with DN of bind user.
user_filter = (memberOf=CN=os-users,OU=OS-Groups,DC=mercury,DC=local)
user_id_attribute = sAMAccountName
user_name_attribute = sAMAccountName
user_mail_attribute = mail # Optional
group_tree_dn = ou=OS-Groups,dc=mercury,dc=local
group_name_attribute = sAMAccountName
group_filter: '(&(objectClass=group)(|(cn=server-ops)(cn=admins)))' # Optional
group_member_attribute: memberUid # Optional
group_id_attribute: gidNumber # Optional
group_members_are_ids: True # Optional
chase_referrals: <True or False> # Optional
```

Condition for LDAP user and password parameters are as follows:

- 1 – Can be optional
- 2 – Should be mutually inclusive
- 3 – If defined, it cannot be empty

To initiate the integration of LDAP with Keystone v3 on an existing pod, copy the setupdata into a local directory, update it manually with the relevant LDAP configuration, and then run the following reconfiguration commands:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to include LDAP info)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

The reconfigure feature supports a full or partial reconfiguration of the LDAP integration service.

⚠ All the parameters within the LDAP are configurable with the exception of the domain parameter.

Integrating identity with LDAP over TLS: The automation supports keystone integration with LDAP over TLS. To enable TLS, the CA root certificate must be presented as part of the */root/openstack-configs/haproxy-ca.crt* file. The url parameter within the LDAP stanza must be set to ldaps. Additionally, the url parameter supports the following format: url: '<ldaps | ldap>://<FQDN | IP-Address>:[port]' The protocol can be one of the following: ldap for non-ssland ldaps when TLS needs to be enabled.

The ldap host can be a fully-qualified domain name (FQDN) or an IPv4 or v6 address depending on how the SSL certificates are generated.

The port number is optional and if not provided assumes that the ldap services are running on the default ports. For example: 389 for non-ssl and 636 for ssl. However, if these are not the defaults, the non-standard port numbers must be provided. Except for the domain, all other item values can be changed via the 'reconfigure' option.

NetApp from http to https

Moving Netapp transport from http to https

For deployments with NetApp running over http protocol, you can migrate it to https post-deployment.

1. To initiate the change, copy the setupdata into a local directory and manually update the name/value pair in the NetApp section:

```
NETAPP:
...
....
server_port: 443
transport_type: https
....
netapp_cert_file: <root ca path for netapp cluster only if protocol is https>
```

2. Execute the following commands, to update the NetApp section:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cd MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml <my_setup_data.yaml>
[root@mgmt1 ~]# vi my_setup_data.yaml (update the setup_data to netapp section as listed above)
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile ~/MyDir/<my_setup_data.yaml>
```

Hardening Cisco VIM Deployment

Hardening Cisco VIM Deployment

If you want to harden the Cisco VIM deployment, setup the firewalls ahead of the external interfaces.

The following table provide information about the expected traffic from the management node interfaces of Cisco VIM.

Interface	Direction	Protocol	UDP /TCP	Port	Application	Note
br_api	incoming	HTTPS	TCP	8445	RestAPI	
br_api	incoming	HTTPS	TCP	8008	RestAPI logs	
br_api	incoming	HTTPS	TCP	9000	Unified Management UI	
br_api	incoming	HTTPS	TCP	5601	Kibana	
br_api	incoming	SSH	TCP	22	SSH	
br_api	incoming	HTTPS	TCP	3000	Grafana	
br_api	outgoing	NTP	UDP	123	NTP	
br_api	outgoing	DNS	UDP	53	DNS	
br_api	outgoing	Syslog	UDP	514	Syslog	User configurable. Default value is 514.
br_api	outgoing	HTTPS	TCP	443	Cisco VIM artifacts	Download artifacts from SDS
br_mgmt	incoming	HTTP	TCP	7081	Fluentd-aggr	From all nodes to management node
br_mgmt	outgoing	HTTP	TCP	8774	CVIM cloud sanity	From management node to all the controller nodes for releases starting from Cisco VIM 3.4.5.
br_api	outgoing	HTTP	TCP	9090	Prometheus	
br_api	outgoing	HTTP	TCP	9093	Alertmanager	
localhost	incoming / outgoing	HTTP	TCP	1162	SNMP / CVIM_MON	Internal communication between processes
br_api	outgoing	SNMP	UDP	162	SNMP	Userdefined. Default value is 162
br_api	incoming	HTTP	TCP	22	SERVER_MON	From CIMC of the UCS servers.
br_api	incoming	Syslog	UDP	5140	SERVER_MON + Syslog	From CIMC of the UCS servers to the management node
br_api	outgoing	LDAP	TCP	389	LDAP	Default: 389 or defined in setup_data
br_api	outgoing	LDAPS	TCP	636	LDAPS	Default: 636 or defined in setup_data
br_api	outgoing	SSH	TCP	22	CIMC	SSH access to CIMC
br_api	outgoing	HTTP	TCP	80	CIMC	
br_api	outgoing	HTTPS	TCP	443	CIMC	

The following table provide information about the expected traffic from the control node interfaces of Cisco VIM.

Interface	Direction	Protocol	UDP/TCP	Port	Application	Note
external_lb_vip	incoming	HTTP	TCP	80	Redirects to 443	
external_lb_vip	incoming	HTTPS	TCP	443	Horizon	
external_lb_vip	incoming	HTTPS	TCP	8774	Nova	
external_lb_vip	incoming	HTTPS	TCP	6080	Nova NoVNC Proxy	
external_lb_vip	incoming	HTTPS	TCP	9696	Neutron	
external_lb_vip	incoming	HTTPS	TCP	8776	Cinder	
external_lb_vip	incoming	HTTPS	TCP	9292	Galance	
external_lb_vip	incoming	HTTPS	TCP	8000	Heat	
external_lb_vip	incoming	HTTPS	TCP	8004	Heat	
external_lb_vip	incoming	HTTPS	TCP	9999	Cloudpulse	
external_lb_vip	incoming	HTTPS	TCP	8777	Ceilometer	

external_lb_vip	incoming	HTTPS	TCP	8041	Gnocchi	
external_lb_vip	incoming	HTTPS	TCP	8778	Placement	
external_lb_vip	incoming	HTTPS	TCP	5000	Keystone	
br_mgmt	outgoing	HTTP	TCP	15672	RabbitMQ monitoring	From management node only
br_mgmt	outgoing	LDAP	TCP	389	LDAP	Default: 389 or defined in setup_data
br_mgmt	incoming	LDAPS	TCP	636	LDAPS	Default: 636 or defined in setup_data
br_mgmt	incoming	HTTP	TCP	7081	Fluentd	To management node

The following table provide information about the expected traffic from the Cisco VIM Software Hub Server node interfaces of Cisco VIM.

Interface	Direction	Protocol	UDP/TCP	Port	Application	Note
br_public	outgoing	NTP	UDP	123	NTP	
br_private	incoming	HTTPS	TCP	443	HTTPD	Browsing artifacts on a web browser and using reverse proxy for docker registry
br_private	incoming	HTTPS	TCP	8441	HTTPD	Cisco VIM pod registration on SDS Software Hub
br_public	incoming	SSH	TCP	22	SSH	

The following table provide information about the expected traffic from the Unified Management node interfaces of Cisco VIM.

Interface	Direction	Protocol	UDP/TCP	Port	Application	Note
br_api	outgoing	HTTPS	TCP	8445	Unified Management	Connect to Cisco VIM management node RestAPI
br_api	incoming	HTTPS	TCP	9000	HTTPD	UI
br_api	incoming	SSH	TCP	22	SSH	

Securing Management Node

Securing Cisco VIM Management Node

Overview

You can match the management node with customer's IT policies from SSH and password protocols point of view. The following section describes the various options to track user activity and ways to get out of a block or failed state. Listed below are the optional setup_entries used to further harden the management node security.

```
PASSWORD_MANAGEMENT:

  ## Password strength checks:                                                  |
  ##-------------------------------------------------------------------------------
  #   a. Minimum length of the password should be 8.
  #   b. 5 characters in the new password must NOT be present in the old password.
  #   c. Passwords should satisfy at least three of the following conditions:
  #        - at least 1 letter between a to z
  #        - at least 1 letter between A to Z
  #        - at least 1 number between 0 to 9
  #        - at least 1 other character
  #      Each of the mentioned condition can be called as 'class'
  #   d. Max number of 3 allowed consecutive same characters ('aaa..').
  #   e. Max number of 4 allowed consecutive characters of the same class ('1234..').
  #   f. Username should NOT be a part of the password.

  # Optional, switch to enable/disable Cisco VIM password strength checks.
  # Type: Boolean, Options: True and False, Not enabled by default.
  strength_check: <True or False>


  ## Password expiration policies:                                              |
  ##-------------------------------------------------------------------------------
  #   a. Not applicable to root user.
  #   b. Force users to change password on first login.
  #   c. max_days can only be used in conjunction with warning_age and vice versa.

  # Optional, max days after which the user is forced to change self password.
  # Type: Integer, Allowed range: 90 to 99999 (default).
  maximum_days: 90

  # Optional, number of days before the expiry of password; users will get expiry
  # notification upon login.
  # Should be less than the value of maximum_days.
  # Type: Integer, Allowed range: 1 to 99998, Default: 7.
  warning_age: 7

  # Optional, number of last passwords to compare with new one.
  # Type: Integer, Allowed range: 2 to 12, Not enabled by default.
  history_check: 2
```

```
SSH_ACCESS_OPTIONS:

  # Optional, defaults to 3600 secs
  # Type: Integer, Allowed range: 300 to 3600.
  session_idle_timeout: 3600

  # Optional, only one active SSH session or KVM/serial console.
  # Type: Boolean, Options: True and False. Not enabled by default.
```

```
enforce_single_session: <True or False>

# Optional, number of tries users will get to login.
# Type: Integer, Allowed range: 3 to 6, By default not enabled.
session_login_attempt: 3

# Optional, lockout session for a duration in seconds for the user who
# exceeded the session_login_attempt using incorrect passwords.
# Defaults to 600 secs, when session_root_lockout_duration is defined,
# otherwise not enabled.
# Type: Integer, Allowed range: 300 to 86400.
session_lockout_duration: 300

# Optional, duration in seconds up to which root user is locked out.
# if session_login_attempt is exceeded.
# Type: Integer, Allowed range: 300 to 1800, By default not enabled.
session_root_lockout_duration: 300

# Optional, days after which inactive users are locked out.
# Type: Integer, Allowed range: 90 to 99999, By default not enabled.
lockout_inactive_users: 90
```

Constraints

Though both PASSWORD_MANAGEMENT and SSH_ACCESS_OPTIONS are optional, the following constraints are applicable:

1. IPA and PASSWORD_MANAGEMENT keys are mutually exclusive.
2. Under the PASSWORD_MANAGEMENT section, the attribute of maximum_days can only be used in conjunction with warning_age and vice versa.
3. IPA and SSH_ACCESS_OPTIONS keys are mutually exclusive.
4. For SSH_ACCESS_OPTIONS, the attribute of session_lockout_duration and session_root_lockout_duration can only exist, if the session login attempts exist. The session_login_attempt cannot exist, if session_lockout_duration or session_root_lockout_duration is not defined.
5. If permit_root_login is False and SSH_ACCESS_OPTIONS is enabled, the administrator must take care of using it to avoid lockout from the system for a long duration. If permit_root_login is set to True, the Admin (root) can intervene whenever a user (vim admin) is blocked from the system either due to invalid access or inactivity.
6. The attribute of enforce_single_session under SSH_ACCESS_OPTIONS is applicable when accessing the management node via SSH session or KVM/serial console.
7. The password expiration policy does not apply to the root user. However, the root user needs to abide by the password strength checks while setting/resetting the password for self or others.
8. Enforce single session does not apply to the root user.
9. Careful planning must be done to enforce single session for non-root users, to avoid lockout due to networking issues such as the disconnection of the VPN access in the middle of the SSH session.
10. Password management forces the vim admins to change their password on the first login. This is not applicable when the feature is enabled via reconfiguration, as the vim admins would already be using the system. The vim admins must also change their password, after the expiry of maximum_days from the date on which their password is set.
11. Following SSH_ACCESS_OPTIONS subkeys are not allowed when vim_ldap_admins is enabled:

    a. session_log_attempt
    b. session_lockout_duration
    c. session_root_lockout_duration
    d. lockout_inactive_users
    e. enforce_single_session

Enabling Management Node Security

You can enable this feature on Day 0 as part of the fresh installation or later on via reconfiguration. Once enabled, you cannot disable the feature/attributes.

To enable this feature via reconfiguration, follow the below steps:

1. Take a backup of the setup data file and update the file manually with the configuration listed above.
2. Run the following reconfiguration command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# # update the setup_data to include PASSWORD_MANAGEMENT and/or SSH_ACCESS_OPTIONS
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

Operation Details

As the VIM admins can enter a blocked state due to invalid password usage or inactivity, the root user can track and rectify such activities.

Listed below are some of the operations the root administration can do to get the vim admins out of the bind.

Check Password Age Policies

Admin (root) user can check the password policy for a particular vim admin or vim admins can also check theirs via the below change utility.

```
# change -l <vim_admin_user_name>
Last password change                                    : Jan 13, 2020
Password expires                                        : Apr 22, 2020
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 100
Number of days of warning before password expires       : 3
```

View/Reset Authentication Failure Records

The vim_admins cannot access their account for session_lockout_duration if the session login attempts are exceeded. Admin (root) user can intervene if required.

```
Display authentication failure records:
# faillock --user <vim_admin_user_name>
<vim_admin_user_name>:
When                Type  Source                                         Valid
2020-01-15 15:25:17 RHOST 10.65.252.219                                      V
2020-01-15 13:41:31 RHOST 10.65.252.219                                      I
2020-01-15 13:41:34 RHOST 10.65.252.219                                      I
2020-01-15 13:41:53 RHOST 10.65.252.219                                      I
2020-01-15 13:41:58 RHOST 10.65.252.219                                      I
2020-01-15 14:15:11 RHOST 10.65.252.219                                      I
2020-01-15 14:15:16 RHOST 10.65.252.219                                      I
2020-01-15 15:25:20 RHOST 10.65.252.219                                      V


Reset authentication failure records for a vim_admin user:
# faillock --user <vim_admin_user_name> --reset

Reset all authentication failure records:
# faillock --reset
```

View/Unlock Inactive Accounts

The vim_admin account is locked out if the login to the management node is not performed for a predetermined number of days specified against lockout_inactive_users.

```
View user account status:
# passwd -S <vim_admin_user_name>

Reset user passwords:
# passwd <vim_admin_user_name>

Unlock user account:
# passwd -u <vim_admin_user_name>
```


Usage of any other commands outside the context of *ciscovim* (Cisco VIM CLI) is strictly not allowed.

Storage

Storage

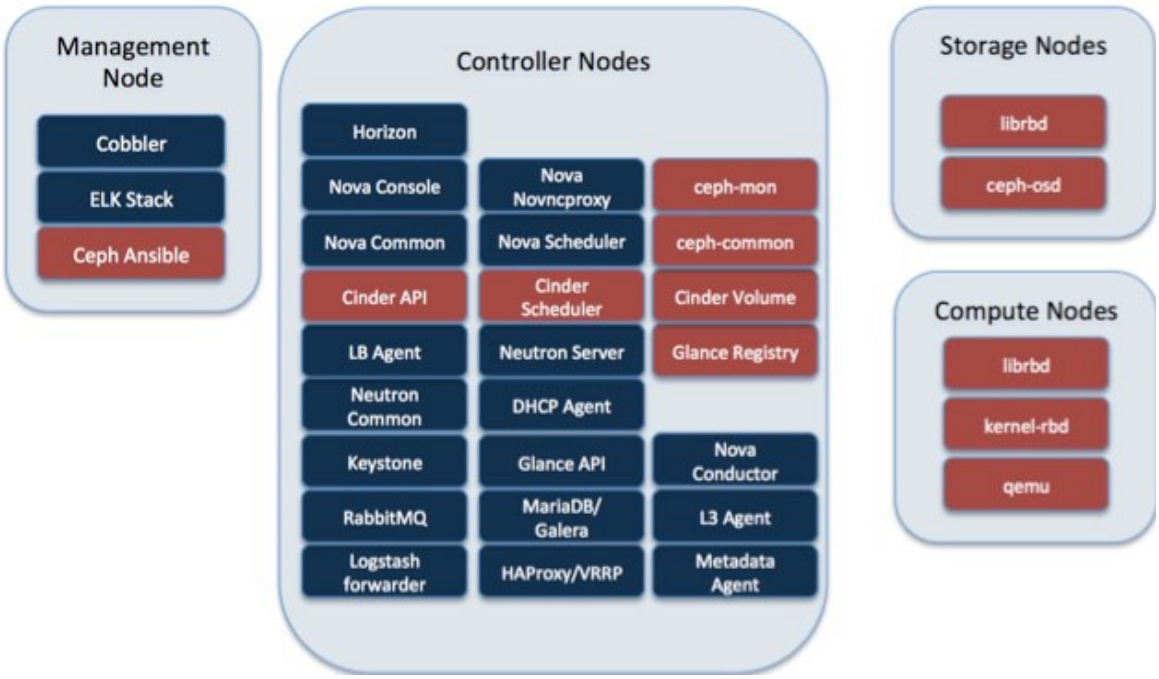
Storage Architecture

Storage Architecture

OpenStack has multiple storage back ends. Cisco NFVI uses the Ceph backend. As Ceph supports both block and object storage, it is used to store VM images and volumes that can be attached to VMs. Multiple OpenStack services that depend on the storage backend include:

- Glance (OpenStack image service): Uses Ceph to store images.
- Cinder (OpenStack storage service): Uses Ceph to create volumes that can be attached to VMs.
- Nova (OpenStack compute service): Uses Ceph to connect to the volumes created by Cinder.

The following figure shows the Cisco NFVI storage architecture component model.



Ceph Storage

Ceph Storage

Verifying and Displaying Ceph Storage Pools

Ceph is configured with four independent pools: images, volumes, vms, and backups. (A default rbd pool is used internally.) Each Ceph pool is mapped to an OpenStack service. The Glance service stores data in the images pool, and the Cinder service stores data in the volumes pool. The Nova service can use the vms pool to boot ephemeral disks directly from the Ceph cluster depending on how the NOVA_BOOT_FROM option in the *~/openstack-configs /setup_data.yaml* is configured prior to Cisco NFVI installation.

If NOVA_BOOT_FROM is set to ceph before you run the Cisco NFVI installation, the Nova service boots up from the Ceph vms pool. By default, NOVA_BOOT_FROM is set to local, which means that all VM ephemeral disks are stored as files in the compute nodes. Changing this option after installation does not affect the use of the vms pool for ephemeral disks.

The Glance, Cinder, and Nova OpenStack services depend on the Ceph cluster for backend storage. Therefore, they need IP connectivity to the controller nodes. The default port used to connect Glance, Cinder, and Nova to the Ceph cluster is 6789. Authentication through cephx is required, which means authentication tokens called keyrings, must be deployed to the OpenStack components for authentication.

To verify and display the Cisco NFVI Ceph storage pools:

1. Launch a SSH session to a controller node, for example:

```
[root@management-server-cisco ~]# ssh root@controller_server-1
```

2. Navigate to the Ceph Monitor container

```
[root@controller_server-1 ~]# cephmon
```

3. List the Ceph pools:

```
cephmon_4612 [root@controller_server-1 ~]# ceph osd lspools
0 rbd,1 images,2 volumes,3 vms,4 backups
```

4. List the images pool content:

```
cephmon_4612 [ceph@controller_server-1 /]$ rbd list images
a4963d51-d3b7-4b17-bf1e-2ebac07e1593
```

Checking the Storage Cluster Health

Cisco recommends that you perform a few verification to determine whether the Ceph cluster is healthy and is connected to the Glance, Cinder, and Nova OpenStack services that have Ceph cluster dependencies. The first task to check the health of the cluster itself by completing the following steps:

1. From the Cisco NFVI management node, launch a SSH session to a controller node, for example:

```
[root@management-server-cisco ~]# ssh root@controller_server-1
```

2. Navigate to Ceph Monitor container:

```
[root@controller_server-1 ~]# cephmon
```

3. Check the Ceph cluster status:

```
cephmon_4612 [ceph@controller_server-1 ceph]$ ceph status
Sample response:
```

```
cluster dbc29438-d3e0-4e0c-852b-170aaf4bd935
health HEALTH_OK
monmap e1: 3 mons at {ceph-controller_server-1=20.0.0.7:6789/0,
ceph-controller_server-2=20.0.0.6:6789/0,ceph-controller_server-3=20.0.0.5:6789/0}
election epoch 8, quorum 0,1,2 ceph-controller_server-3,
ceph-controller_server-2,ceph-controller_server-1
osdmap e252: 25 osds: 25 up, 25 in
pgmap v593: 1024 pgs, 5 pools, 406 MB data, 57 objects
2341 MB used, 61525 GB / 61527 GB avail
1024 active+clean
```

This example displays three monitors, all in good health, and 25 object storage devices (OSDs). All OSDs show as up and in the cluster.

4. To see a full listing of all OSDs sorted by storage node, enter:

```
cephmon_4612 [ceph@controller_server-1 ceph]$ ceph osd tree
Sample response:
ID WEIGHT TYPE NAME UP/DOWN REWEIGHT PRIMARY-AFFINITY
-1 60.18979 root default
-2 18.96994 host controller_server-2
1 2.70999 osd.1 up 1.00000 1.00000
5 2.70999 osd.5 up 1.00000 1.00000
6 2.70999 osd.6 up 1.00000 1.00000
11 2.70999 osd.11 up 1.00000 1.00000
12 2.70999 osd.12 up 1.00000 1.00000
17 2.70999 osd.17 up 1.00000 1.00000
20 2.70999 osd.20 up 1.00000 1.00000
-3 18.96994 host controller_server-1
0 2.70999 osd.0 up 1.00000 1.00000
4 2.70999 osd.4 up 1.00000 1.00000
8 2.70999 osd.8 up 1.00000 1.00000
10 2.70999 osd.10 up 1.00000 1.00000
13 2.70999 osd.13 up 1.00000 1.00000
16 2.70999 osd.16 up 1.00000 1.00000
18 2.70999 osd.18 up 1.00000 1.00000
-4 18.96994 host controller_server-3
2 2.70999 osd.2 up 1.00000 1.00000
3 2.70999 osd.3 up 1.00000 1.00000
7 2.70999 osd.7 up 1.00000 1.00000
9 2.70999 osd.9 up 1.00000 1.00000
14 2.70999 osd.14 up 1.00000 1.00000
15 2.70999 osd.15 up 1.00000 1.00000
19 2.70999 osd.19 up 1.00000 1.00000
-5 3.27997 host controller_server-4
21 0.81999 osd.21 up 1.00000 1.00000
22 0.81999 osd.22 up 1.00000 1.00000
23 0.81999 osd.23 up 1.00000 1.00000
24 0.81999 osd.24 up 1.00000 1.00000
```

5. After you verify that the Ceph cluster is in good health, check whether the individual OpenStack components have connectivity and their authentication tokens or keyrings match with the Ceph Monitor keyrings. That is, check the connectivity and authentication between Ceph and Glance, Ceph and Cinder, and Ceph and Nova.

Working with Multi-Backend Ceph

The OpenStack component that provides an API to create block storage for cloud is called OpenStack Block Storage service or Cinder. Cinder requires you to configure single backend (by default) or multiple backends.
Cisco VIM supports the following Cinder backends either configured in isolation or parallel.

- Storage nodes full of SSDs disks
- Storage nodes full of HDDs disks

Choosing multi-backend ceph is available as a Day 0 option, that is, the cloud administrator must choose single backend or multi-backend storage option at the beginning. It is recommended to have four nodes with a minimum being three nodes for each type of storage (HDD or SSD).
To enable support for Cinder multi-backends, update the *setup_data.yaml* to include the *osd_disk_type* as HDD/SSD under *hardware_info* of the storage server as given below:

```
storage-hdd-server-1: ---I Need minimum of 3; recommended to have 4
 cimc_info: {cimc_ip: <cimc_ip}
```

```
hardware_info: {osd_disk_type: HDD}
rack_info: {rack_id: RackA}
storage-ssd-server-1: --I ---I Need minimum of 3; recommended to have 4
cimc_info: {cimc_ip: <cimc_ip>}
hardware_info: {osd_disk_type: SSD}
rack_info: {rack_id: RackB}
```

After successful deployment of Cisco VIM, follow the below steps to create Cinder multi-backends:

1. Log into Horizon of the cloud and navigate to <**Admin/Volume/Volume Types** tab:

    a. Specify the Name and Description (Optional). The Name can be **volume-ssd** or **volume-hdd** for SSD or HDD, respectively.
    b. Select **view extraspecs** from the dropdown.
    c. Click **Create** and update the **Key** with **volume_backend_name**.
    d. Enter the **Value** as given below:

    For SSD, the Value is **ceph-ssd**. For HDD, the Value is **ceph**.
2. Create Volume from Horizon for each backend type:

    a. Choose **Project/Volumes/Volumes**
    b. Click **CreateVolume**

    Volume name : SSD volume (example)

    Description: Optional

    Volume Source : use the default

    Type : Choose the volume type from the dropdown. It can be volume-ssd/volume-hdd.
3. Attach the volume to Instance.

    a. Navigate to **Project/compute/instance**.
    b. Select the instance to be attached the volume.
    c. From the drop down **Attach volume**, select the Volume ID.

Ceph Storage Expansion

From release Cisco VIM 3.0.0, a command expand-storage is available to add disks to expand an already deployed Ceph storage cluster. You can deploy the storage nodes in the Openstack PoD in one of the two ways given below:

- Combination of HDD and SSD drives with Ceph deployed with dedicated journals.
- All SSD drives with Ceph deployed with collocated journals.

The expand-storage command is supported only on storage nodes with a combination of HDD and SSD drives.

You must install disk drives based on how the node is originally deployed. If you have a storage node with a 1 SSD/4 HDDs ratio, insert the disks with the same SSD/HDD ratio for expanding the storage. The expand-storage command looks for the blocks of disks with that ratio during the expansion, and installs one block at a time.

Workflow

- Use ciscovim list-nodes to find a node with a role of *block-storage*.
- Insert a block of disks, based on your storage deployment into the target node.
- Log into the CIMC of the target node and navigate to the storage panel.
- Verify that no disks are reporting errors.
- If any disk reports foreign configuration, clear the configuration.
- Enable JBOD, if RAID controller is used.
- Run cloud-sanity and ensure that no failure occurs.
- Run osdmgmt check-osds to check the state and number of the OSDs currently installed.
- Run expand-storage with the name of the target storage node.
- Run osdmgmt check-osds to check the state and number of the OSDs .
- Compare the outputs of the two osdmgmt check-osd commands and verify whether the new disks are added as additional OSDs.

The expand storage command runs in the same manner as other *ciscovim* commands but with various steps executed at a time. The command execution is stopped in case of any failure. You can view the logs once the command execution is complete. The steps for the expand-storage command are:

- Hardware validations
- Baremetal
- CEPH for expansion
- VMTP

Command Help

```
$ ciscovim help expand-storage
usage: ciscovim expand-storage --setupfile SETUPFILE [-y] <node>
Expand storage node capacity
Positional arguments:
<node> Expand Storage capacity of a storage node
Optional arguments:
--setupfile SETUPFILE <setupdata_file>. Mandatory for any POD management
operation.
-y, --yes Yes option to perform the action
```

Workflow command examples:

To expand the storage of node i13-27-test, get the current number/state of the OSDs in the cluster.

```
$ ciscovim list-nodes
+-------------+--------+---------------+---------------+
| Node Name   | Status | Type          | Management IP |
+-------------+--------+---------------+---------------+
| i13-20      | Active | control       | 15.0.0.7      |
| i13-21      | Active | control       | 15.0.0.8      |
| i13-22      | Active | control       | 15.0.0.5      |
| i13-23      | Active | compute       | 15.0.0.6      |
| i13-24      | Active | compute       | 15.0.0.10     |
| i13-25      | Active | block_storage | 15.0.0.11     |
| i13-26      | Active | block_storage | 15.0.0.9      |
| i13-27-test | Active | block_storage | 15.0.0.4      |
+-------------+--------+---------------+---------------+
ciscovim osdmgmt show check-osds --id <id>
+--------------------+-------------+---------------+-----------+---------+
| Message                  | Host        | Role          | Server    | State   |
+--------------------+-------------+---------------+-----------+---------+
| Overall OSD Status | i13-25            | block_storage | 15.0.0.11 | Optimal |
|                            | i13-26      | block_storage | 15.0.0.9  | Optimal |
|                    | i13-27-test | block_storage | 15.0.0.4  | Optimal |
|                            |             |               |           |         |
| Number of OSDs     | i13-25      | block_storage | 15.0.0.11 | 10      |
|                    | i13-26      | block_storage | 15.0.0.9  | 10      |
|                    | i13-27-test | block_storage | 15.0.0.4  | 12      |
+--------------------+-------------+---------------+-----------+---------+
+-------------+--------+--------+----+------------+-----------+-----------
| Host              | OSDs   | Status | ID | HDD Slot   | Path      | Mount
+-------------+--------+--------+----+------------+-----------+-----------
....
| i13-27-test | osd.2  | up     | 2  | 4 (JBOD)   | /dev/sda1 |
|                  | osd.5  | up     | 5  | 3 (JBOD)   | /dev/sdb1 |
|                   | osd.8  | up     | 8  | 6 (JBOD)   | /dev/sdc1 |
|             | osd.11 | up     | 11 | 2 (JBOD)   | /dev/sdd1 |
|             | osd.14 | up     | 14 | 5 (JBOD)   | /dev/sde1 |
|                  | osd.19 | up     | 19 | 9 (JBOD)   | /dev/sdi1 |
|                  | osd.24 | up     | 24 | 10 (JBOD)  | /dev/sdj1 |
|             | osd.27 | up     | 27 | 8 (JBOD)   | /dev/sdl1 |
|             | osd.28 | up     | 28 | 12 (JBOD)  | /dev/sdm1 |
|             | osd.29 | up     | 29 | 11 (JBOD)  | /dev/sdn1 |
|             | osd.30 | up     | 30 | 13 (JBOD)  | /dev/sdo1 |
|             | osd.31 | up     | 31 | 17 (JBOD)  | /dev/sdp1 |
+-------------+--------+--------+----+------------+-----------+
```

Run the expand-storage command:

```
# ciscovim expand-storage i13-27-test --setupfile setup_data.yaml
Perform the action. Continue (Y/N)Y
Monitoring StorageMgmt Operation
. . . . Cisco VIM Runner logs
The logs for this run are available in
<ip>:/var/log/mercury/05f068de-86fd-479c-afda-c54b14ffdd3e
############################################
Cisco Virtualized Infrastructure Manager
############################################
```

```
[1/3][VALIDATION: INIT] [ / ]
0min 0sec
Management Node Validations!
..
Omitted for doc
..
[1/3][VALIDATION: Starting HW Validation, takes time!!!] [ DONE! ]
Ended Installation [VALIDATION] [Success]
[2/3][CEPH: Checking for Storage Nodes] [ DONE! ]
[2/3][CEPH: Creating Ansible Inventory] [ DONE! ]
..
Omitted for doc
..
[2/3][CEPH: Waiting for server to come back first try] [ DONE! ]
Ended Installation [CEPH] [Success]
VMTP Starts
/home/vmtp/.ssh/id_rsa already exists.
Omitted for doc
..
[3/3][VMTP: INIT] [ DONE! ]
Ended Installation [VMTP] [Success]
The logs for this run are available in
<ip>:/var/log/mercury/05f068de-86fd-479c-afda-c54b14ffdd3e
===========
Check the OSDs
ciscovim osdmgmt create check-osds
+------------+--------------------------------------+
| Field      | Value                                |
+------------+--------------------------------------+
| action     | check-osds                           |
| command    | create                               |
| created_at | 2019-01-07T19:00:23.575530+00:00     |
| id         | adb56a08-fdc5-4810-ac50-4ea6c6b38e3f |
| locator    | False                                |
| osd        | None                                 |
| result     |                                      |
| servers    | None                                 |
| status     | not_run                              |
| updated_at | None                                 |
+------------+--------------------------------------+
ciscovim osdmgmt list check-osds
+--------------------------------------+------------+----------+----------
| ID                                   | Action     | Status   |  Created  |
+--------------------------------------+------------+----------+----------
| cd108b85-2678-4aac-b01e-ee05dcd6fd02 | check-osds | Complete | 2019-01-
| adb56a08-fdc5-4810-ac50-4ea6c6b38e3f | check-osds | Complete | 2019-01-|
+--------------------------------------+------------+----------+----------
ciscovim osdmgmt show check-osds --id <id>
+--------------------+-------------+---------------+-----------+---------+
| Message            | Host        | Role          | Server    | State   |
+--------------------+-------------+---------------+-----------+---------+
| Overall OSD Status | i13-25      | block_storage | 15.0.0.11 | Optimal |
|                    | i13-26      | block_storage | 15.0.0.9  | Optimal |
|                    | i13-27-test | block_storage | 15.0.0.4  | Optimal |
| Number of OSDs     | i13-25      | block_storage | 15.0.0.11 | 10      |
|                    | i13-26      | block_storage | 15.0.0.9  | 10      |
|                    | i13-27-test | block_storage | 15.0.0.4  | 16      |
+--------------------+-------------+---------------+-----------+---------+
+-------------+--------+--------+----+------------+-----------+-----------
| Host        | OSDs   | Status | ID | HDD Slot   | Path      | Mount
+-------------+--------+--------+----+------------+-----------+-----------
omitted for doc
|i13-27-test  | osd.2  | up     | 2  | 4 (JBOD)   | /dev/sda1 |
|             | osd.5  | up     | 5  | 3 (JBOD)   | /dev/sdb1 |
|             | osd.8  | up     | 8  | 6 (JBOD)   | /dev/sdc1 |
|             | osd.11 | up     | 11 | 2 (JBOD)   | /dev/sdd1 |
|             | osd.14 | up     | 14 | 5 (JBOD)   | /dev/sde1 |
|             | osd.19 | up     | 19 | 9 (JBOD)   | /dev/sdi1 |
|             | osd.24 | up     | 24 | 10 (JBOD)  | /dev/sdj1 |
|             | osd.27 | up     | 27 | 8 (JBOD)   | /dev/sdl1 |
```

```
|             | osd.28 | up         | 28 | 12 (JBOD)  | /dev/sdm1 |
|             | osd.29 | up         | 29 | 11 (JBOD)  | /dev/sdn1 |
|             | osd.30 | up           | 30 | 13 (JBOD)  | /dev/sdo1 |
|             | osd.31 | up          | 31 | 17 (JBOD)  | /dev/sdp1 |
|             | osd.32 | up         | 32 | 15 (JBOD)  | /dev/sdq1 |
|             | osd.33 | up         | 33 | 14 (JBOD)  | /dev/sdr1 |
|             | osd.34 | up         | 34 | 16 (JBOD)  | /dev/sds1 |
|             | osd.35 | up         | 35 | 7 (JBOD)   | /dev/sdt1 |
+-------------+--------+--------+----+------------+-----------+------------
```

Glance

Glance

Checking Glance Connectivity

The Glance API container must be connected to the Cisco NFVI controller nodes. Complete the following steps to verify the Glance connectivity to controller node:

1. From the management node, examine the IP addresses of controller node:

   ```
   [root@management-server-cisco ~]# cat /root/openstack-configs/mercury_servers_info
   ```

2. From the management node, launch a SSH session to a controller node, for example:

   ```
   [root@management-server-cisco ~]# ssh root@controller_server-1
   ```

3. Navigate to the Glance API container:

   ```
   [root@controller_server-1 ~]# glanceapi
   ```

4. Check the Glance API container connectivity to the storage IP address of the controller node different from the one entered in Step 2:

   ```
   glanceapi_4612 [glance@controller_server-1 /]$ curl <storage_ip_of_another_controller>:6789
   ```

   If the connection is successful, no message is displayed, but you need to do Ctrl+C to terminate the connection:

   ```
   glanceapi_4612 [glance@controller_server-1 /]$ curl 7.0.0.16:6789
   ```

   If the connection is not successful, the following message is shown:

   ```
   glanceapi_4612 [glance@controller_server-1 /]$ curl 7.0.0.16:6789 curl: (7)
   Failed connect to controller_server-2:6789; Connection refused
   ```

   The above message indicates that the Ceph monitor running on the target controller node controller_server-2 is not listening on the specified port or there is no route to it from the Glance API container.
5. To ensure that one connection path is available for the Glance API, checking one controller node is sufficient. As Cisco NFVI controller nodes run as part of an HA cluster, you should run Step 3 above targeting all the controller nodes in the Cisco NFVI pod.
6. After you verify the Glance API connectivity to all Cisco NFVI controller nodes, check the Glance keyring to ensure that it matches with the Ceph monitor keyring.

Verifying Glance and Ceph Monitor Keyrings

Complete the following steps to verify the Glance API keyring matches the Ceph Monitor keyring.

1. Launch a SSH session to a controller node, for example:

   ```
   [root@management-server-cisco ~]# ssh root@controller_server-1
   ```

2. Navigate to the Glance API container:

   ```
   [root@controller_server-1 ~]# glanceapi
   ```

3. Check the Glance keyring content, for example:

```
glanceapi_4612 [glance@controller_server-1 /]$ cat /etc/ceph/client.glance.keyring [client.glance]
key = AQA/pY1XBAnHMBAAeS+0Wmh9PLZe1XqkIW/p0A==
```

4. On the management node, check the CEPH cluster UUID:

```
[root@management-server-cisco ~]# cat /root/openstack-configs/ceph/fetch/ceph_cluster_uuid.conf
0e96e7f2-8175-44b3-ac1a-4f62de12ab9e
```

5. Display the Ceph Glance keyring content:

```
[root@management-server-cisco ~]# cat
/root/openstack-configs/ceph/fetch/0e96e7f2-8175-44b3-ac1a-4f62de12ab9e/etc/ceph/ceph.client.glance.
keyring
[mon.]
key = AQA/pY1XBAnHMBAAeS+0Wmh9PLZe1XqkIW/p0A==
```

6. Verify whether the keyring matches the Glance API keyring displayed in Step 3.
7. To ensure that Ceph and Glance are connected, import a Glance image using Horizon or the Glance CLI. After you import an image, compare the IDs seen by Glance and by Ceph. If the IDs match, it indicates that Ceph is handling the backend for Glance.

Verifying Glance Image ID on Ceph

The following steps verify whether Ceph is properly handling new Glance images, by checking that the image ID for a new Glance image is the same as the image ID displayed in Ceph.

1. From the management node, load the OpenStack authentication variables:

```
[root@management-server-cisco ~]# source ~/openstack-configs/openrc
```

2. Import any Glance image. In the example below, a RHEL 7.1 qcow2 image is used.

```
[root@management-server-cisco images]# openstack image create
"rhel" --disk-format qcow2 --container-format bare --file rhel-guest-image-7.1-20150224.0.x86_64.qcow2
```

3. List the Glance images:

```
[root@management-server-cisco images]# openstack image list | grep rhel
| a4963d51-d3b7-4b17-bf1e-2ebac07e1593 | rhel
```

4. Navigate to the Ceph Monitor container:

```
[root@controller_server-1 ~]# cephmon
```

5. Display the contents of the Ceph images pool:

```
cephmon_4612 [ceph@controller_server-1 ceph]$ rbd list images | grep
a4963d51-d3b7-4b17-bf1e-2ebac07e1593
a4963d51-d3b7-4b17-bf1e-2ebac07e1593
```

6. Verify that the Glance image ID displayed in Step 3 matches with the image ID displayed by Ceph.

Cinder

Cinder

Checking Cinder Connectivity

The Cinder volume container must have connectivity to the Cisco NFVI controller nodes. Complete the following steps to verify that Cinder volume has connectivity to the controller nodes:

1. From the management node, examine the IP addresses of controller node:

   ```
   [root@management-server-cisco ~]# cat /root/openstack-configs/mercury_servers_info
   ```

2. From the management node, launch a SSH session to a controller node, for example:

   ```
   [root@management-server-cisco ~]# ssh root@controller_server-1
   ```

3. Navigate to the Cinder volume container:

   ```
   [root@controller_server-1 ~]# cindervolume
   ```

4. Check the Cinder volume container connectivity to the storage IP address of controller node different from the one entered in Step 1:

   ```
   cindervolume_4612 [cinder@controller_server-1 /]$ curl 7.0.0.16:6789
   ```

   If the connection is successful, no message is displayed, but you need to do a Ctrl-C to terminate the connection:

   ```
   cindervolume_4612 [cinder@controller_server-1 /]$ curl 7.0.0.16:6789
   ```

   If the connection is not successful, the following is displayed:

   ```
   cindervolume_4612 [cinder@controller_server-1 /]$ curl controller_server-2:6789
   curl: (7) Failed connect to controller_server-2:6789; Connection refused
   ```

   The above message indicates that the Ceph monitor running on the target controller node controller_server-2 is not listening on the specified port or there is no route to it from the Cinder volume container.
5. To ensure that one connection path is available for the Cinder volume, it is enough to check one controller node. As the Cisco NFVI controller nodes run as part of an HA cluster, repeat Step 3 targeting all the controller nodes in the Cisco NFVI pod.
6. After you verify the Cinder volume connectivity to all Cisco NFVI controller nodes, check whether the Cinder keyring matches the Ceph monitor keyring.Verifying Cinder and Ceph Monitor Keyrings.

Verifying Cinder and Ceph Monitor Keyrings

Complete the following steps to verify whether the Cinder volume keyring matches with the Ceph Monitor keyring.

1. From the management node, launch a SSH session to a controller node, for example:

   ```
   [root@management-server-cisco ~]# ssh root@controller_server-1
   ```

2. Navigate to the Cinder volume container:

   ```
   [root@controller_server-1 ~]# cindervolume
   ```

3. Check the Cinder keyring content, for example:

```
cindervolume_4612 [cinder@controller_server-1 /]$ cat /etc/ceph/client.cinder.keyring
[client.cinder]
key = AQA/pY1XBAnHMBAAeS+0Wmh9PLZe1XqkIW/p0A==
```

4. On management node, check the CEPH cluster UUID:

```
[root@management-server-cisco ~]# cat /root/openstack-configs/ceph/fetch/ceph_cluster_uuid.conf
0e96e7f2-8175-44b3-ac1a-4f62de12ab9e
```

5. Display the Ceph Cinder keyring content:

```
[root@management-server-cisco ~]# cat
/root/openstack-configs/ceph/fetch/0e96e7f2-8175-44b3-ac1a-4f62de12ab9e/etc/ceph/ceph.client.cinder.
keyring
[client.cinder]
key = AQA/pY1XBAnHMBAAeS+0Wmh9PLZe1XqkIW/p0A==
```

6. Verify whether the keyring matches with the Cinder volume keyring displayed in Step 3.
7. For final verification of Ceph and Cinder connectivity, import a Cinder image using Horizon or the Cinder CLI. After you import the image, compare the IDs seen by Cinder and by Ceph. If the IDs match, it indicates that Ceph is handling the backend for Cinder.

Verifying Cinder Volume ID on Ceph

The following steps verify whether Ceph is properly handling new Cinder volumes by checking that the volume ID for a new Cinder volume is the same as the volume ID displayed in Ceph.

1. From the management node, load the OpenStack authentication variables:

```
[root@management-server-cisco ~]# source ~/openstack-configs/openrc
```

2. Create an empty volume:

```
[root@management-server-cisco ~]# openstack volume create --size 5 ciscovol1
```

   The preceding command creates a new 5 GB Cinder volume named ciscovol1.
3. List the Cinder volumes:

```
[[root@management-server-cisco ~]# openstack volume list
+--------------------------------------+-----------+-----------+------+-------------+
| ID                                   | Name      | Status    |
Size | Attached to |
+--------------------------------------+-----------+-----------+------+-------------+
| 3017473b-6db3-4937-9cb2-bd0ba1bf079d | ciscovol1 | available | 5    |                      |
+--------------------------------------+-----------+-----------+------+-------------+
```

4. Navigate to the Ceph Monitor container:

```
[root@controller_server-1 ~]# cephmon
```

5. Display the contents of the Ceph volumes pool:

```
cephmon_4612 [ceph@controller_server-1 ceph]$ rbd list volumes
volume-3017473b-6db3-4937-9cb2-bd0ba1bf079d
```

6. Verify whether the Cinder volume ID displayed in Step 3 matches with the volume ID displayed by Ceph, excluding the *volume-* prefix.

Nova

Nova

Checking Nova Connectivity

The Nova libvirt container must have connectivity to the Cisco NFVI controller nodes. Complete the following steps to verify Nova has connectivity to the controller nodes:

1. From the management node, examine the IP addresses of controller node:

```
[root@management-server-cisco ~]# cat /root/openstack-configs/mercury_servers_info
```

2. From the management node, launch a SSH session to a controller node, for example:

```
[root@management-server-cisco ~]# ssh root@Computenode_server-1
```

3. Navigate to the Nova libvirt container:

```
[root@compute_server-1 ~]# libvirt
```

4. Check the Nova libvirt container connectivity to the storage address of the controller node different from the one entered in Step 1:

```
novalibvirt_4612 [root@compute_server-1 /]$ curl 7.0.0.16:6789
```

   If the connection is successful, no message is displayed, but you need to do a Ctrl-C to terminate the connection:

   If the connection is not successful, a message is displayed as follows:

```
novalibvirt_4612 [root@compute_server-1 /]$ curl 7.0.0.16:6789
curl: (7) Failed connect to controller_server-1:6789; Connection refused
```

   The above message indicates that the Ceph monitor running on the target controller node controller_server-1 is not listening on the specified port or there is no route to it from the Nova libvirt container.
5. To ensure that one connection path is available for the Nova libvirt, checking one controller node is sufficient. As Cisco NFVI controller nodes run as part of an HA cluster, you should run Step 3 above targeting all the controller nodes in the Cisco NFVI pod.
6. After you verify the Nova libvirt connectivity to all Cisco NFVI controller nodes, check the Nova keyring to ensure that it matches with the Ceph monitor keyring.

Verifying Nova and Ceph Monitor Keyrings

Complete the following steps to verify whether the Nova libvirt keyring matches with the Ceph Monitor keyring.

1. From the management node, launch a SSH session to a controller node, for example:

```
[root@management-server-cisco ~]# ssh root@compute_server-1
```

2. Navigate to the Nova libvert container:

```
[root@compute_server-1 ~]# libvirt
```

3. Extract the libvirt secret that contains the Nova libvirt keyring:

```
novalibvirt_4612 [root@compute_server-1 /]# virsh secret-list
UUID                                                                 Usage ...
```

```
--------------------------------------------------------------------
b5769938-e09f-47cb-bdb6-25b15b557e84 ceph client.cinder
```

4. Get the keyring from the libvert secret:

```
novalibvirt_4612 [root@controller_server-1 /]# virsh secret-get-value
b5769938-e09f-47cb-bdb6-25b15b557e84 AQBApY1XQCBBEBAAroXvmiwmlSMEyEoXKl/sQA==
```

5. On management node, check the CEPH cluster UUID:

```
[root@management-server-cisco ~]# cat /root/openstack-configs/ceph/fetch/ceph_cluster_uuid.conf
0e96e7f2-8175-44b3-ac1a-4f62de12ab9e
```

6. Display the Ceph Cinder keyring content:

```
[root@management-server-cisco ~]# cat
/root/openstack-configs/ceph/fetch/0e96e7f2-8175-44b3-ac1a-4f62de12ab9e/etc/ceph/ceph.client.cinder.
keyring
[client.cinder]
key = AQBApY1XQCBBEBAAroXvmiwmlSMEyEoXKl/sQA==
```

7. Verify whether the keyring matches with the Nova libvirt keyring displayed in Step 3.

> ⚠ In the above example, the Cinder keyring is checked even though this procedure is for the Nova libvirt keyring. This occurs because the Nova services need access to the Cinder volumes and hence authentication to Ceph uses the Cinder keyring.

8. Complete a final check to ensure that Ceph and Nova are connected, by attaching a Nova volume using Horizon or the Nova CLI. After you attach the Nova volume, check the libvirt domain.

Verifying Nova Instance ID

From the management node, complete the following steps to verify the Nova instance ID of a guest VM having a cinder volume attached:

1. Load the OpenStack authentication variables:

```
[root@management-server-cisco installer]# source ~/openstack-configs/openrc
```

2. List the Nova instances:

```
[root@management-server-cisco images]# nova list
+--------------------------------------+------------+--------+--------
| ID                                                                    | Name                | Status
| Task
+--------------------------------------+------------+--------+--------
| 77ea3918-793b-4fa7-9961-10fbdc15c6e5 | cisco-vm         | ACTIVE | -
+--------------------------------------+------------+--------+-------
```

3. Show the Nova instance ID for one of the instances:

```
[root@management-server-cisco images]# nova show
77ea3918-793b-4fa7-9961-10fbdc15c6e5 | grep instance_name
| OS-EXT-SRV-ATTR:instance_name | instance-00000003
```

The Nova instance ID in this example is instance-00000003. This ID is used later with the virsh command. Nova instance IDs are actually the libvirt IDs of the libvirt domain associated with the Nova instance.

4. Identify the compute node where the VM is deployed:

```
[root@management-server-cisco images]# nova show 77ea3918-793b-4fa7-9961-10fbdc15c6e5 | grep
hypervisor
| OS-EXT-SRV-ATTR:hypervisor_hostname | compute_server-1
```

The compute node in this case is compute_server-1. Connect to this compute node to call the virsh commands.

Next, you can get the volume ID from the libvirt domain in the Nova libvirt container.

5. Launch a SSH session to the identified compute node, compute_server-1:

```
[root@management-server-cisco ~]# ssh root@compute_server-1
```

6. Navigate to the Nova libvirt container:

```
[root@compute_server-1 ~]# libvirt
```

7. Get the instance libvirt domain volume ID:

```
novalibvirt_4612 [root@compute_server-1 /]# virsh dumpxml instance-00000003 | grep rbd
<source protocol='rbd' name='volumes/volume-dd188a5d-f822-4769-8a57-c16694841a23'>
```

8. Launch a SSH session to a controller node:

```
[root@management-server-cisco ~]# ssh root@controller_server-1
```

9. Navigate to the Ceph monitor container:

```
[root@compute_server-1 ~]# cephmon
```

10. Verify whether the volume ID matches the ID in Step 7:

```
cephmon_4612 [ceph@controller_server-1 ceph]
$ rbd list volumes | grep volume-dd188a5d-f822-4769-8a57-c16694841a23
volume-dd188a5d-f822-4769-8a57-c16694841a23
```

Docker Disk Space Usage

Displaying Docker Disk Space Usage

Docker supports multiple storage backends such as Device Mapper, thin pool, overlay, and a Union File System (AUFS). Cisco VIM uses the devicemapper storage driver as it provides strong performance and thin provisioning. Device Mapper is a kernel-based framework that supports advanced volume management capability.

Complete the following steps to display the disk space used by Docker containers.

1. Launch a SSH session to a controller or compute node, for example:

```
[root@management-server-cisco ~]# ssh root@controller_server-1
```

2. Enter the *docker info* command to display the disk space used by Docker containers:

```
[root@controller_server_1 ~]# docker info
Containers: 24
Images: 186
Storage Driver: devicemapper
Pool Name: vg_var-docker--pool
Pool Blocksize: 524.3 kB
Backing Filesystem: xfs
Data file:
Metadata file:
Data Space Used: 17.51 GB
Data Space Total: 274.9 GB
Data Space Available: 257.4 GB...
```

Monitoring with CVIM-MON

Monitoring with CVIM-MON

Alerting Rules Customization

Alerting Rules Customization

Cisco VIM monitor is deployed with a set of built-in alerting rules that cover the most important error conditions that can occur in the pod. You can view the alerts from the Grafana user interface or alerting dashboard, or send them optionally to a number of supported receivers.
After deployment, the pod administrators can customize the alerting rules based on their requirements.

Managing Alerting Rules

The alerting rules define how alerts should be triggered based on conditional expressions on any available metric. For example, you can trigger an alert when any performance metric such as CPU usage, network throughput or disk usage reaches certain threshold.
You can add new alerting rules and modify or delete the pre-built existing alerting rules by following the below steps:

1. Create a proper custom alerting rules configuration file:
    a. Create a custom alerting rule configuration file named alerting_custom_rules.yml under the management node openstack-configs directory.
    b. Add the new rules, modified rules and deleted rules in that file using your favorite editor (see the file format below)
    c. Verify that the custom alerting rule file is valid using a provided tool.
2. Once validated, if needed, you can rename it and issue a standard reconfiguration using the ciscovim cli.

Alerting Rules Customization Workflow

Once the custom alerting rules file is validated, you must merge the two files such as default pre-existing alerting rules and custom alerting rules. Whenever a reconfigure operation with --alerting_rules_config option is performed, a merge tool starts with the default alerting rules as a base for all customizations. Any previous modifications are overwritten based on the current content of alerting_custom_rules.yml file. The merge tool output file consists of:

1. All rules from alerting_custom_rules.yml that do not belong to group change-rules or delete-rules.
2. Rules from default_alerting_rules.yml:
    - that do not duplicate from custom file rules.
    - that are not supposed to be deleted.
    - that can be modified based on change-rules input.

Custom Alerting Rule File Format

The *alerting_custom_rules.yml* file must follow the format defined in this section. This format is identical to the one used by the Prometheus configuration file, with a few additional semantic extensions to support deletion and modification of pre-built existing rules.

General Format

The group entry contains a list of groups identified by (group_name), where each group can include one or more rules. Use the labels to determine the severity and other snmp trap attributes.
Following are the limitations to set labels:

- severity, snmp_fault_code, and snmp_fault_severity must be set to one of the values specified in the example below.
- snmp_fault_source should indicate the metric used in the alert expression
- snmp_node must not be changed.
- snmp_podid must be same as the pod name specified insetup_data.yaml

```
groups:
- name: {group_name}
rules:
- alert: {alert_name}
annotations:
description: {alert_description}
summary: {alert_summary}
expr: {alert_expression}
for: {pending_time}
labels:
severity: {informational/warning/critical}
snmp_fault_code:
```

```
{other/resourceUsage/resourceThreshold/serviceFailure/hardwareFailure/networkConnectivity}
snmp_fault_severity: {emergency/critical/major/alert/informational}
snmp_fault_source: {fault_source}
snmp_node: '{{ $labels.instance }}'
snmp_podid: {pod_id}
```

Addition of Alerting Rules

Any alert rule specified under a group other than **change-rules** group or **delete-rules** group is populated to the merged output file. You can prioritize the custom rules over the pre-existing rules if there are two alerts with the same name in both the files, such that only the one from custom file is kept as a result of the merge.

Modification of Alerting Rules

You can modify any pre-existing rule using the following syntax:

```
groups:
- name: change-rules
rules:
- alert: {alert_name}
expr: {new_alert_expression}
annotations:
summary: {new_alert_summary}
```

The above merge script finds only the group named **change-rules** and modifies the expression and/or summary of the corresponding alert.
If the alert to be changed does not exist, it will not be created and no changes are performed.

Deletion of Alerting Rule

You can delete any built-in rule using the following construct:

```
groups:
        name: delete-rules
        rules:
        alert: {alert_name/regular_expression}
```

The above merge script finds only the group named **delete-rules** and deletes the pre-existing rules that match the alert name or regular expressions.

If the alert to be deleted does not exist, no changes are performed.

Example

The following custom configuration file includes examples of new alerting rule, modified alerting rule and deleted alerting rules:

```
groups:
- name: cpu
rules:
- alert: cpu_idle
annotations:
description: CPU idle usage is too high - resources under-utilized
summary: CPU idle too high
expr: cpu_usage_idle > 80
for: 5m
labels:
severity: informational
snmp_fault_code: resourceUsage
snmp_fault_severity: informational
snmp_fault_source: cpu_usage_idle
snmp_node: '{{ $labels.instance }}'
snmp_podid: pod7
- alert: cpu_iowait
annotations:
description: CPU iowait usage is too high
summary: CPU iowait too high
```

```
expr: cpu_usage_iowait > 10
for: 3m
labels:
severity: warning
snmp_fault_code: resourceUsage
snmp_fault_severity: alert
snmp_fault_source: cpu_usage_iowait
snmp_node: '{{ $labels.instance }}'
snmp_podid: pod7
- name: change-rules
rules:
- alert: disk_used_percent
expr: disk_used_percent > 99
annotations:
summary: Disk used > 99%
- alert: reboot
annotations:
summary: Server rebooted
- alert: system_n_users
expr: system_n_users > 10
- name: delete-rules
rules:
- alert: disk_filling_up_in_4h
- alert: mem.*
```

Validation Script

Validate any custom configuration file prior to reconfiguration, by executing the following CLI command from any location on the management node:

```
check_alerting_rules (no additional parameters are required)
```

The validation script uses the prometheus "promtool", but skips some of its checks to allow the modification and deletion of rules. It also checks if the provided SNMP severities and fault codes are supported. When no custom file is present, the expected location is mentioned in the output.

Ouput of validation script in case of success

```
check_alerting_rules
check_promtool.py: checking /prometheus/alerting_custom_rules.yml
check_promtool.py: success:
check_promtool.py: regular expressions for rules to be deleted: 2
check_promtool.py: rules to be changed: 3
check_promtool.py: rules to be added: 2
```

Output of validation script in case of failure

```
# check_alerting_rules
check_promtool.py: checking custom-rules.yml
check_promtool.py: failure:
check_promtool.py: group "new_group", rule 0, "new_alert": could not parse expression:
parse error at char 8:
could not parse remaining input "@$"...
check_promtool.py: group "new_group2", rule 0, "new_alert_3": could not parse expression:
parse error at char 7:
bad number or duration syntax: "1"
# check_alerting_rules
check_promtool.py: checking /prometheus/alerting_custom_rules.yml
check_promtool.py: failure:
check_promtool.py: line 36: field custom_field not found in type rulefmt.Rule
```

Alert Manager and Receiver Customization

Alert Manager and Receiver Customization

The alert manager component in Cisco VIM monitor controls the routing, grouping, and inhibiting alerts that are sent by the Prometheus alert rules engine to the appropriate receivers.
The default configuration in Cisco VIM monitor allows every alert to be forwarded as SNMP traps to the SNMP managers through SNMP agent if enabled in the Cisco VIM configuration file.
After deployment, you can add custom alert routes, alert grouping, alert inhibitions and receivers by following the below steps:

1. Create a proper custom alerting rules configuration file:
    a. Create a custom alert manager rule configuration file named alertmanager_custom_config.yml.
    b. Edit the content using your favorite editor (see format below).
    c. Copy that file to the management node openstack-configs directory
    d. Verify that the custom alerting rule file is valid using a provided tool.
2. Once the file is validated, if needed, you can either leave it in *openstack-configs* directory or move it to your preferred location. Then use a **ciscovim reconfigure** command with an additional parameter:

```
[root@mgmt1 ~]# ciscovim reconfigure --alertmanager_config <alertmanager_config_file>
```

Supported Receivers

The alert manager supports the following list of receivers:

- webhook
- pagerduty
- e-mail
- pushover
- wechat
- opsgenie
- victorops

Alert Manager Custom Configuration File Format

General Format
The following listing shows the general format of the alert manager configuration file. Most custom configuration files should only include a small subset of the available options.

```
global:
# ResolveTimeout is the time after which an alert is declared resolved # if it has not been
updated.
[ resolve_timeout: <duration> | default = 5m ]
# The default SMTP From header field. [ smtp_from: <tmpl_string> ]
# The default SMTP smarthost used for sending emails, including port number.
# Port number usually is 25, or 587 for SMTP over TLS (sometimes referred to as STARTTLS).
# Example: smtp.example.org:587 [ smtp_smarthost: <string> ]
# The default hostname to identify to the SMTP server. [ smtp_hello: <string> | default =
"localhost" ]
[ smtp_auth_username: <string> ]
# SMTP Auth using LOGIN and PLAIN. [ smtp_auth_password: <secret> ]
# SMTP Auth using PLAIN.
[ smtp_auth_identity: <string> ] # SMTP Auth using CRAM-MD5.
[ smtp_auth_secret: <secret> ]
# The default SMTP TLS requirement.
[ smtp_require_tls: <bool> | default = true ]
# The API URL to use for Slack notifications. [ slack_api_url: <secret> ]
[ victorops_api_key: <secret> ]
[ victorops_api_url: <string> | default =
"https://alert.victorops.com/integrations/generic/20131114/alert/" ]
[ pagerduty_url: <string> | default = "https://events.pagerduty.com/v2/enqueue" ] [
opsgenie_api_key: <secret> ]
[ opsgenie_api_url: <string> | default = "https://api.opsgenie.com/" ] [ hipchat_api_url:
<string> | default = "https://api.hipchat.com/" ] [ hipchat_auth_token: <secret> ]
```

```
[ wechat_api_url: <string> | default = "https://qyapi.weixin.qq.com/cgi-bin/" ] [
wechat_api_secret: <secret> ]
[ wechat_api_corp_id: <string> ]

# The default HTTP client configuration [ http_config: <http_config> ]
# Files from which custom notification template definitions are read.
# The last component may use a wildcard matcher, e.g. 'templates/*.tmpl'. templates:
[ - <filepath> ... ]
# The root node of the routing tree. route: <route>
# A list of notification receivers. receivers:
- <receiver> ...
# A list of inhibition rules. inhibit_rules:
[ - <inhibit_rule> ... ]
```

The custom configuration must be a full working configuration file with the following template. It should contain three main keys (global, route, receiver).

The global configuration must have at least one attribute, for example, resolve_timeout = 5m. Ensure that all new receivers must be part of the route so the alerts can be routed to the proper receivers. The receiver name cannot be snmp.

You can find the configuration details for creating route/receiver in the Prometheus Alert Manager documentation (publicly available online).

```
global: resolve_timeout: 5m
route: <route>
receivers:
- <receiver> ...
The following is a custom config to add a webhook receiver.
global:
resolve_timeout: 5m
route:
group_by: ['alertname', 'cluster', 'service']
group_wait: 30s
group_interval: 5m
repeat_interval: 8737h
receiver: receiver-webhook
receivers:
- name: 'receiver-webhook'
webhook_configs:
- send_resolved: true
url: 'http://webhook-example:####/xxxx/xxx'
```

Default Built-in Configuration File

Two different default configuration files are available to define the following in order:

1. Generic route for all alerts to the SNMP agent running on the management node.
2. Route to a generic receiver that can be customized to add a channel of notification (webhook, slack and others).

Default Configuration file with SNMP enabled

```
:
global:
resolve_timeout: 5m
route:
group_by: ['alertname', 'cluster', 'service']
group_wait: 30s
group_interval: 5m
repeat_interval: 8737h
# A default receiver
receiver: snmp
receivers:
- name: 'snmp'
webhook_configs:
- send_resolved: true
url: 'http://localhost:1161/alarms'
```

Default configuration file with SNMP disabled

```
route:
receiver: recv
group_by:
- alertname
- cluster
- service
group_wait: 30s
group_interval: 5m
repeat_interval: 8737h
receivers:
- name: recv
```

SNMP Trap Receivers

You can send the SNMP traps to SNMP managers enabled in the Cisco VIM configuration file setup_data.yaml.

Example: inhibit (mute) alerts matching a set of labels

Inhibit alerts is a tool that prevents certain alerts to be trigged if other alert/alerts is/are trigged. If one alert having the target attribute matches with the another alert having source attribute, this tool inhibits the alert with target attribute.
This is the general format for inhibit alerts. You can set a regex to match both the source and target alerts and to filter the alerts per label name.

```
# Matchers that have to be fulfilled in the alerts to be muted.
target_match:
[ <labelname>: <labelvalue>, ... ]
target_match_re:
[ <labelname>: <regex>, ... ]
# Matchers for which one or more alerts have to exist for the
# inhibition to take effect.
source_match:
[ <labelname>: <labelvalue>, ... ]
source_match_re:
[ <labelname>: <regex>, ... ]
# Labels that must have an equal value in the source and target
# alert for the inhibition to take effect.
[ equal: '[' <labelname>, ... ']' ]
```

Example: Inhibit alerts if other alerts are active

The following is an example of inhibit rule that inhibits all the warning alerts that are already critical.

```
inhibit_rules:
- source_match:
severity: 'critical'
target_match:
severity: 'warning'
# Apply inhibition if the alertname is the same.
equal: ['alertname', 'cluster', 'service']
```

This is an example of inhibit all alerts docker_container in containers that are down (alert docker_container_down).

```
inhibit_rules:
- target_match_re:
alertname: 'docker_container.+'
source_match:
alertname: 'docker_container_down'
equal: ['job', 'instance']
```

Validation Script

When a new configuration is set, execute the check_alertmanager_config from anywhere in the management node and ensure that you get a **SUCCESS** in the output from the configuration POV.

```
> check_alertmanager_config
Checking '/var/lib/cvim_mon/alertmanager_custom_config.yml' SUCCESS
```

```
Found:
- global config
- route
- 0 inhibit rules
- 1 receivers
- 0 templates
```

Silencing Alerts

Silencing Alerts

Silences

During administrative pod operations, it is sometimes necessary to temporarily disable alerting as these operations can trigger alerts. The alerts caused by these operations can be silenced to avoid unnecessary escalation in applications that receive and handle alerts.

CVIM-MON provides the ability to silence alerts based on arbitrary filters on the alert labels by creating silences. A silence is a filter programmed in the alert manager component with the following attributes:

- start: indicates when the silence starts to be active
- end: indicates when the silence is no longer active
- duration: an alternate way to specify the duration of the silence (might be easier than programming an end date)
- matchers: a list of one or more filters on alert labels. Each matcher has a label name, a label value, and a regex flag which indicates whether the label value is a regular expression or an exact match.
- creator: arbitrary text identifying the silence creator
- comment: arbitrary text describing the purpose of the silence

When a silence is active, any alert that matches the filters are effectively silenced such that:

- these alerts should not be counted in the Grafana UI alert counters
- they should not be visible in the Grafana UI alert table
- no receiver should receive these alerts (SNMP traps, webhooks)

The administrator can create as many silences as required, list silences, expire them, or delete them using two different interfaces: web UI or REST API.

Credentials and Certificates

The username and password can be:

- *admin* and the static auto-generated password available on the management node in the *openstack-configs/secrets.yaml* with the property name CVIM_MON_SERVER_PASSWORD
- LDAP user credentials associated to the Prometheus/Alertmanager role

In the case of HTTP access, a certificate file is required to certify that you are connecting to the right server.
Depending on the way you generate and manage the certificates, you may or may not need to do anything specific to use the right certificate.
If you use self-signed certificates, you need to download it on the server that will connect to the alert manager.
You can download the self-signed certificates from the target management node at the following location:

```
/var/www/mercury/mercury.crt
```

Managing Silences Using Web UI

Point your browser to the CVIM-MON Alert Manager UI which is available at the following URL:

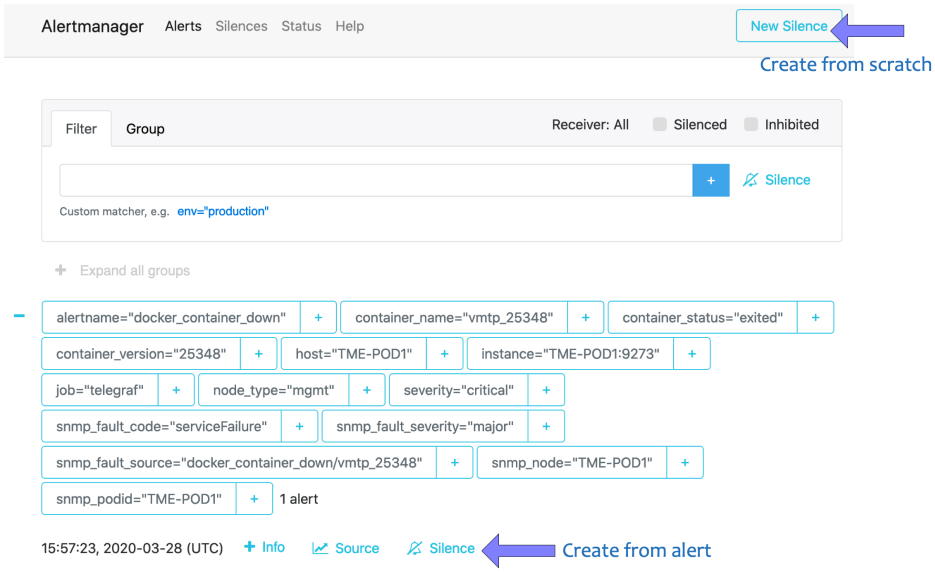
```
https://<mgmt_node_ip>:9093
```

The username is *admin* and the password is the same password as for accessing the Prometheus service.

The landing page shows the list of all standing alerts.

Create a Silence

1. To create a new silence, click **New Silence** on the top right corner of the dashboard or click on **Silence** on the **Filter** pane for the existing standing alert. The **Silence Create** page is displayed.

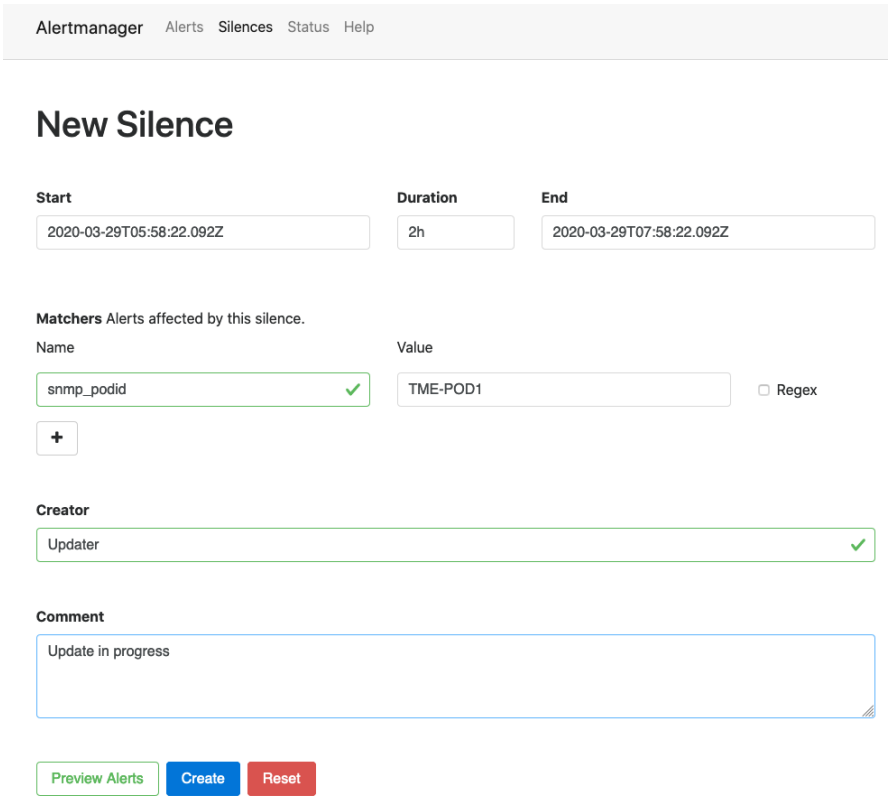


2. Enter the mandatory fields such as start time, duration or end time.
3. Edit the filters if it is created from an alert (mostly removing unneeded filters) or add the necessary filters, a creator and comment, and then click **C reate**.
4. You can view, edit, or set expiry for the silences from the **Silences** tab.

Example: Silencing all alerts from the current pod

To silence all alerts from the local pod preceding a software upgrade, for example, you can define a silence with just one filter which matches on the label *s nmp_podid* and set the value to the local pod name, where the pod name is defined in the *openstack-configs/setup_data.yaml*. You can set the duration to any arbitrary value or a high value and expire the silence later at the right time.

Example of silence for the pod named TME_POD1:



View, Edit, or Expire a Silence

You can view, edit, reactivate or set expiry for silences from the **Silences** tab.

Each selected silence shows the count and list of affected alerts.

Managing Silences using REST API

The alert manager service can also handle silence operations using the REST API. This interface allows easier implementation of any alert silencing policy through script.

The HTTP requests must be sent from an external server with the appropriate credentials and certificates.

Create a Silence Using HTTP

To create an alert silence, send an HTTP POST request with the following URL:

```
https://<mgmt_node_ip>:9093/api/v2/silences
```

The body of the POST request is a JSON string with the following content:

```
{
   "comment": <silence description>,
   "createdBy": <silence creator>,
   "startsAt": <date_time>,
   "endsAt":   <date_time>,
   "matchers": [{"isRegex": <true|false>,"name": <label name>,"value": <label value>},
                {"isRegex": <true|false>,"name": <label name>,"value": <label value>},
                ...]
}
```

The *startsAT* and *endsAT <date_time>* values must comply to RFC-3339 (Date and Time on the Internet: Timestamps).

For example "`2019-07-20T18:01:30.00Z`" represents July 20, 2019 1:30am in UTC.
The label name must correspond to a label associated to the alert that needs to be silenced.
The *isRegex* field indicates whether a regular expression is used in the label value.
You can provide as many matchers as needed, but the alerts that are silenced must match all matchers (that is, they are AND not OR).

Each silence is uniquely identified by its silence ID, which is a UUID assigned by the alert manager and returned by the POST operation.

Example of curl request to create a silence that disables all alerts from the pod TME-POD1 and have a critical severity:

```
$ curl -sS -H "Content-Type: application/json" -u admin:8EavKsAK4IdHZrnO --cacert ./certificates.crt
https://172.23.105.218:9093/api/v2/silences -X POST -d '{"comment": "test sample silence","createdBy":
"tester","startsAt": "2019-07-20T18:00:00.00000000Z", "endsAt": "2019-07-20T18:00:59.46418637Z","matchers":
[{"isRegex": false,"name": "snmp_podid","value": "TNE-POD1"},{"isRegex": false,"name": "severity","value":
"critical"}]}'


{"silenceID":"6ae6e8c5-9de8-44c1-8cd7-2e3da825a786"}
$
```

Retrieve Silences

You can retrieve silences using an HTTP GET operation.

Example of silence retrieval

```
$ curl -sS -u admin:8EavKsAK4IdHZrnO --cacert ./certificates.crt https://172.23.105.218:9093/api/v2/silences |
python -m json.tool
[
    {
        "comment": "test",
        "createdBy": "devops",
        "endsAt": "2019-06-09T17:45:40.814Z",
        "id": "95ba1628-4d24-462b-9a68-a325980f8ef7",
        "matchers": [
            {
                "isRegex": false,
```

```
                "name": "alertname",
                "value": "diskmon_physical_drive_state"
            },
            {
                "isRegex": false,
                "name": "snmp_podid",
                "value": "bn-champagne"
            }
        ],
        "startsAt": "2019-06-09T15:46:09.350Z",
        "status": {
            "state": "active"
        },
        "updatedAt": "2019-06-09T15:46:09.350Z"
    }
]
```

You can also retrieve a silence from its silence ID by appending the ID to the URL:

```
https://<mgmt_nod_ip>:9093/api/v2/silence/<silence_ID>
```

Example of silence retrieval from its ID

```
$ curl -sS -u admin:8EavKsAK4IdHZrnO --cacert ./certificates.crt https://172.23.105.218:9093/api/v2/silence
/95ba1628-4d24-462b-9a68-a325980f8ef7 | python -m json.tool
{
    "comment": "test",
    "createdBy": "devops",
    "endsAt": "2019-06-09T17:45:40.814Z",
    "id": "95ba1628-4d24-462b-9a68-a325980f8ef7",
    "matchers": [
        {
            "isRegex": false,
            "name": "alertname",
            "value": "diskmon_physical_drive_state"
        },
        {
            "isRegex": false,
            "name": "check",
(---SNIP---)
```

Delete a Silence

To delete a silence, use the delete HTTP request on the following URL:

```
https://<mgmt_nod_ip>:9093/api/v2/silence/<silence_ID>
```

Example of silence deletion using curl

```
$ curl -sS -u admin:8EavKsAK4IdHZrnO --cacert ./certificates.crt -X DELETE https://172.23.105.218:9093/api/v2
/silence/95ba1628-4d24-462b-9a68-a325980f8ef7
```

Day 2 Operations of UM

Day 2 Operations of Cisco VIM Unified Management

Shutting Down UM

Shutting Down Cisco VIM Unified Management

To stop the Cisco VIM Unified Management Container services, shut down Cisco UCS VIM Unified Management by running the *systemctl stop service* command.

1. Log into a server in which the Unified Management container is running.
2. Stop the Unified Management service by running the following command from the shell window:

```
systemctl stop docker-insight
```

   a. Check the status of Unified Management Container by running the following command: *docker ps -a* | *grep* insight.

```
STATUS
Up 6 seconds
```

   b. Check the status of the service by running the following command:

```
systemctl staus docker-insight
```

   The following information is displayed:

```
Docker-insight.service - Insight Docker Service
Loaded: loaded (/usr/lib/systemd/system/docker-insight.service; enabled; vendor preset: disabled)
Active: inactive (dead) since <Date and Time since it was last active>
```

Restarting UM

Restarting Cisco VIM Unified Management

1. Log into the server in which the Unified Management container is stopped.
2. Restart the Unified Management service by running the following command from the shell window:

```
systemctl restart docker-insight
```

   a. Check the status of Unified Management container by running the following command: *docker ps -a* | *grep* insight.

```
STATUS
 Up 6 seconds
```

   b. Check the status of the service by running the following command:

```
systemctl status docker-insight
```

   The following output is displayed:

```
Docker-insight.service - Insight Docker Service
Loaded: loaded (/usr/lib/systemd/system/docker-insight.service; enabled; vendor preset: disabled)
Active: active (running) since <Date and Time when it got active.
```

Reconfiguring UM

Reconfiguring VIM Unified Management

UM reconfigure action provides you with three major functionalities:

1. Reconfigure Unified Management TLS certificate.
2. Switch from self-signed TLS certificate to third-party TLS certificate.
3. Reconfigure Unified Management MySQL database password.

> ⚠ UM reconfiguration is not allowed after an update, as the update is an intermediate stage between rollback and commit.

Reconfiguring Unified Management TLS Certificate

As the UM web-service is protected by TLS, reconfigure action provides flexibility to change the existing TLS certificate. As there were two approaches to configure it, there are two approaches to change it.

Reconfiguring Third-party TLS Certificate

If you had provided your own TLS certificate before Insight installation through PEM_PATH key in *insight_setup_data.yaml,* perform the following steps to reconfigure it.

1. Fetch the latest *insight_setup_data.yaml* file

   a. For releases prior to Cisco VIM 3.4.5, execute the below commands:

   ```
   # cd /root/
   # mkdir MyDir
   # cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
   ```

   b. For Cisco VIM 3.4.5, enter the below commands:

   ```
   # cd /root/
   # mkdir MyDir
   # cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
   ```

2. Edit the *insight_setup_data.yaml* to change the value of PEM_PATH and/or SSL_CERT_CHAIN_FILE key to point to the path of your new valid TLS/cert chain file certificate. Then, save the file.
   For example:

   ```
   PEM_PATH: "/root/new_tls.pem"
   SSL_CERT_CHAIN_FILE: "/root/new_ssl.crt"
   ```

3. Start reconfiguration:

   a. For releases prior to Cisco VIM 3.4.5:

   ```
   # cd <insight_ws>
   # ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
   VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
   Perform the action. Continue (Y/N)y
   Management node validation!
   ```

```
+------------------------------+--------+-------+
| Rule                                                | Status | Error |
+------------------------------+--------+-------+
| Check Kernel Version                          | PASS          | None  |
| Check Docker Version                          | PASS          | None  |
| Check Management Node Tag                | PASS   | None  |
| Check Bond Intf. Settings                | PASS          | None  |
| Root Password Check                           | PASS          | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings        | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition            | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition                          | PASS          | None  |
| Check LVM partition                           | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+------------------------------+--------+-------+
Insight standalone input validation!
+-----------------------------------------+--------+-------+
| Rule                                                                          | Status |
Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation                | PASS          | None  |
| Valid key check in Insight setup data         | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check     | PASS   | None  |
| Check registry connectivity                                 | PASS   | None  |
| Check Email server for Insight                    | PASS   | None  |
+-----------------------------------------+--------+-------+
WARNING!! reconfigure will have few secs of Outage for Insight!
Cisco VIM Insight Already Exists!
+----------------------+--------+-------------------------------------------------------------+
| Description                        | Status |
Details
|
+----------------------+--------+-------------------------------------------------------------+
| VIM Insight UI URL         | PASS          | https://<br_api:
9000>                                                          |
| VIM UI Admin Email ID | PASS          | Check for info @: <abs path of insight_setup_data.yaml> |
|                                                |
|
|
| VIM UI Admin Password | PASS          | Check for info @ /opt/cisco/insight/secrets.
yaml                  |
| VIM Insight Workspace | PASS   | /root
/<insight_ws>                                                                  |
+----------------------+--------+-------------------------------------------------------------+
Cisco VIM Insight backup Info!
+----------------------+--------+-------------------------------------------------------------------+
| Description                    | Status |
Details
|
+----------------------+--------+-------------------------------------------------------------------+
| Insight backup Status | PASS   | Backup done
@                                                                                                  |
|                                                 |                | /var/cisco/insight_backup
/backup-<release_tag>-<date_time>         |
+----------------------+--------+-------------------------------------------------------------------+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
As the summary table describes Insight gets autobacked up after reconfigure at /var/cisco
/insight_backup
to preserve the latest state of Insight.
```

b. For Cisco VIM 3.4.5, enter the following commands:

```
# cd Insight-<tag_id>

$ ./insight/insight_runner.py --reconfigure -f </root/insight_setup_data.yaml>
```

```
Perform the action. Continue (Y/N)y

The logs for this run are available at /var/log/insight/bootstrap/<date>_<time>

                 ##############################
                  CISCO INSIGHT ORCHESTRATOR
                 ##############################

[1/2][INPUT_VALIDATION: INIT]                                                [   \   ]    0min
1sec


Management Node validation!
+-------------------------------+--------+------+
| Rule                          | Status | Error|
+-------------------------------+--------+------+
| Check Kernel Version          | PASS   | None |
| Check Ansible Version         | PASS   | None |
| Check Docker Version          | PASS   | None |
| Check Management Node Tag     | PASS   | None |
| Check Bond Intf. Settings     | PASS   | None |
| Root Password Check           | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings        | PASS   | None |
| Check Docker Pool Settings    | PASS   | None |
| Check Home Dir Partition      | PASS   | None |
| Check Root Dir Partition      | PASS   | None |
| Check /var Partition          | PASS   | None |
| Check LVM partition           | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+-------------------------------+--------+------+

Insight standalone Input validation!
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone Schema Validation    | PASS   | None  |
| Valid Key Check in Insight Setup Data   | PASS   | None  |
| Duplicate Key Check In Insight Setup Data | PASS   | None  |
| CVIM/Insight Workspace Conflict Check   | PASS   | None  |
| Check Registry Connectivity             | PASS   | None  |
| Check LDAP Connectivity                 | PASS   | None  |
| Test Email Server for Insight           | PASS   | None  |
+-----------------------------------------+--------+-------+
.
.

[2/2][BOOTSTRAP_INFRA: vim-admins-Restart and enable sss daemon]             [ DONE! ]    1min
23secs

.
.

Cisco VIM Insight already Installed!
+------------------+--------+-------------------------------------------------------+
| Description      | Status | Details                                               |
+------------------+--------+-------------------------------------------------------+
| Insight UI URL   | PASS   | https://<br_api>:9000                                 |
| UI Admin Email ID | PASS   | Check for info @: /root/insight-openstack-            |
|                  |        | configs/insight_setup_data.yaml                       |
| UI Admin Password | PASS   | Check for info @: /opt/cisco/insight/secrets.yaml     |
+------------------+--------+-------------------------------------------------------+

Backup Validation Passed
[***][AUTOBACKUP: Completed Step 1 of backup, backupdir:... /var/cisco/insight_backup
/insight_autobackup_3.4.5_<date>_<time>]
[***][AUTOBACKUP: Starting post-backup..please wait!!]
[***][AUTOBACKUP: Completed Cisco UM backup ... /var/cisco/insight_backup/insight_autobackup_3.4.5
_<date>_<time>
```

```
Ended Installation [BOOTSTRAP_INFRA] [Success]

The logs for this run are available at /var/log/insight/bootstrap/<date>_<time>


As the summary table describes Insight gets autobacked up after reconfigure at /var/cisco
/insight_backup to preserve the latest state of Insight.
```

Reconfiguring Self-signed TLS Certificate

If you have created a new TLS Certificate through *tls_insight_cert_gen.py* before UM installation, follow the steps to reconfigure it.

1. Fetch the latest *insight_setup_data.yaml* file
   a. For releases prior to Cisco VIM 3.4.5, run the following commands:

   ```
   # cd /root/
   # mkdir MyDir
   # cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
   ```

   b. For Cisco VIM 3.4.5, enter the below commands:

   ```
   # cd /root/
   # mkdir MyDir
   # cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
   ```

2. Run the following commands to reconfigure the self-signed TLS certificate:

```
# cd Insight-<tag_id>/insight
# ./tls_insight_cert_gen.py -h
usage: tls_insight_cert_gen.py [-h] [--overwrite] --file INSIGHTSETUPDATA

TLS cert generator Insight

optional arguments:
  -h, --help            show this help message and exit
  --overwrite, -o       Overwrite Insight certificates if already present in openstack config directory
  --file INSIGHTSETUPDATA, -f INSIGHTSETUPDATA
                        Location of insight_setup_data.yaml


# ./tls_insight_cert_gen.py -f <path insight_setup_data.yaml> --overwrite
This will overwrite the existing TLS certificate.
Management node validation
+---------------------------------+-------+-------+
| Rule                                                |Status | Error |
+---------------------------------+-------+-------+
| Check Kernel Version            | PASS  | None  |
| Check Ansible Version                   | PASS  | None  |
| Check Docker Version                            | PASS  | None  |
| Check Management Node Tag                   | PASS  | None  |
| Check Bond Intf. Settings           | PASS  | None  |
| Root Password Check                         | PASS  | None  |
| Check Boot Partition Settings          | PASS  | None  |
| Check LV Swap Settings                    | PASS  | None  |
| Check Docker Pool Settings           | PASS  | None  |
| Check Home Dir Partition                  | PASS  | None  |
| Check Root Dir Partition                   | PASS  | None  |
| Check /var Partition                          | PASS  | None  |
| Check LVM partition                         | PASS  | None  |
| Check RHEL Pkgs Install State   | PASS  | None  |
+---------------------------------+-------+-------+
Insight standalone input validation
+-----------------------------------------+--------+-------+
| Rule                                                                  | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation               | PASS   | None  |
```

```
| Valid key check in Insight setup data            | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check     | PASS   | None  |
| Check registry connectivity               | PASS   | None  |
| Check Email server for Insight            | PASS   | None  |
+-------------------------------------------+--------+-------+
Generating a 4096 bit RSA private key
.....................................................................................++
.......++
writing new private key to '../openstack-configs/insight.key'
```

3. Start reconfiguration:

   a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

```
# ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Perform the action. Continue (Y/N)y
Management node validations
+------------------------------+--------+-------+
| Rule                                          | Status | Error |
+------------------------------+--------+-------+
| Check Kernel Version                          | PASS           | None  |
| Check Ansible Version                         | PASS   | None  |
| Check Docker Version                          | PASS           | None  |
| Check Management Node Tag          | PASS   | None  |
| Check Bond Intf. Settings     | PASS   | None  |
| Root Password Check                       | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings                | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition      | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition          | PASS   | None  |
| Check LVM partition           | PASS   | None  |
| Check RHEL Pkgs Install state | PASS   | None  |
+-------------------------------+--------+-------+
Insight standalone input validation
+-------------------------------------------+--------+-------+
| Rule                                                                                | Status | Error
|
+-------------------------------------------+--------+-------+
| Insight standalone schema validation      | PASS   | None  |
| Valid key check in Insight setup data     | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check     | PASS   | None  |
| Check registry connectivity               | PASS   | None  |
| Check Email server for Insight            | PASS   | None  |
+-------------------------------------------+--------+-------+
WARNING!! Reconfiguration will have few secs of outage for Insight
Cisco VIM Insight Already Exists!
+----------------------+--------+-------------------------------------------------------------+
| Description          | Status |
Details
|
+----------------------+--------+-------------------------------------------------------------+
| VIM Insight UI URL        | PASS   | https://<br_api:
9000>                                                          |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml> |
|                       |        |                                                             |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml        |
| VIM Insight Workspace | PASS   | /root/<insight_ws>                                      |
+----------------------+--------+-------------------------------------------------------------+
Cisco VIM Insight backup Info!
+----------------------+--------+-------------------------------------------------------------------------
+
| Description          | Status | Details
|
+----------------------+--------+-------------------------------------------------------------------------
```

```
+
| Insight backup Status | PASS   | Backup done @
|                             |        /var/cisco/insight_backup
/insight_backup_<release_tag>_<date_time>|
|
+---------------------+-------+-------------------------------------------------------------------------
+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
Insight gets autobacked up after reconfiguration at /var/cisco/insight_backup, to preserve the
latest
state of Insight.
```

b. For Cisco VIM 3.4.5, enter the following command:

```
# cd Insight-<tag_id>
$ ./insight/insight_runner.py --reconfigure -f </root/insight_setup_data.yaml>
```

Switch from Self-signed TLS Certificate to Third-party TLS Certificate

If you have created a new TLS certificate through *tls_insight_cert_gen.py* before Insight Installation and wanted to switch to your own TLS certificate, perform the following steps.

> ⚠ You cannot switch from third-party TLS certificate to self-signed TLS certificate.

1. Fetch the latest *insight_setup_data.yaml* file

   a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

   ```
   # cd /root/
   # mkdir MyDir
   # cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
   ```

   b. For Cisco VIM 3.4.5:

   ```
   # cd /root/
   # mkdir MyDir
   # cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
   ```

2. Edit the *insight_setup_data.yaml* to add PEM_PATH and SSL_CERT_CHAIN_FILE key to point to path of your new valid TLS and SSL_CERT_CHAIN certificate. Save the file after editing.

   For example:

   ```
   PEM_PATH: "/root/new_tls.pem"
   SSL_CERT_CHAIN_FILE: "/root/new_ssl.crt"
   ```

3. Start reconfiguration:

   a. For releases prior to Cisco VIM 3.4.5, run the following commands:

   ```
   # cd <insight_ws>
   # ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
   VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
   Perform the action. Continue (Y/N)y
   Management node validation
   +-------------------------------+--------+-------+
   | Rule                                                  | Status | Error |
   +-------------------------------+--------+-------+
   | Check Kernel Version                        | PASS          | None  |
   | Check Ansible Version                       | PASS   | None  |
   | Check Docker Version                        | PASS          | None  |
   ```

```
| Check Management Node Tag         | PASS         | None  |
| Check Bond Intf. Settings         | PASS         | None  |
| Root Password Check                         | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings                | PASS         | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition                | PASS   | None  |
| Check Root Dir Partition                | PASS          | None  |
| Check /var Partition                        | PASS   | None  |
| Check LVM partition                     | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+-------------------------------+--------+-------
Insight standalone input validation
+-----------------------------------------+--------+-------+
| Rule                                                                                  | Status |
Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation                | PASS          | None  |
| Valid key check in Insight setup data         | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check         | PASS   | None  |
| Check registry connectivity                               | PASS   | None  |
| Check Email server for Insight                      | PASS   | None  |
+-----------------------------------------+--------+-------+
WARNING!! Reconfiguration will have few secs of outage for Insight!
Cisco VIM Insight Already Exists!
+----------------------+--------+-------------------------------------------------------------+
| Description          | Status | Details                                                     |
+----------------------+--------+-------------------------------------------------------------+
| VIM Insight UI URL    | PASS   | https://<br_api:9000>                                       |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml> |
|                       |        |                                                             |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml        |
| VIM Insight Workspace | PASS   | /root/<insight_ws>                                          |
+----------------------+--------+-------------------------------------------------------------+
Cisco VIM Insight backup Info!
+---------------------+-------+-------------------------------------------------------------------------
+
| Description          | Status| Details
|
+---------------------+-------+-------------------------------------------------------------------------
+
| Insight backup Status| PASS  | Backup done @
|
|                             | /var/cisco/insight_backup
/insight_backup_<release_tag>_<date_time>|
+---------------------+-------+-------------------------------------------------------------------------
+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
Insight gets autobacked up after reconfiguration at /var/cisco/insight_backup to preserve the
latest state of Insight
```

b. For Cisco VIM 3.4.5, run the below commands:

```
# cd Insight-<tag_id>
$ ./insight/insight_runner.py --reconfigure -f </root/insight_setup_data.yaml>
```

Reconfiguring Unified Management MySQL Database Password

You can use one of the below methods to reconfigure the MySQL DB password:

1. System generated Unified Management DB password.
2. User supplied Unified Management DB password.

System-generated Unified Management DB Password

Following are the steps to generate MySQL Unified Management DB password:

1. Fetch the latest *insight_setup_data.yaml* file. For releases prior to Cisco VIM 3.4.5, use the following command:

```
# cd /root/
# mkdir MyDir
# cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
```

2. To generate the Unified Management DB Password:

   a. For releases prior to Cisco VIM 3.4.5, run the following commands:

```
# cd <insight_ws>
# ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml> --regenerate_secrets

VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Perform the action. Continue (Y/N)y
Management node validation
+-------------------------------+--------+-------+
| Rule                                                | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None  |
| Check Docker Version          | PASS   | None  |
| Check Management Node Tag     | PASS   | None  |
| Check Bond Intf. Settings     | PASS   | None  |
| Root Password Check           | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings        | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition      | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition          | PASS   | None  |
| Check LVM partition           | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+-------------------------------+--------+-------+

Insight standalone input validation
+-----------------------------------------+--------+-------+
| Rule                                                                                | Status |
Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation      | PASS   | None  |
| Valid key check in Insight setup data     | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check     | PASS   | None  |
| Check registry connectivity               | PASS   | None  |
| Check Email server for Insight            | PASS   | None  |
+-----------------------------------------+--------+-------+

WARNING!! reconfiguration will have few secs of Outage for Insight!
Cisco VIM Insight Already Exists!
+----------------------+--------+-------------------------------------------------------------+
| Description                     | Status |
Details
|
+----------------------+--------+-------------------------------------------------------------+
| VIM Insight UI URL    | PASS   | https://<br_api:9000>                                       |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml>     |
|                       |        |                                                             |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml            |
| VIM Insight Workspace | PASS   | /root/<insight_ws>                                          |
+----------------------+--------+-------------------------------------------------------------+

Cisco VIM Insight backup Info!
+----------------------+--------+-------------------------------------------------------------+
| Description          | Status | Details                                                     |
+----------------------+--------+-------------------------------------------------------------+
| Insight backup Status | PASS   | Backup done @                                               |
|                       |        | /var/cisco/insight_backup/backup-<release_tag>-<date_time>  |
```

```
+----------------------+--------+-------------------------------------------------------------------+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
As the summary table describes Insight gets autobacked up after reconfigure at /var/cisco
/insight_backup to preserve the latest state of Insight.
```

b. For Cisco VIM 3.4.5, enter the below commands:

```
# cd Insight-<tag_id>
$ ./insight/insight_runner.py --reconfigure --regenerate_secrets
```

3. Verify the password change by running the following command:

```
# cat /opt/cisco/insight/secrets.yaml
DB_ROOT_PASSWORD: <new_db_password>
```

User-supplied Unified Management DB Password

1. Fetch the latest *insight_setup_data.yaml* file. For releases prior to 3.4.5, use the below commands:

```
# cd /root/
# mkdir MyDir
# cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
```

2. To provide your own MYSQL DB password:

   a. For releases prior to Cisco VIM 3.4.5, follow the below steps:

   ⚠ Your new DB password must contain alphanumeric characters with a length of at least eight characters.

```
# cd <insight_ws>
# ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml> --setpassword
VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Perform the action. Continue (Y/N)y
Password for DB_ROOT_PASSWORD: <enter_valid_db_password>
Management node validation
+-------------------------------+--------+-------+
| Rule                          | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None  |
| Check Ansible Version         | PASS   | None  |
| Check Docker Version          | PASS   | None  |
| Check Management Node Tag     | PASS   | None  |
| Check Bond Intf. Settings     | PASS   | None  |
| Root Password Check           | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings        | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition      | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition          | PASS   | None  |
| Check LVM partition           | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+-------------------------------+--------+-------+
Insight standalone input validation
+----------------------------------------+--------+-------+
| Rule                                   | Status | Error |
+----------------------------------------+--------+-------+
| Insight standalone schema validation   | PASS   | None  |
| Valid key check in Insight setup data  | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check  | PASS   | None  |
```

```
| Check registry connectivity               | PASS   | None  |
| Check Email server for Insight            | PASS   | None  |
+-------------------------------------------+--------+-------+
WARNING!!Reconfiguration will have few secs of Outage for Insight!
Cisco VIM Insight Already Exists!
+----------------------+--------+-----------------------------------------------------------+
| Description                        | Status |
Details
|
+----------------------+--------+-----------------------------------------------------------+
| VIM Insight UI URL    | PASS   | https://<br_api:9000>                                     |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml> |
|                       |        |                                                           |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml          |
| VIM Insight Workspace | PASS   | /root/<insight_ws>                                        |
+----------------------+--------+-----------------------------------------------------------+
Cisco VIM Insight backup Info!
+----------------------+-------+-------------------------------------------------------------------------
+
| Description          | Status| Details
|
+----------------------+-------+-------------------------------------------------------------------------
+
| Insight backup Status| PASS  | Backup done
@
|
|                      |
|
| | /var/cisco/insight_backup/insight_backup_<release_tag>_<date_time>
|
+----------------------+-------+-------------------------------------------------------------------------
+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
As the summary table describes Insight gets autobacked up after reconfigure at /var/cisco
/insight_backup
to preserve the latest state of Insight.
```

b. For Cisco VIM 3.4.5, run the below commands:

```
# cd Insight-<tag_id>
$ ./insight/insight_runner.py --reconfigure --setpassword
```

The password must satisfy at least three of the following without a blank space. Also, the length of the password must be in the range of 8 to 16.
   a. at least a letter between a to z
   b. at least a letter between A to Z
   c. at least a number between 0 to 9
   d. at least a character from !@-_+=

3. Verify the password change by running the following command:

```
#cat /opt/cisco/insight/secrets.yaml
DB_ROOT_PASSWORD: <new_db_password>
```

Reconfiguring Unified Management SMTP Server

UM requires a valid SMTP Server to send mails to Pod-Admin, UI-Admin, and regular users. If SMTP server is down, you can reconfigure it. Following values can be reconfigured:

- INSIGHT_SMTP_SERVER
- INSIGHT_EMAIL_ALIAS_PASSWORD (only needed for Authenticated SMTP server)
- INSIGHT_EMAIL_ALIAS
- INSIGHT_SMTP_PORT (optional, defaults to 25)

1. Fetch the latest *insight_setup_data.yaml* file

a. For Releases prior to 3.4.5:

```
# cd /root/
# mkdir MyDir
# cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
```

b. For Release 3.4.5:

```
# cd /root/
# mkdir MyDir
# cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
```

2. Edit the *insight_setup_data.yaml* to add the desired values. Save the file after editing.
3. Start reconfiguration:

a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

```
# cd <insight_ws>
# ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Perform the action. Continue (Y/N)y
Management node validation
+-------------------------------+--------+-------+
| Rule                          | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None  |
| Check Ansible Version         | PASS   | None  |
| Check Docker Version          | PASS   | None  |
| Check Management Node Tag     | PASS   | None  |
| Check Bond Intf. Settings     | PASS   | None  |
| Root Password Check           | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings        | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition      | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition          | PASS   | None  |
| Check LVM partition           | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+-------------------------------+------- -+-------+

Insight standalone input validation
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation    | PASS   | None  |
| Valid key check in Insight setup data   | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check   | PASS   | None  |
| Check registry connectivity             | PASS   | None  |
| Check Email server for Insight          | PASS   | None  |
+-----------------------------------------+--------+-------+

WARNING!! Reconfiguration will have few secs of Outage for Insight!
Cisco VIM Insight Already Exists!
+----------------------+--------+-------------------------------------------------------------+
| Description          | Status | Details                                                     |
+----------------------+--------+-------------------------------------------------------------+
| VIM Insight UI URL   | PASS   | https://<br_api:9000>                                       |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml> |
|                      |        |                                                             |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml        |
| VIM Insight Workspace | PASS   | /root/<insight_ws>                                          |
+----------------------+--------+-------------------------------------------------------------+

Cisco VIM Insight backup Info!
+---------------------+-------+-------------------------------------------------------------------------
+
```

```
| Description          | Status| Details
|
+----------------------+-------+-------------------------------------------------------------------------
+
| Insight backup Status| PASS  | Backup done @
|                      |
|                            | /var/cisco/insight_backup
/insight_backup_<release_tag>_<date_time>|
+----------------------+-------+-------------------------------------------------------------------------
+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
Insight gets autobacked up after reconfiguration at /var/cisco/insight_backup to preserve the
latest
state of Insight.
```

b. For Cisco VIM 3.4.5, run the below commands:

```
# cd Insight-<tag_id>
$ ./insight/insight_runner.py --reconfigure -f </root/insight_setup_data.yaml>
```

Reconfiguring Unified Management LDAP Server

UM supports both LDAP and LDAP over SSL (LDAPS) for an Active Directory (AD) environment. If the LDAP server is down or if you need to change any of its configuration, execute UM reconfigure action.

1. Reconfigure the LDAP(s) server:

   a. Fetch the latest *insight_setup_data.yaml* file

      i. For releases prior to Cisco VIM 3.4.5, enter the below commands:

      ```
      # cd /root/
      # mkdir MyDir
      # cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
      ```

      ii. For Cisco VIM 3.4.5, enter the below commands:

      ```
      # cd /root/
      # mkdir MyDir
      # cp /root/insight-openstack-configs/insight_setup_data.yaml
      ```

   b. Edit the *insight_setup_data.yaml* to change the value of LDAP keys.

      LDAP keys are listed below:

      - LDAP_MODE: This key can be reconfigured only to 'True', to allow the user to switch only from No-LDAP to LDAP, and not vice-versa.
      - LDAP_SERVER: This key is reconfigurable to switch to new LDAP server.
      - LDAP_PORT: Reconfiguration of this key is allowed.
      - LDAP_ADMIN: Reconfiguration of this key is allowed.
      - LDAP_ADMIN_PASSWORD: Reconfiguration of this key is allowed.
      - LDAP_SECURE: This key can be reconfigured only to 'True', to allow the user to switch from non-secure LDAP to secure LDAP connection, and not vice-versa.
      - LDAP_CERT_PATH: This key can be reconfigured, to switch from self-signed certificate to CA-signed certificate, and not vice-versa.
      - LDAP_USER_ID_ATTRIBUTE: This key can be reconfigured to point to new LDAP user id attribute.
      - LDAP_GROUP_SEARCH_FILTER: This key be reconfigured to set new group search filter.
      - LDAP_GROUP_MEMBER: This key can be reconfigured to set new attribute used on LDAP server for defining user-group association.
      - LDAP_GROUP_USER_SEARCH_FILTER: This key can be reconfigured to set new group-user search filter.
      - UM_ADMIN_GROUP: This key can be reconfigured to map LDAP role/group to Insight UM-Admin(s). This key is used when Insight authorization is via LDAP server.
      - POD_ADMIN_GROUP: This key can be reconfigured to map LDAP role/group to Insight Pod-Admin(s). This key is used when Insight authorization is via LDAP server.
      - POD_USER_GROUP: This key can be reconfigured to map LDAP role/group to Insight pod users with 'Full-pod-access'. This key is used, when Insight authorization is via LDAP server.

- READ_ONLY_POD_USER_GROUP: This key can be reconfigured to map LDAP role/group to Insight pod users with 'Read-only-access'. This key is used when Insight authorization is via LDAP server.
- LDAP_ROLE_MEMBER: This key can be reconfigured to set new attribute used on LDAP server for defining user-role/group-role association.

c. Save the edited file.

2. Run the bootstrap command:

a. For releases prior to Cisco VIM 3.4.5, execute the following commands:

```
# cd <insight_ws>
# ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Perform the action. Continue (Y/N)y
Management node validation
+-------------------------------+--------+-------+
| Rule                          | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None  |
| Check Ansible Version         | PASS   | None  |
| Check Docker Version          | PASS   | None  |
| Check Management Node Tag     | PASS   | None  |
| Check Bond Intf. Settings     | PASS   | None  |
| Root Password Check           | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings        | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition      | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition          | PASS   | None  |
| Check LVM partition           | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+-------------------------------+--------+--------

Insight standalone input validation
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation    | PASS   | None  |
| Valid key check in Insight setup data   | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check   | PASS   | None  |
| Check registry connectivity             | PASS   | None  |
| Check LDAP connectivity                 | PASS   | None  |
| Check Email server for Insight          | PASS   | None  |
+-----------------------------------------+--------+-------+

WARNING!! Reconfiguration will have few secs of Outage for Insight!
Cisco VIM Insight Already Exists!
+----------------------+--------+-------------------------------------------------------+
| Description          | Status | Details                                               |
+----------------------+--------+-------------------------------------------------------+
| VIM Insight UI URL   | PASS   | https://<br_api:9000>                                 |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml> |
|                      |        |                                                       |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml      |
| VIM Insight Workspace | PASS   | /root/<insight_ws>                                    |
+----------------------+--------+-------------------------------------------------------+

Cisco VIM Insight backup Info!
+----------------------+-------+-------------------------------------------------------------------------
+
| Description          | Status| Details
|
+----------------------+-------+-------------------------------------------------------------------------
+
| Insight backup Status| PASS | Backup done @
|                      |
|                      | /var/cisco/insight_backup/insight_backup_<release_tag>_<date_time>
|
+----------------------+-------+-------------------------------------------------------------------------
```

```
+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
Insight gets autobacked up after reconfiguration at /var/cisco/insight_backup to preserve the
latest
state of Insight.
```

b. For Cisco VIM 3.4.5, enter the following command:

```
# cd Insight-<tag_id>
$ ./insight/insight_runner.py --reconfigure -f </root/insight_setup_data.yaml>
```

Reconfiguring Unified Management Optional Features

UM supports reconfiguration of optional features.

1. Reconfigure the UM optional feature:
   a. Fetch the latest *insight_setup_data.yaml* file:
      i. For Releases prior to Cisco VIM 3.4.5, enter the following commands:

```
# cd /root/
# mkdir MyDir
# cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
```

      ii. For Cisco VIM 3.4.5, enter the following commands:

```
# cd /root/
# mkdir MyDir
# cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
```

   b. Edit the *insight_setup_data.yaml* to change the value of optional feature keys listed below:
      - UM_ADMIN_AS_POD_ADMIN: If set to True, all UM-Admins are added as pod-users with *Full-Pod-Access* during pod registration.
      - DISPLAY_ALL_POD_USERS: If set to True, a drop-down appears in the user-registration form with a list of all the users with pod-user permissions while adding a new pod-user.
2. Run the bootstrap command:
   a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

```
# cd <insight_ws>
# ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
VIM Insight reconfigure logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log Perform
the action. Continue (Y/N)y
Management node validation
+-------------------------------+--------+-------+
| Rule                          | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None |
| Check Ansible Version         | PASS   | None |
| Check Docker Version          | PASS   | None |
| Check Management Node Tag     | PASS   | None |
| Check Bond Intf. Settings     | PASS   | None |
| Root Password Check           | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings        | PASS   | None |
| Check Docker Pool Settings    | PASS   | None |
| Check Home Dir Partition      | PASS   | None |
| Check Root Dir Partition      | PASS   | None |
| Check /var Partition          | PASS   | None |
| Check LVM partition           | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+-------------------------------+--------+-------
Insight standalone input validation
```

```
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation    | PASS   | None  |
| Valid key check in Insight setup data   | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check   | PASS   | None  |
| Check registry connectivity             | PASS   | None  |
| Check LDAP connectivity                 | PASS   | None  |
| Check Email server for Insight          | PASS   | None  |
+-----------------------------------------+--------+-------+
WARNING!! Reconfiguration will have few secs of Outage for Insight
Cisco VIM Insight Already Exists!
+----------------------+--------+-----------------------------------------------------------+
| Description          | Status | Details                                                   |
+----------------------+--------+-----------------------------------------------------------+
| VIM Insight UI URL   | PASS   | https://<br_api:9000>                                     |
| VIM UI Admin Email ID | PASS   | Check for info @: <abs path of insight_setup_data.yaml> |
|                      |        |                                                           |
| VIM UI Admin Password | PASS   | Check for info @ /opt/cisco/insight/secrets.yaml          |
| VIM Insight Workspace | PASS   | /root/<insight_ws>                                        |
+----------------------+--------+-----------------------------------------------------------+

Cisco VIM Insight backup Info!
+----------------------+-------+-------------------------------------------------------------------------
+
| Description          | Status| Details
+----------------------+-------+-------------------------------------------------------------------------
+
| Insight backup Status| PASS  | Backup done @
|                      |
|                      | /var/cisco/insight_backup/insight_backup_<release_tag>_<date_time>
|
+----------------------+-------+-------------------------------------------------------------------------
+
Done with VIM Insight reconfigure!
VIM Insight reconfigure logs are at: "/var/log/insight/bootstrap_insight/"
Insight gets autobacked up after reconfiguration at /var/cisco/insight_backup to preserve the
latest
state of Insight
```

b. For Cisco VIM 3.4.5, enter the following commands:

```
# cd Insight-<tag_id>
$ ./insight/insight_runner.py --reconfigure -f </root/insight_setup_data.yaml>
```

Adding/Reconfiguring VIM Admin

Adding and Reconfiguring VIM Administrators

Cisco VIM UM supports management of the VIM Administrators. VIM administrator can log into the unified management node through SSH or the console using the configured password. By configuring to one VIM admin account, administrators do not have to share credentials. Administrators have individual accountability.
To enable one or more VIM administrators, perform the following steps:

1. Fetch the latest *insight_setup_data.yaml* file

    a. For releases prior to Cisco VIM 3.4.5, use the following commands:

    ```
    # cd /root/
    # mkdir MyDir
    # cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
    ```

    b. For Cisco VIM 3.4.5, use the following commands:

    ```
    # cd /root/
    # mkdir MyDir
    # cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
    ```

2. Modify the *insight_setup_data.yaml* file manually with the configurations listed as below:

```
# Each vim admin must have a vim_admin_password_hash, a vim_admin_public_key,
# or both.

## 1. vim_admin_username: ADMIN USER NAME                                |
##-----------------------------------------------------------------------
## vim admin user names should satisfy following criteria:
##     a. Required
##     b. Unique
##     c. ASCII chars
##     d. No space allowed
##     e. 1 <= Length <=32
##     f. Only lower case letters
##     g. Digits, underscores, or dashes
##     h. First character must be a letter or an underscore


## 2. vim_admin_password_hash: ADMIN USER PASSWORD HASH                  |
##-----------------------------------------------------------------------
## Optional, to generate a password hash:
## -> python -c 'import crypt; print crypt.crypt ("<plaintxt_strong_pwd>")'


## 2. vim_admin_public_key: ADMIN USER PUBLIC KEY                        |
##-----------------------------------------------------------------------
## Optional,, vim_admin_public_key is a user's public key.
## It can be generated with 'ssh-keygen'.
## Should be a string that starts with "ssh-rsa AAAA" or "ssh-ed25519 AAAA"


# Optional, must have at least one sub key defined.
vim_admins:
     # vim admin with only password hash.
  -  vim_admin_username: non_root_admin_1
     vim_admin_password_hash: $6.....

     # vim admin with password hash and public key
  -  vim_admin_username: non_root_admin_2
     vim_admin_password_hash: $6.....
     vim_admin_public_key: ssh-rsa AAAA... or ssh-ed25519 AAAA...
```

```
   # vim admin with only public key
-  vim_admin_username: non_root_admin_3
   vim_admin_public_key: ssh-rsa AAAA... or ssh-ed25519 AAAA...
```

3. Run the following reconfiguration commands:

   a. For releases prior to Cisco VIM 3.4.5, run the below commands:

   ```
   # cd <insight_ws>
   # ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
   ```

   b. For Cisco VIM 3.4.5, execute the below commands:

   ```
   # cd Insight-<tag_id>
   # ./insight/insight_runner.py --reconfigure -f <path_to insight_setup_data.yaml>
   ```

   ⚠ Cisco VIM administrators can manage their own passwords using the Linux *passwd* command. You can add or remove Cisco VIM administrator through the reconfigure option, while the passwords for their existing accounts remain unchanged.

Enabling Root Login

Enabling Root Login Post UM Node Installation

To complement the management of Cisco VIM administrators, Cisco VIM supports an option to enable/disable root access at login. By default, this option is set to True. You can optionally disable this facility through reconfiguration.
Following are the steps to enable root login:

1. Fetch the latest *insight_setup_data.yaml* file
    a. For releases prior to Cisco VIM 3.4.5, run the below commands:

    ```
    # cd /root/
    # mkdir MyDir
    # cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
    ```

    b. For Cisco VIM 3.4.5, run the below commands:

    ```
    # cd /root/
    # mkdir MyDir
    # cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
    ```

2. Modify the *insight_setup_data.yaml* file manually with the configurations listed as below:

    ```
    # True: root can SSH to the UM management node.
    # False: root cannot SSH to the UM management node.
    #        At least one vim_admin must be configured if this is False
    #        One has to use su to drop down to root and execute administrator functionalities
    permit_root_login: False
    ```

3. Run the following reconfiguration commands:
    a. For releases prior to Cisco VIM 3.4.5, run the below commands:

    ```
    # cd <insight_ws>
    # ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
    ```

    b. For Cisco VIM 3.4.5, run the below commands:

    ```
    # cd Insight-<tag_id>
    # ./insight/insight_runner.py --reconfigure -f <path_to insight_setup_data.yaml>
    ```

Enabling SSH Banner

Enabling Banner During SSH Login

Cisco VIM supports enabling of banner during SSH login to the management node. To enable banner during login, perform the following steps:

1. Fetch the latest *insight_setup_data.yaml* file
    a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

    ```
    # cd /root/
    # mkdir MyDir
    # cp /root/Insight-<tag-id>/openstack-configs/insight_setup_data.yaml /root/MyDir/
    ```

    b. For Cisco VIM 3.4.5, enter the following commands:

    ```
    # cd /root/
    # mkdir MyDir
    # cp /root/insight-openstack-configs/insight_setup_data.yaml /root/MyDir/
    ```

2. Modify the *insight_setup_data.yaml* file manually with the configurations listed as below:

    ```
    ssh_banner:
     <your Banner Text>
    ```

3. Run the following commands for reconfiguration:
    a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

    ```
    # cd <insight_ws>
    # ./bootstrap_insight.py -a reconfigure -f <path_to insight_setup_data.yaml>
    ```

    b. For Cisco VIM 3.4.5, enter the following commands:

    ```
    # cd Insight-<tag_id>
    # ./insight/insight_runner.py --reconfigure -f <path_to insight_setup_data.yaml>
    ```

Upgrade/Update UM

Upgrade/Update VIM Unified Management

Cisco VIM Unified Management update allows you to switch to a new UM release. To move the UM node from Cisco VIM 3.2.x or Cisco VIM 3.4.y where x<=4 and y is less than the maintenance release version of the current release, to the current Cisco VIM release, execute the *update* action.

The *update* action makes the old docker containers of UM and mariadb in exit state, and brings up new ones with the new tag. The old containers and images are restored until you perform the *Commit* action.
Update is an intermediate action and allows you to do either a *Commit* action to settle for the current version or do a *Rollback* to revert back to the old version.
The old workspace is preserved, if you want to do a rollback to the previous version.

Old and new workspaces are preserved after commit and rollback respectively in */opt/cisco/insight/insight_archive*

After an update:

- Your UM workspace is set as the new workspace that you just extracted out of the tarball.
- Backup and reconfigure action are not allowed either from old or new UM workspace.

Update Scenarios

Following are the update scenarios:

- Insight and MariaDB containers gets updated to the new tag.
- Either insight or MariaDB container gets updated to the new tag.
- Data containers get updated to the new tag but not reverted to old tag after rollback. This is done to preserve potential security and kernel fixes.

Update Cisco VIM UM with Internet Access from 3.2.x (x<=4) or 3.4.y

The value of *y* is less than the maintenance release version of the current Cisco VIM release.

Following are the steps to update VIM UM:

1. Get the new installer tarball, which is available after each release. Extract the tarball to get the new Unified Management workspace by running the following command:

```
tar --no-same-owner -xvzf mercury-installer.tar.gz
```

2. Create an empty directory for Insight workspace: *Insight-<tag_id>*
3. Copy the contents of the extracted directory *installer-<tag_ig>* within *Insight-<tag_id>:*

```
# cp -r installer-<tag_ig>/* Insight-<tag_id>
```

4. Update the Cisco VIM UM:
    a. For releases prior to Cisco VIM 3.4.5, run the following commands:

```
# cd /root/<new_insight_ws>/insight/
/bootstrap_insight.py -a update
VIM Insight update logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Management Node validation!
+-------------------------------+--------+-------+
| Rule                          | Status | Error|
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None |
| Check Docker Version          | PASS   | None |
| Check Management Node Tag     | PASS   | None |
```

```
| Check Bond Intf. Settings     | PASS   | None |
| Root Password Check           | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings        | PASS   | None |
| Check Docker Pool Settings    | PASS   | None |
| Check Home Dir Partition      | PASS   | None |
| Check Root Dir Partition      | PASS   | None |
| Check /var Partition          | PASS   | None |
| Check LVM partition           | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+-------------------------------+--------+------+
Insight standalone input validation
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation    | PASS   | None  |
| Valid key check in Insight setup data   | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check   | PASS   | None  |
| Check registry connectivity             | PASS   | None  |
| Check Email server for Insight          | PASS   | None  |
+-----------------------------------------+--------+-------+
Downloading Updated VIM Insight Artifacts, will take time!!!
Cisco VIM Insight update Info!
+-----------------------------------------+--------+-------------------------------+
| Description                             | Status | Details                       |
+-----------------------------------------+--------+-------------------------------+
| VIM Insight Container: insight_<new_tag> | PASS   | Updated from insight_<old_tag>|
| VIM Mariadb Container: mariadb_<new_tag> | PASS   | Updated from mariadb_<old_tag>|
+-----------------------------------------+--------+-------------------------------+
Done with VIM Insight update!
VIM Insight update logs are at: "/var/log/insight/bootstrap_insight/"
```

b. For Cisco VIM 3.4.5, execute the following commands:

```
# cd /root/Insight-<tag_id>

Check the containers lined up for update
# ./insight/insight_runner.py --update --dry-run

Start the update
# ./insight/insight_runner.py --update
```

5. Verify the UM update:

a. For releases prior to Cisco VIM 3.4.5, execute the following commands:

```
# cd /root/<new_insight_ws>/insight/
# ./bootstrap_insight.py -a update-status
Cisco VIM Insight Update Status!
+-----------------------------------------+--------+--------------------------------+
| Description                             | Status | Details                        |
+-----------------------------------------+--------+--------------------------------+
| VIM Insight Container: insight_<new_tag> | PASS   | Updated from insight_<old_tag> |
| VIM Mariadb Container: insight_<new_tag> | PASS   | Updated from mariadb_<old_tag> |
+-----------------------------------------+--------+--------------------------------+
```

b. For Cisco VIM 3.4.5, execute the following commands::

```
# cd /root/Insight-<tag_id>
# ./insight/insight_runner.py --update-status

Cisco VIM Insight Update Status!
+-----------------------------------------+--------+----------------------------------+
|              Description                | Status |           Details                |
+-----------------------------------------+--------+----------------------------------+
```

```
| VIM Insight Container: insight_<new_tag> | PASS   |  Updated from insight_<old_tag>  |
| VIM Mariadb Container: insight_<new_tag> | PASS   |  Updated from mariadb_<old_tag>  |
+------------------------------------------+--------+----------------------------------+
```

Update Cisco VIM UM without Internet Access from 3.2.x (x<=4) or 3.4.y

⚠ The value of *y* is less than the maintenance release version of the current Cisco VIM release.

1. Copy the new installer tarball to the UM node. Extract the tarball to get the new UM workspace by running the following command:

```
tar --no-same-owner -xvzf mercury-installer.tar.gz
```

2. Create an empty directory for Insight workspace: *Insight-<tag_id>*
3. Copy the contents of the extracted directory *installer-<tag_ig>* within *Insight-<tag_id>*

```
# cp -r installer-<tag_ig>/* Insight-<tag_id>
```

4. To download, test and import the new UM artifacts, follow the steps given in UM Without Internet Access only till Step 11.
5. Update the Cisco VIM UM by running the following commands:

   a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

```
# cd /root/<new_insight_ws>/insight/
/bootstrap_insight.py -a update
VIM Insight update logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Management Node validation!
+-------------------------------+--------+------+
| Rule                          | Status | Error|
+-------------------------------+--------+------+
| Check Kernel Version          | PASS   | None |
| Check Docker Version          | PASS   | None |
| Check Management Node Tag     | PASS   | None |
| Check Bond Intf. Settings     | PASS   | None |
| Root Password Check           | PASS   | None |
| Check Boot Partition Settings | PASS   | None |
| Check LV Swap Settings        | PASS   | None |
| Check Docker Pool Settings    | PASS   | None |
| Check Home Dir Partition      | PASS   | None |
| Check Root Dir Partition      | PASS   | None |
| Check /var Partition          | PASS   | None |
| Check LVM partition           | PASS   | None |
| Check RHEL Pkgs Install State | PASS   | None |
+-------------------------------+--------+------+
Insight standalone input validation
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone schema validation    | PASS   | None  |
| Valid key check in Insight setup data   | PASS   | None  |
| Duplicate key check In Insight setup data | PASS   | None  |
| CVIM/Insight workspace conflict check   | PASS   | None  |
| Check registry connectivity             | PASS   | None  |
| Check Email server for Insight          | PASS   | None  |
+-----------------------------------------+--------+-------+
Downloading Updated VIM Insight Artifacts, will take time!!!
Cisco VIM Insight update Info!
+-----------------------------------------+--------+--------------------------------+
| Description                             | Status | Details                        |
+-----------------------------------------+--------+--------------------------------+
| VIM Insight Container: insight_<new_tag> | PASS   | Updated from insight_<old_tag>|
| VIM Mariadb Container: mariadb_<new_tag> | PASS   | Updated from mariadb_<old_tag>|
+-----------------------------------------+--------+--------------------------------+
Done with VIM Insight update!
VIM Insight update logs are at: "/var/log/insight/bootstrap_insight/"
```

b. For Cisco VIM 3.4.5, enter the following commands:

```
# cd /root/Insight-<tag_id>

Check the containers lined up for update
# ./insight/insight_runner.py --update --dry-run

Start the update
# ./insight/insight_runner.py --update
```

6. Verify the UM update:

a. For releases prior to Cisco VIM 3.4.5, enter the following commands::

```
# cd /root/<new_insight_ws>/insight/
# ./bootstrap_insight.py -a update-status
Cisco VIM Insight Update Status!
+-----------------------------------------+--------+---------------------------------+
| Description                             | Status | Details                         |
+-----------------------------------------+--------+---------------------------------+
| VIM Insight Container: insight_<new_tag> | PASS   | Updated from insight_<old_tag> |
| VIM Mariadb Container: insight_<new_tag> | PASS   | Updated from mariadb_<old_tag> |
+-----------------------------------------+--------+---------------------------------+
```

b. For Cisco VIM 3.4.5, enter the following commands:

```
# cd /root/Insight-<tag_id>
# ./insight/insight_runner.py --update-status

Cisco VIM Insight Update Status!
+-----------------------------------------+--------+-----------------------------------+
|              Description                | Status |           Details                 |
+-----------------------------------------+--------+-----------------------------------+
| VIM Insight Container: insight_<new_tag> | PASS   |  Updated from insight_<old_tag>  |
| VIM Mariadb Container: insight_<new_tag> | PASS   |  Updated from mariadb_<old_tag>  |
+-----------------------------------------+--------+-----------------------------------+
```

Upgrade Scenario

The changes to the underlying infrastructure such as docker, RHEL and database schema, exist in Cisco VIM UM code between versions of 2.4.x (x=15 or 16 or 17 or 18) and the current release.

Upgrade Cisco VIM UM from 2.4.x

To address the upgrade of major infrastructure change, upgrade the Cisco VIM UM node from 2.4.x (x=15 or 16 or 17 or 18) to the current release of Cisco VIM UM node using the following steps:

1. Get the installer tarball for 3.4.3 release. Extract the tarball to get the new UM workspace by running the following command:

```
tar --no-same-owner -xvzf mercury-installer.tar.gz
```

2. Create an empty directory to take a backup of Cisco VIM UM node.
3. Run Insight upgrade script with *-b [backup]* option:

```
# cd /root/installer-<tag_id>/tools
# ./insight_upgrade.sh -b -d <path of backup directory>
```


Ensure that you provide the backup directory path with a '/' at its end.

4. Copy the backup directory to the remote server. For example, to copy the backup directory */var/cisco/insight_upgrade_backup/* from the management node to the remote host (for example: 20.0.0.5), execute the following command sequence:

```
rsync -e ssh -go -rtvpX --numeric-ids /var/cisco/insight_upgrade_backup/ root@20.0.0.5:/var/cisco
/insight_upgrade_backup
```

> ⚠ Ensure that the path root@20.0.0.5*:/var/cisco/insight_upgrade_backup/* is available at the remote location.

5. Re-image the UM node with the ISO of the current release version and with the same IP address.
6. Copy the backup directory from the remote server to the management node. For example, to copy the backup directory */var/cisco /insight_upgrade_backup/* from remote host 20.0.0.5 to the management node, execute the following command sequence.

```
rsync -e ssh -go -rtvpX --numeric-ids root@20.0.0.5:/var/cisco/insight_upgrade_backup/ /var/cisco
/insight_upgrade_backup/.
```

> ⚠
> - Ensure that the path */var/cisco/insight_upgrade_backup/* is present on UM node.
> - For installation with Internet access, skip Step 9.

7. Create an empty directory for Insight workspace: *Insight-<tag_id>*.
8. Copy the contents of the extracted directory *installer-<tag_ig>* within *Insight-<tag_id>:*

```
# cp -r installer-<tag_ig>/* Insight-<tag_id>
```

9. To download, test, and import the new UM artifacts, follow the steps given in UM Without Internet Access only till Step 11.
10. Run Insight upgrade with *-r [restore]* option:

```
# cd /root/installer_<tag_id>/tools
# ./insight_upgrade.sh -r -d <path of backup directory>'
```

11. After successful execution of upgrade, use the *reconfigure* option to enable new Insight features or *install-status* to check Insight installation status:

    a. For releases prior to Cisco VIM 3.4.5, execute the below commands:

    ```
    # cd /root/Insight-<tag_id>/insight

    # ./bootstrap_insight.py -a install-status
    # ./bootstrap_insight.py -a reconfigure -f <insight_setup_data.yaml>
    ```

    b. For Cisco VIM 3.4.5, execute the below commands:

    ```
    # cd /root/Insight-<tag_id>

    # ./insight/insight_runner.py --install-status
    # ./insight/insight_runner.py --reconfigure -f <insight_setup_data.yaml>
    ```

Rollback UM

Rollback VIM Unified Management

Cisco VIM Unified Management rollback feature allows you to revert to the old UM release which is used before the update.
Following are some of the key points:

- The rollback action removes the new docker containers of Unified Management and mariaDB which is created after an update and bring up old ones with the old tag.
- After rollback, your UM workspace is the old workspace which you were using before the update.

Following are the steps to perform UM rollback:

1. Run the following command from the new workspace to rollback VIM Unified Management:

   a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

```
# cd /root/Insight-<tag_id>/insight
# ./bootstrap_insight.py -a rollback
VIM Insight rollback logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Management node validation!
+-------------------------------+--------+-------+
| Rule                          | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None  |
| Check Ansible Version         | PASS   | None  |
| Check Docker Version          | PASS   | None  |
| Check Management Node Tag     | PASS   | None  |
| Check Bond Intf. Settings     | PASS   | None  |
| Root Password Check           | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings        | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition      | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition          | PASS   | None  |
| Check LVM partition           | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None
+-------------------------------+--------+-------+
Insight standalone input validation
+----------------------------------------+--------+-------+
| Rule                                   | Status | Error |
+----------------------------------------+--------+-------+
| Insight standalone schema validation   | PASS   | None |
| Valid key check in Insight setup data  | PASS   | None |
| Duplicate key check In Insight setup data | PASS   | None |
| CVIM/Insight workspace conflict check  | PASS   | None |
| Check registry connectivity            | PASS   | None |
| Check Email server for Insight         | PASS   | None |
+----------------------------------------+--------+-------+
VIM Insight rollback in progress, Kindly wait!!!
Cisco VIM Insight rollback Info!
+----------------------------------------+--------+---------------------------------+
| Description                            | Status | Details                         |
+----------------------------------------+--------+---------------------------------+
| VIM Insight UI URL                     | PASS   | https://<br_api:9000>           |
| VIM Insight Container: insight_<old_tag> | PASS   | Rollback from insight_<new_tag> |
| VIM Mariadb Container: mariadb_<old_tag> | PASS   | Rollback from mariadb_<new_tag> |
| VIM Insight Workspace                  | PASS   | /root/<old_insight_ws>          |
+----------------------------------------+--------+---------------------------------+
Done with VIM Insight rollback!
VIM Insight rollback logs are at: "/var/log/insight/bootstrap_insight/"
```

   b. For Cisco VIM 3.4.5, enter the following commands:

```
# cd /root/Insight-<tag_id>
# ./insight/insight_runner.py --rollback
```

2. Verify the rollback status by running the following command:

   a. For releases prior to Cisco VIM 3.4.5, enter the following commands:

```
# ./bootstrap_insight.py -a install-status
Cisco VIM Insight Install Status!
+-----------------------+--------+----------------------------------+
| Description           | Status | Details                          |
+-----------------------+--------+----------------------------------+
| VIM Insight Version   | PASS   | <release_tag>                    |
| VIM Insight UI URL    | PASS   | https://<br_api:9000>            |
| VIM Insight Container | PASS   | insight_<tag_id>                 |
| VIM Mariadb Container | PASS   | mariadb_<tag_id>                 |
| VIM Insight Workspace | PASS   | /root/<insight_ws>               |
+-----------------------+--------+----------------------------------+
```

   b. For Cisco VIM 3.4.5, enter the following commands:

```
# ./insight/insight_runner.py --install-status

Cisco VIM Insight Install Status!
+-----------------------+--------+----------------------------------+
| Description           | Status | Details                          |
+-----------------------+--------+----------------------------------+
| VIM Insight Version   | PASS   | <release_tag>                    |
| VIM Insight UI URL    | PASS   | https://<br_api:9000>            |
| VIM Insight Container | PASS   | insight_<tag_id>                 |
| VIM Mariadb Container | PASS   | mariadb_<tag_id>                 |
+-----------------------+--------+----------------------------------+
```

Commit UM

Commit VIM Unified Management

From Cisco VIM 3.4.5, Insight commit is enabled after an update. Following are some of the key points:

- The old workspace is not deleted and retained as it is.
- After the commit, your Unified Management workspace that is used for the update becomes the new workspace.

1. Run the following command to commit VIM Insight:

   a. For releases prior to Cisco VIM 3.4.5:

```
# cd /root/<new_insight_ws>/Insight
# ./bootstrap_insight.py -a commit
VIM Insight commit logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Management Node Validation!
+-------------------------------+--------+-------+
| Rule                          | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version          | PASS   | None  |
| Check Ansible Version         | PASS   | None  |
| Check Docker Version          | PASS   | None  |
| Check Management Node Tag     | PASS   | None  |
| Check Bond Intf. Settings     | PASS   | None  |
| Root Password Check           | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings        | PASS   | None  |
| Check Docker Pool Settings    | PASS   | None  |
| Check Home Dir Partition      | PASS   | None  |
| Check Root Dir Partition      | PASS   | None  |
| Check /var Partition          | PASS   | None  |
| Check LVM partition           | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+-------------------------------+--------+-------+
Insight standalone Input Validation!
+-----------------------------------------+--------+-------+
| Rule                                    | Status | Error |
+-----------------------------------------+--------+-------+
| Insight standalone Schema Validation    | PASS   | None  |
| Valid Key Check in Insight Setup Data   | PASS   | None  |
| Duplicate Key Check In Insight Setup Data | PASS   | None  |
| CVIM/Insight workspace conflict         | PASS   | None  |
| Check registry connectivity             | PASS   | None  |
| Check Email server for Insight          | PASS   | None  |
+-----------------------------------------+--------+-------+
VIM Insight commit in progress, Kindly wait!!!
Cisco VIM Insight commit Info!
+---------------------------------------- +--------+-------------------------------------------
| Description                             | Status | Details                                   |
+-----------------------------------------+--------+-------------------------------------------+
| VIM Insight UI URL                      | PASS   | https://<br_api:9000>                     |
| VIM Insight Container: insight_<old_tag> | PASS   | Old container: insight-<old_tag> removed> |
| VIM Mariadb Container: mariadb_<old_tag> | PASS   | Old container: mariadb-<old_tag> removed> |
| VIM Insight Workspace                   | PASS   | /root/<old_insight_ws>                    |
+-----------------------------------------+--------+-------------------------------------------+
Done with VIM Insight commit!
VIM Insight commit logs are at: "/var/log/insight/bootstrap_insight/"
```

   b. For release Cisco VIM 3.4.5:

```
# cd /root/Insight-<tag_id>
# ./insight/insight_runner.py --commit
```

   ⚠ If update is done from 3.0.x to 3.4.2, the following warning message to reconfigure Insight is displayed.

Warning: Insight setup-data key UM_ADMIN_AS_POD_ADMIN is deprecated from version 3.4.2 and please reconfigure using UM_ADMIN_WITH_FULL_POD_ACCESS as the new name of the key

2. Verify the commit status by running the following command:

   a. For releases prior to Cisco VIM 3.4.5:

```
# ./bootstrap_insight.py -a install-status
Cisco VIM Insight Install Status!
+-----------------------+--------+-----------------------+
| Description           | Status | Details               |
+-----------------------+--------+-----------------------+
| VIM Insight Version   | PASS   | <release_tag>         |
| VIM Insight UI URL    | PASS   | https://<br_api:9000> |
| VIM Insight Container | PASS   | insight_<tag_id>      |
| VIM Mariadb Container | PASS   | mariadb_<tag_id>      |
| VIM Insight Workspace | PASS   | /root/<insight_ws>    |
+-----------------------+--------+-----------------------+
```

   b. For release Cisco VIM 3.4.5:

```
# ./insight/insight_runner.py --install-status

Cisco VIM Insight Install Status!
+-----------------------+--------+---------------------------------+
| Description           | Status | Details                         |
+-----------------------+--------+---------------------------------+
| VIM Insight Version   | PASS   | <release_tag>                   |
| VIM Insight UI URL    | PASS   | https://<br_api:9000>           |
| VIM Insight Container | PASS   | insight_<tag_id>                |
| VIM Mariadb Container | PASS   | mariadb_<tag_id>                |
+-----------------------+--------+---------------------------------
```

Uploading Glance Images

Uploading Glance Images

1. On Day 0, keep all the Glance Images to be uploaded in a folder. To view those images under **Pod Image Management**, copy those images using the ***glance_image_copy.sh script***. The *glance_image_copy.sh* script is available in the insight folder, same as the *bootstrap_insight.py* level:

```
[root@gg34-bn insight]# ./glance_image_copy.sh -h
glance_image_copy.sh : Cisco Glance Images Validator
-----------------------------------------------------
-d : Input Glance Images Directory.
Allowed Images Formats:
- 'raw', 'qcow2', 'iso', 'ami', 'ari', 'aki', 'vhd', 'vhdx', 'vmdk', 'vdi','ploop'
-h : To display this help
```

2. Use *-d* option, which represents the directory path of Glance Images to be uploaded, and copy the Glance Images by running the following command:

```
[root@gg34-bn insight]# ./glance_image_copy.sh -d /root/ImagesDir/
Copying /root/ImagesDir/mini.iso ...
Copying /root/ImagesDir/xenial-server-cloudimg-amd64-disk1.vmdk ...
Copying /root/ImagesDir/cirros-0.4.0-x86_64-disk.img ...
Copying /root/ImagesDir/CentOS-7-x86_64-GenericCloud-1905.raw ...
```

3. After copying images using the *glance_image_copy.sh* script, refresh Cisco VIM Unified Management appliance to view the Glance Images under **Pod Image Management**. You can select multiple images and upload them.

Backup and Restore

Backup and Restore of Management/UM Node

Backing Up Management Node

Backing Up Management Node

Overview

The management node hosts critical services such as Cisco VIM REST API, Cobbler for PXE, ELK for logging/Kibana dashboard, and VMTP for the cloud validation in Cisco VIM.
As the management node is not redundant, ensure that you take the backup of the management node. If you are facing any issues with the platform, you can restore the management node using the saved management node information.

Management Node Backup

An administrator must maintain the number of backup snapshots on the management node. The backup of the management node is possible only after the complete deployment of at least one Cisco VIM. Two copies of backup, either manual or autobackup is maintained at the management node itself and the older copy is overwritten when a next backup is performed.

Following are some of the activities that cannot be performed during backup:

- Pod management.
- Software update or upgrade.
- Addition, deletion or replacement of nodes.

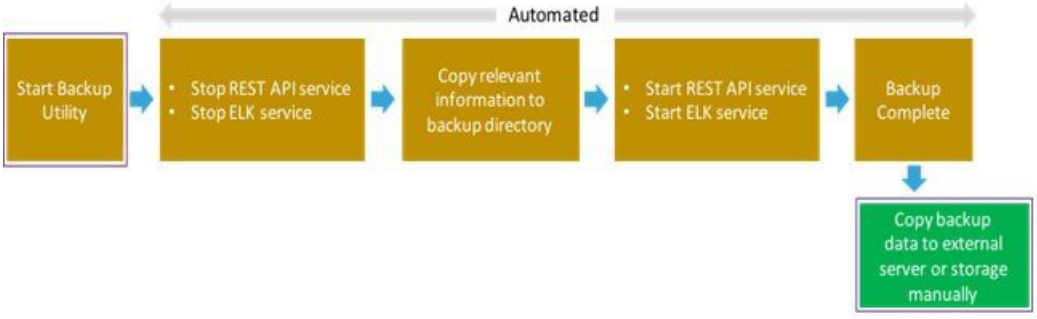
During backup, the REST API service is stopped and the OpenStack logs are cached on the control, compute, and storage nodes until the restoration of the management node is complete.
As part of the backup operation, two files are created:

- .backup_files
- .backup_hash

where *.backup_files* is a list of files that are backed up and the second one is the hash. These two files are also placed at the */var/cisco/ folder* of all the controllers and are used during the restore validation. However, these files are not visible to users and are compressed under *cvim_<RELEASE_TAG>.tar.gz* in the backup directory. Modification of *cvim_<RELEASE_TAG>.tar.gz* and its files is strictly not permitted.

When you attempt to restore from a particular backup, these two files within backup are compared with the files kept in the controllers. If there is any discrepancy, the restore validation fails and you are prompted to either terminate the restore operation or continue despite the validation failure.

Only one copy of the .backup_files and .backup_hash are kept at the controllers. That is, whenever a new backup is created, these two files are overwritten with the most recent ones. Hence the restore validation passes only when the latest backup is used for restore. The following figure illustrates the management node backup operation.



Before you begin

- Save the management node information, for example, IP address of the management node, for use during the restore operation.
- Ensure that you have the br_mgmt and br_api IP addresses and the respective network information.

1. Launch a SSH session with the Cisco NFVI management node.
2. Navigate to *<installer-ws>/tools/mgmt/ directory*.
3. Execute *mgmt_node_backup.py*. The backup operation takes approximately 30 minutes and creates *backup_<tag>_<date-time>* directory in the */var/cisco/ path* for disconnected installation. From Cisco VIM 3.4.3, an optimization to reduce the backup size is available for connected installation. This reduces the overhead needed to copy the backup out of the pod during restoration. However, ensure that the management node is connected to the registry to download the artifacts for which additional time is required.

4. Copy the directory to a remote server using *rsync* or *scp,* to recover the management node via restore.
   For example, to copy the backup directory to the remote server *<target_ip>:/var/cisco/directory*, execute the following command sequence:

```
# autobackup triggered as part of pod management operation
rsync -e ssh -go -rtvpX --numeric-ids /var/cisco/autobackup_<version>_<date-time>
root@<remote_ip_address>:/var/cisco/

# manual backup triggered by admin
rsync -e ssh -go -rtvpX --numeric-ids /var/cisco/backup_<version>_<date-time> root@<remote_ip_address>:
/var/cisco/

# scp command can also be used for remote copy (starting CVIM 3.4.3)
# Note that scp command can only be used when copying Cisco VIM backup directories.
scp -r /var/cisco/autobackup_<version>_<date-time> <username>@<remote_ip_address>:/var/cisco/
```


On the remote server, protect the backup directory from unauthorized access as the backup files may contain sensitive information. To preserve the file ownership and Linux markings, run as *root* to sync the remote server. The remote server must run RHEL or CentOS 7. x, so that no permission or markings are lost.

5. At the remote server, change the directory to where the backup directory is copied to. In this example, */var/cisco/backup_<version>_<date-time>/.*
6. To verify whether the backup is not corrupted or modified, execute *./check_integrity.*
   Check_integrity depends on the following packages. The packages are installed on the server where check_integrity is executed.

```
python-prettytable
python-jinja2
python-babel
python-markupsafe
python-setuptools
pytz
```

Backup with Cisco VIM Service Logs

By default, Cisco VIM service logs are not backed up during autobackup or manual backup. These logs include *REST-API*, *VMTP, SNMP,* and so on. You can take its backup manually, if required.

For manual backup, you can override by appending the *-l* or *--logs* option to the backup command.

```
# cd installer/tools/mgmt
# ./mgmt_node_backup.py --help
Usage: ./mgmt_node_backup.py [options]
Options:

-h, --help  show this help message and exit
-l, --logs  force to also collect Cisco VIM service logs on backup
```

Pods Hosting Central Management VMs

You must take manual backup of QCOW2 images used for hosting the central management VMs, as automated backup does not take care of those target images. Get the location of these images from the IMAGE section of */root/openstack-configs/setup_data.CentralMgmt.yaml.*

Restoring Management Node

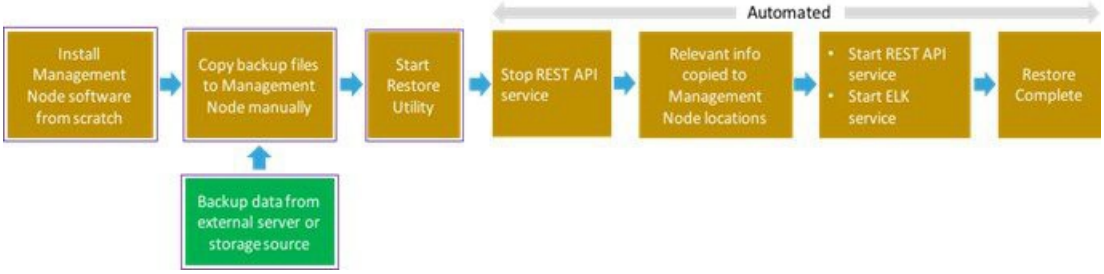
Restoring Management Node

You have to reimage the management node with the running Cisco VIM release ISO version when the backup is performed, before initiating the restore operation. The restoration fails, in case of a version mismatch.

> ⚠ Version checking is available only for offline installation.

During restore operation, the system checks for the management node's IP address information to match the prior configuration. The logs are cached on the control, compute, and storage nodes from the moment of the management node failure until its restoration.

The following figure illustrates Cisco VIM management node restore operation.



> ⓘ Ensure that you have the br_mgmt and br_api IP addresses of the failed management node.

> ⚠ Ensure that you execute the following restoration procedure only with *root* user.

1. Reimage the management node with the ISO version with which you want to restore the node, and with the same IP address that is used before the failure of the node. For more information on management node, see Management Node on UCS C-series (M4/M5) or Management Node on Quanta Servers based on the type of management node that you use.
2. Navigate to */var/cisco/directory* at the remote server where the backup folder is copied during the backup operation. Execute *./check_integrity*, to verify if the backup is not corrupted or modified.
3. Copy the backup file to the */var/cisco/directory* of the reimaged management node.
   For example, to copy the backup folder from the remote host <remote_ip> to the management node */var/cisco/directory*, execute the following command sequence from the management node:

   ```
   rsync -e ssh -go -rtvpX --numeric-ids root@<remote_ip>:/var/cisco/backup_2017-01-09_14-04-38 /var/cisco/

   Or
   ## on the management node, create /var/cisco/ directory, if it does not exist
   # mkdir /var/cisco/
   # scp command can also be used (starting Cisco VIM 3.4.3)
   # scp -r <remote_username>@<remote_ip>:/var/cisco/backup_2017-01-09_14-04-38 /var/cisco/
   ```

   > ⚠ Ensure that you preserve the backup directory at the remote node until the entire process of restore is complete.

4. Navigate to the backup folder and execute the following command to verify if the backup is not corrupted or modified.

   ```
   # cd /var/cisco/backup_<date-time>
   # ./check_integrity
   ```

5. In */var/cisco/backup_<date-time>* folder, execute the following command, when restoring a baremetal management node that is Layer 2 adjacent to the pod or a management node VM that is Layer 3 adjacent to the pod (in both conditions the api and management network does not change before and after the restore):

   ```
   /var/cisco/backup_<date-time> # ./restore
   ```

For migrating the management node that is Layer 2 or Layer 3 adjacent from the pod, to one in a VM that is in Layer 3 adjacent to the pod, do the following (in both conditions the api and management network changes before and after the restore):

In */var/cisco/backup_<date-time>* folder, execute the following command:

```
/var/cisco/backup_<date-time> # ./restore --remote
```


The restore operation takes around 45 to 60 minutes. As the central management of VMs do not support NFVBench, the corresponding information gets deleted from the *setup_data.yaml* in the central management VM.

6. Before restoration, the restore script performs validation of the backup folder. If validation fails, restore operation is halted and an error message is displayed. The script also verifies the last performed backup folder in the management node. If any defects are detected, you must confirm to proceed with restore operation.

```
....
2017-02-02 21:25:23 INFO Starting Cisco VIM restore...
2017-02-02 21:25:23 INFO Cisco VIM restore: estimated run time is approx. 45 mins...
2017-02-02 21:25:23 INFO Please see progress log for restore at
/var/log/mercury/installer/restore_2017-02-02_21:25:23.log
2017-02-02 21:25:27 ERROR Error: Backup id is not the one expected
Error: Found hashID file only in controller(s): controller-2, controller-3
Management backup files are ok (as per controller-2)
Management backup files are ok (as per controller-3)
The management node changed after the last backup was stored. Do you still want to proceed restoring
this management node? [Y/n] y
2017-02-02 22:17:55 INFO Workspace restored to /root/installer-6518
2017-02-02 22:17:55 INFO Cisco VIM restore: Executing restore playbook ...
2017-02-02 22:18:47 INFO Cisco VIM restore: Executing bootstrap playbook ...
```


The default behavior is to continue by keying **Return** or **Y**. Keying **N** terminates the restore operation

```
...
2017-02-02 21:25:23 INFO Starting Cisco VIM restore...
2017-02-02 21:25:23 INFO Cisco VIM restore: estimated run time is approx. 45 mins...
2017-02-02 21:25:23 INFO Please see progress log for restore at
/var/log/mercury/installer/restore_2017-02-02_21:25:23.log
2017-02-02 21:25:27 ERROR Error: Backup id is not the one expected
Error: Found hashID file only in controller(s): controller-2, controller-3
Management backup files are ok (as per controller-2)
Management backup files are ok (as per controller-3)
The management node changed after the last backup was stored. Do you still want to proceed restoring
this management node? [Y/n] n
Aborting the restore operation as per user request
```

7. Once the restoration is done, several health check points are automatically executed and the summary of results for that particular cloud availability is displayed:
8. Run the following checks manually to verify the restore status:

    a. Check the status of the REST API server:

    ```
    # cd installer-<tagid>/tools
    #./restapi.py -a status
    Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h ago
    REST API launch directory: /root/installer-<tagid>/
    ```

    b. Check the setup_data and runtime consistency of the management node:

    ```
    # cd installer-<tagid>/; ciscovim run --perform 1,3 -y
    ```

    c. Execute the cloud sanity using *ciscovim* command:

    ```
    # ciscovim cloud-sanity create test all
    ```

d. To view the results of cloud sanity, use the command:

```
# ciscovim cloud-sanity show result all -id <uid of the test>
```


If the pod is hosting VMs for central management, post restoration of the management node, copy the QCOW2 images to the directory location as defined in the IMAGE section of */root/openstack-configs/setup_data.CentralMgmt.yaml*.

Management Node Autobackup

Management Node Autobackup

Cisco VIM supports the backup and recovery of the management node. By default, the feature is enabled. Auto-snapshots of the management node happens during pod management operation. You can disable the autobackup of the management node. After the successful completion of certain pod management operations, a backup of the management node is performed automatically. Only two copies of the backup, either manual or automatic is kept at */var/cisco/* at any given time.

The directory format is autobackup_<tag>_<timestamp>.

Following are the list of operations:

- Fresh installation of Cisco VIM.
- Commit an update.
- Replace controller.
- Add or remove compute nodes.
- Add or remove the storage node.
- Reconfiguration.
- CVIM-MON.

1. To enable or disable the management node, update the *setup_data.yaml* file as follows:

```
AutoBackup Configuration

# Default is True
#autobackup: <True or False>
```

2. Take a backup of setupdata file and update it manually with the configuration details by running the following command:

```
[root@mgmt1 ~]# cd /root/
[root@mgmt1 ~]# mkdir MyDir
[root@mgmt1 ~]# cp /root/openstack-configs/setup_data.yaml /root/MyDir/
[root@mgmt1 ~]# # update the setup_data to change autobackup
[root@mgmt1 ~]# cd /root/MyDir/
[root@mgmt1 ~]# vi setup_data.yaml
[root@mgmt1 ~]# cd ~/installer-xxxx
[root@mgmt1 ~]# ciscovim reconfigure --setupfile /root/MyDir/setup_data.yaml
```

The following table shows the scenarios of when autobackup is performed:

Pod operation	Autobackup performed
Update	No
Rollback	No
Commit	Yes
Update fail with auto rollback	No

After the successful creation of the autobackup folder, you can copy it to an external server for later restoration as mentioned in Restoring Management Node.

Management Node Migration

Management Node Migration: Baremetal to VM

With the advent of management node in VMs, Cisco VIM provides a second level of optimization for migrating the management node from baremetal (that is Layer 2 adjacent to the Cisco VIM pod) to VMs (that is Layer 3 adjacent to the Cisco VIM pod).

To get the migration, follow the below steps:

1. Use the standard steps to backup the management node preferably without the logs. For details, see Backing Up Management Node
2. SSH into the baremetal management node, and shut down all the services running on the management node only via the following:

```
# cd installer-XXXXX
# ./tools/mgmt/mgmt_node_teardown.sh
```

3. Launch the central management VM in the Cisco VIM cloud. For more details, see Centralizing Management Node
4. Restore the snapshot onto the management node VM. For more details, see Restoring Management Node
5. Continue using the VM based management node for any new pod management operation.

Backing Up UM Node

Backing Up Unified Management (UM) Node

Overview

The UM node hosts critical services such as certificates, mariadb, and so on for the UI solution of Cisco VIM. As the UM node is not redundant, ensure that you take the backup of the same. This way if the UM node goes through a non-recoverable failure, you can restore the UM node using the saved UM node information.

Backing up Cisco VIM UM

The administrator maintains the backup for UM on the management node. The UM backup is done only after the complete deployment of the UM bootstrap. Only two copies of the backup directory are maintained at the management node. The older copy is overwritten, when a next UM backup or autobackup takes place.

UM backup is stored at the default backup location */var/cisco/insight_backup/insight_backup_<release_tag><date><time>*.

For releases prior to Cisco VIM 3.4.5, if you want to take a backup of UM at a different location, use *-backupdir/-b* option from bootstrap_insight.

UM UI triggers an autobackup whenever it detects any operation related to MySQL database entry to preserve the latest state of UM.

> ⚠ UM backup is not allowed after an update. The update is an intermediate stage between rollback and commit. Any change relevant to MySQL database entry is not backed up, after an update from UM UI.

Autobackup UM

If there is a change, UM Installation automatically runs a daemon process to take the autobackup.
Get the live status of the process by checking the log located at */var/log/insight/insight_autobackup/insight_autobackup.logs* or *systemctl status insight-autobackup*.

> ⚠ A maximum of 10 log files of size 1024*1024 is maintained in the directory.

Following are the scenarios where autobackup is initiated:

Unified Management Operation	Auto-backup Performed
Adding or deleting pod	Yes
Changing pod REST password and certificate	Yes
Add/Edit/Delete all types of users	Yes
Add/Edit/Delete roles	Yes
Modify user and role association	Yes
Revoking or adding user permission	Yes
Log in or Logout	No
Context switching	No
Change user password	Yes

1. To check the status of UM, perform the following steps:

```
systemctl status insight-autobackup
insight-autobackup.service - Insight Autobackup Service
Loaded: loaded (/usr/lib/systemd/system/insight-autobackup.service; enabled; vendor preset:
disabled)
Active: active (running) since Wed 2017-08-30 01:17:18 PDT; 19s ago
Main PID: 19949 (python)
Memory: 12.4M
CGroup: /system.slice/insight-autobackup.service
19949 /usr/bin/python /root/<installer-tag>/insight/playbooks/../insight_autobackup.py
```

2. To stop UM autobackup, do the following:

```
systemctl stop insight-autobackup
insight-autobackup.service - Insight Autobackup Service
Loaded: loaded (/usr/lib/systemd/system/insight-autobackup.service; enabled; vendor preset:
disabled)
Active: inactive (dead) since Mon 2017-09-04 00:43:43 PDT; 5s ago
Process: 19993 ExecStop=/bin/kill ${MAINPID} (code=exited, status=0/SUCCESS)
Main PID: 19984
Memory: 56.0K
CGroup: /system.slice/insight-autobackup.service
```

3. To start UM autobackup, use the following command:

```
systemctl start insight-autobackup
insight-autobackup.service - Insight Autobackup Service
Loaded: loaded (/usr/lib/systemd/system/insight-autobackup.service; enabled; vendor preset:
disabled)
Active: active (running) since Wed 2017-08-30 01:17:18 PDT; 19s ago
Main PID: 19949 (python)
Memory: 12.4M
CGroup: /system.slice/insight-autobackup.service
19949 /usr/bin/python /root/<installer-tag>/insight/playbooks/../insight_autobackup.py
```

4. UM performs the following operations.
    a. Installation
        - Invokes the script when the Galera DB and UM containers are up.
        - Stores the log in */var/log/insight/insight_autobackup_logs/insight_autobackup.log*.
        - Notifies if the service is up or not with 10-seconds pulse.

        ```
        [2017-09-04 00:49:01,504] INFO [Insight Autobackup] Insight Autobackup Service Running.
        [2017-09-04 00:49:11,514] INFO [Insight Autobackup] Insight Autobackup Service Running.
        [2017-09-04 00:49:21,525] INFO [Insight Autobackup] Insight Autobackup Service Running.
        ```

        - If there is any change, it takes a backup (time to check if SQL difference is 30 seconds).
        - Creates *rbac_latest.sql* and *insight_latest.tar.gz* and dump in the latest backup directory.
        - During restore, the bootstrap script checks if *rbac_latest.sql* or *insight_latest.tar.gz* is present in the backup directory.
    b. Update
        - During the update, it does not support backup.
        - Terminates autobackup service and does not maintain a backup in the intermediate state.
    c. Rollback: Re-invokes the script from the previous workspace.
    d. Commit: Invokes the script again from the new workspace.
    e. Uninstall: Deletes the service files, but retains the log directory.

Backup UM at Default Backup Location

Launch an SSH session with Cisco UM node and follow the below steps:

1. For releases prior to Cisco VIM 3.4.5, execute the below commands:

```
# cd Insight-<tag_id>/insight
# ./bootstrap_insight.py -a backup
VIM Insight backup logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Cisco VIM Insight backup Info!
+----------------------+-------
```

```
+-------------------------------------------------------------------------------+
| Description               | Status|
Details                                                                        |
+----------------------+-------
+-------------------------------------------------------------------------------+
| Insight backup Status| PASS  | Backup done @ /var/cisco/insight_backup
/insight_backup_<release_tag>_<date_time>|
+----------------------+-------
+-------------------------------------------------------------------------------+
Done with VIM Insight backup!
```

2. For Cisco VIM 3.4.5, execute the following commands:

```
# cd Insight-<tag_id>/insight/backup_restore/
#./um_node_backup.py -h

Usage:  ./um_node_backup.py [options]
Options:
    -h, --help   show this help message and exit


# ./um_node_backup.py

2020-05-29 03:14:42 INFO     Backup Validation Passed
2020-05-29 03:14:42 INFO     Starting Cisco UM backup ...
2020-05-29 03:14:42 INFO     Cisco UM backup: estimated run time is approx. 30 mins...
2020-05-29 03:14:42 INFO     Please see backup progress log at /var/log/insight_backup
/insight_backup_<version>_<date>_<time>.log

2020-05-29 03:14:42 INFO     Cisco UM prebackup: executing prepbackup playbook ...
2020-05-29 03:14:45 INFO     Cisco UM backup: executing backup playbook ...
2020-05-29 03:15:00 INFO     Cisco UM states backed up /var/cisco/insight_backup
/insight_backup_<version>_<date>_<time>
2020-05-29 03:15:00 INFO     Executing Cisco UM postbackup .../var/cisco/insight_backup
/insight_backup_<version>_<date>_<time>
2020-05-29 03:15:00 INFO     Insight DB backed up ...
2020-05-29 03:15:06 INFO     Cisco UM backup completed: backupdir at /var/cisco/insight_backup
/insight_backup_<version>_<date>_<time>
```

From Cisco VIM 3.4.5, an optimization to reduce the backup size is available for connected installation. This reduces the overhead needed to copy the backup from the pod during restoration. However, ensure that the management node is connected to the registry during restoration to download the artifacts for which additional time is required.

Backup UM at User-defined Backup Location

Launch a SSH session with Cisco UM node only for releases earlier to Cisco VIM 3.4.5, and follow the below steps:

```
# cd Insight-<tag_id>/insight
# ./bootstrap_insight.py -a backup --backupdir <user_defined_path>
VIM Insight backup logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Cisco VIM Insight backup Info!
+----------------------+--------+-------------------------------------------------------------+
| Description          | Status | Details                                                     |
+----------------------+--------+-------------------------------------------------------------+
| Insight backup Status | PASS   | Backup done @ <user_defined_path>                          |
+----------------------+--------+-------------------------------------------------------------+
Done with VIM Insight backup!
```

Preserving Backup Directory at Remote Node

1. Copy the backup directory to a remote server using *rsync* to recover the Insight later. Cisco recommends you to copy backup directory using *rsync* as it preserves the permissions of the files.

   For example, to copy the backup directory to the remote server <*target_ip*>*:/var/cisco/insight_backup/directory*, execute the following command sequence:

   ⚠

For releases prior to Cisco VIM 3.4.5, the usage of below *rsync* command with *root* user for the remote node is strictly recommended. Do not use any *copy* command other than *rsync.*

```
# autobackup triggered as part of UM management operation
rsync -e ssh -go -rtvpX --numeric-ids /var/cisco/insight_backup/insight_backup_<version>_<date-time>
root@<remote_ip_address>:/var/cisco/insight_backup/

# manual backup triggered by admin
rsync -e ssh -go -rtvpX --numeric-ids /var/cisco/insight_backup/insight_backup_<version>_<date-time>
root@<remote_ip_address>:/var/cisco/insight_backup/

# scp command can also be used for remote copy (For CVIM 3.4.5 Release only)
scp -r /var/cisco/insight_backup/insight_backup_<version>_<date-time> <username>@<remote_ip_address>:/var
/cisco/insight_backup/
```

⚠ On the remote server, protect the backup directory from unauthorized access, as the backup files may contain sensitive information.

2. For Cisco VIM 3.4.5, change the directory to the location where the backup directory is copied on the remote server. In this example, */var/cisco /insight_backup/insight_backup_<version>_<date-time>/* . To verify whether the backup is not corrupted or modified*./check_integrity* and install the packages on the server where *check_integrity* is executed.

```
python-prettytable
python-jinja2
python-babel
python-markupsafe
python-setuptools
pytz
```

Restoring UM Node

Restoring Unified Management (UM) Node

You can restore the Cisco VIM UM to its previous running state that existed at the time of backup.

⚠ Ensure that you do not run the UM on the node on which restore operation is performed.

1. Reimage the UM node with the ISO version with which you want to restore the node, and with the same IP address that is used before the failure of the node.
2. Navigate to */var/cisco/insight_backup/* directory at the remote server where the backup directory is copied during backup.
3. Copy the backup directory to the */var/cisco/insight_backup/* directory of the re-imaged UM node. For example, to copy the backup directory from the remote host *<remote_ip>* to the management node */var/cisco/insight_backup/*directory, execute the following command sequence:

```
rsync -e ssh -go -rtvpX --numeric-ids <remote_username>@<remote_ip>:/var/cisco/insight_backup
/backup_2020-01-09_14-04-38 /var/cisco/insight_backup


Or
# scp command can also be used (For Cisco VIM 3.4.5 Release only)
# scp -r <remote_username>@<remote_ip>:/var/cisco/insight_backup/insight_backup_2020-01-09_14-04-38 /var
/cisco/insight_back
```

4. Start the restoration:

⚠
- It is highly recommended to use a KVM session instead of SSH for restoring the UM node.
- Ensure that you preserve the backup directory at the remote node until the entire process of restore is complete.

a. For releases prior to Cisco VIM 3.4.5:

i. Execute the following command in */var/cisco/insight_backup/backup_<date-time>* directory:

```
# ./insight_restore -h
insight_restore : Cisco VIM Insight Restore Script
-------------------------------------------------
Usage: ./insight_restore
-v : Enable verbose mode
-h : To display this help message
# ./insight_restore
This will initiate an Insight install with the backed up data.
VIM Insight restore logs are at: /var/log/insight/<bootstrap_insight_<date>_<time>.log
Management Node Validations!
+-------------------------------+--------+-------+
| Rule                                             | Status | Error |
+-------------------------------+--------+-------+
| Check Kernel Version                          | PASS   | None  |
| Check Docker Version                          | PASS          | None  |
| Check Management Node Tag                | PASS          | None  |
| Check Bond Intf. Settings          | PASS   | None  |
| Root Password Check                          | PASS   | None  |
| Check Boot Partition Settings | PASS   | None  |
| Check LV Swap Settings                 | PASS   | None  |
| Check Docker Pool Settings         | PASS   | None  |
| Check Home Dir Partition                | PASS   | None  |
| Check Root Dir Partition                 | PASS   | None  |
| Check /var Partition                        | PASS   | None  |
| Check LVM partition                     | PASS   | None  |
| Check RHEL Pkgs Install State | PASS   | None  |
+-------------------------------+--------+-------+
Insight standalone Input Validations!
+-----------------------------------------+--------+-------+
| Rule                                                                                |
Status | Error |
```

```
+-----------------------------------------+--------+-------+
| Insight standalone schema validation            | PASS         | None  |
| Valid key check in Insight Setup Data         | PASS          | None  |
| Duplicate key check In Insight Setup Data | PASS         | None  |
| CVIM/Insight workspace conflict check         | PASS   | None  |
| Check registry connectivity                                | PASS          | None  |
| Check Email server for Insight                    | PASS          | None  |
+-----------------------------------------+--------+-------+
Setting up Insight, Kindly wait!!!
Cisco VIM Insight Installed successfully!
+----------------------+----------------
+-------------------------------------------------------+
| Description                        | Status         |
Details
|
+----------------------+------------
+-----------------------------------------------------------+
| VIM Insight UI URL         | PASS                  | https://<br_api:
9000>                                                                |
| VIM UI Admin Email ID | PASS                  | Check for info @: <abs path of
insight_setup_data.yaml> |
|                                                 |
|
|
| VIM UI Admin Password | PASS                  | Check for info @ /opt/cisco/insight
/secrets.yaml            |
| VIM Insight Workspace | PASS                  | /root
/<insight_ws>                                                                        |
+-------------------+-------
+-------------------------------------------------------------------+
Cisco VIM Insight Autobackup Service Info!
+------------------------+--------+-------------------------------------------------+
| Description                          | Status |
Details                                                                 |
+------------------------+--------+-------------------------------------------------+
| VIM Insight Autobackup | PASS | [ACTIVE]: Running 'insight-autobackup.service'   |
+------------------------+--------+-------------------------------------------------+
VIM Insight restore successfully completed!
Done with VIM Insight restore!
VIM Insight restore logs are at: /var/log/insight/bootstrap_insight/
As the summary table describes, your VIM Insight workspace is restored and hence you need
to use
bootstrap_insight.py from the mentioned workspace for performing any actions from here on.
```

ii. Run the following command, to verify UM status after the restore operation.

```
# cd /root/Insight-<tag_id>/insight
# ./bootstrap_insight.py -a install-status
Cisco VIM Insight Install Status!
+----------------------+------------+-----------------------------------------------+
| Description                        | Status          |
Details                                                                  |
+----------------------+------------+-----------------------------------------------+
| VIM Insight Setup         | PASS                |
Success                                                                                |
| VIM Insight Version   | PASS       |
<release_tag>                                                                  |
| VIM Insight UI URL         | PASS                  | https://<br_api:
9000>                                                    |
| VIM Insight Container | PASS                |
insight_<tag_id>                                                       |
| VIM Mariadb Container | PASS                |
mariadb_<tag_id>                                                       |
| VIM Insight Autobackup| PASS                  | [ACTIVE]: Running 'insight-autobackup.
service'|
| VIM Insight Workspace | PASS                  | /root/installer-<tag_id>
/insight                          |
+----------------------+--------+-----------------------------------------------+
```

b. For Cisco VIM 3.4.5:

i. Navigate to the backup folder and execute the following command to verify if the backup is not corrupted or modified.

```
# cd /var/cisco/insight_backup/insight_backup_<date-time>
# ./check_integrity
```

ii. In */var/cisco/insight_backup/insight_backup_<date-time>* directory, execute the following command:

```
# ./restore -h

Usage of um_node_restore script
Options:
 -h --help
     Show this help text
 --verbose
     Set the logging level to debug



#./restore

Running System validation. May take time....
Restore Checksum Validation Passed
Restore Validation Passed
2020-05-29 05:04:15 INFO     Starting Cisco UM restore...
2020-05-29 05:04:15 INFO     Cisco UM restore: estimated run time is approx. 45 mins...
2020-05-29 05:04:15 INFO     Please see progress log for restore at /var/log/insight_restore
/insight_restore_2020-05-29_05:04:15.log
2020-05-29 05:04:15 INFO     Workspace restored to /root/insight-3.4.6
2020-05-29 05:04:15 INFO     Cisco UM restore: Executing restore playbook ...
2020-05-29 05:04:19 INFO     Executing UM node validation and orchestration step....
2020-05-29 05:14:25 INFO     Verifying UM install status..

Fetching Insight install status..


 Cisco VIM Insight Install Status!
+--------------------+--------+-----------------------------------------------+
| Description        | Status | Details                                       |
+--------------------+--------+-----------------------------------------------+
| Insight Setup      | PASS   | Success                                       |
| Insight Version    | PASS   | OG: 3.4.6                                     |
| Insight UI URL     | PASS   | https://<br_api>:9000                         |
| Mariadb Container  | PASS   | mariadb_26349                                 |
| Insight Container  | PASS   | insight_26349                                 |
| Insight Autobackup | PASS   | [ACTIVE]: Running 'insight-autobackup.service' |
+--------------------+--------+-----------------------------------------------+

[WARNING]: UM Management node needs to be rebooted for following to take effect:
         * Updated core libraries and services.


2020-05-29 05:14:25 INFO     Completed Cisco UM Restore successfully ...
```

Managing Cisco VIM Software Hub

Managing Cisco VIM Software Hub

Cisco VIM Software Hub helps mitigate the need to ship USBs across different pods during Cisco VIM installation or update. To ensure the long-term viability of Cisco VIM Software Hub, it is designed to handle the following Day 2 scenarios:

Updating Cisco VIM Software Hub TLS Certificate and Registry Credentials

Before installing the release artifacts from the Cisco VIM Software Hub server, you must provide a valid TLS certificate and Cisco VIM Software Hub registry credentials in the sds_setup_data.yaml file. Taking into account the security policies of an organization, Cisco VIM Software Hub allows you to update the TLS certificate and registry credentials on the Cisco VIM Software Hub server as required.

1. Navigate to the last installed release workspace using the *ls –lrt* command.
2. Replace the TLS certificate in the *openstack-configs* directory.
3. Modify the credentials in the *sds_setup_data.yaml* file.
4. Run the following command for the changes to take effect:

```
# cd /root/cvim_sds-<last-tag> # directory of last installed release and execute the following command.
# ./sds_runner/runner.py
```

This operation validates the changes in the *sds_setup_data.yaml* file and new TLS certificate. It reconfigures the Cisco VIM Software Hub server components with this new information.

> ⚠ The Cisco VIM Software Hub registry credentials of the pods that rely on Cisco VIM Software Hub are also reconfigured.

Cisco VIM Software Hub Server Backup and Restore

Cisco VIM Software Hub triggers an autobackup operation when a new Cisco VIM release is installed on the Cisco VIM Software Hub server. It takes a backup of the relevant files from the Cisco VIM Software Hub server, and saves it in the following location on the Cisco VIM Software Hub server:

```
directory /var/cisco/autobackup_<tag>_<date-time>
```

Cisco VIM Software Hub maintains only the latest two backup directories. The older copy is overwritten when the next autobackup operation is triggered. If you want to use an older backup directory for a restore operation later, you need to save it to another location before it is overwritten. You can use the *rsync* or *scp* commands to save it to an RHEL7/CentOS based system which is external to the Cisco VIM Software Hub server.

Checking Integrity of Autobackup Files

You can use the script provided in the autobackup directory to check the integrity of the autobackup files after using the *rsync* or *scp* commands.

> ⓘ **Before you begin**
>
> Ensure that the following packages are installed on the backup server using yum:
>
> - python-prettytable
> - python-jinja2
> - python-babel
> - python-markupsafe
> - python-setuptools
> - pytz

1. Navigate to the autobackup directory.
2. Execute the following command to run the script:

```
# ./check_integrity
```

Restoring Cisco VIM Software Hub from Backup

An Cisco VIM Software Hub restore operation is done when the original Cisco VIM Software Hub server is being replaced by a new one.

1. Reimage the Cisco VIM Software Hub server with the ISO version with which you want to restore the node, and with the same IP address that is used before the failure of the node.
2. Navigate to the location where the backup directory is copied during the backup operation.
3. Verify the integrity of the backup files as described in Checking Integrity of Autobackup Files
4. Copy the backup file to the directory of the reimaged Cisco VIM Software Hub node.

   For example, you can copy the backup directory from the remote host 20.0.0.5 to the Cisco VIM Software Hub node directory */var/cisco/* as follows:

   ```
   rsync -e ssh -go -rtvpX --numeric-ids root@20.0.0.5:/var/cisco/autobackup_2017-01-09_14-04-38
    /var/cisco/
   ```

5. Navigate to the backup directory and execute the following command to verify if the backup is not corrupted or modified.
6. In the */var/cisco/autobackup_<tag>_<date-time>* directory, execute the following commands:

   ```
   # cd /var/cisco/backup_<date-time>
   # ./restore
   ```

   It may take about 45 minutes for the restore operation to complete.

   > Before restoring a backup directory, the restore script validates the backup directory. If the validation fails, the restore operation is interrupted and an error message is displayed. The restore script also verifies the latest backup directory in the Cisco VIM Software Hub Node. If defects are detected, you need to confirm whether you want to proceed with the restore operation.

   For example:

   ```
   2017-02-02 21:25:23 INFO Starting Cisco VIM restore...
   2017-02-02 21:25:23 INFO Cisco VIM restore: estimated run time is approx. 45 mins...
   2017-02-02 21:25:23 INFO Please see progress log for restore at
   /var/log/mercury/installer/restore_2017-02-02_21:25:23.log
   2017-02-02 21:25:27 ERROR Error: Backup id is not the one expected
   Error: Found hashID file only in controller(s): controller-2, controller-3 Management backup
   files are ok (as per controller-2)
   Management backup files are ok (as per controller-3)
   The management node changed after the last backup was stored. Do you still want to proceed restoring
   this management node? [Y/n] y
   2017-02-02 22:17:55 INFO Workspace restored to /root/installer-6518
   2017-02-02 22:17:55 INFO Cisco VIM restore: Executing restore playbook ...
   2017-02-02 22:18:47 INFO Cisco VIM restore: Executing bootstrap playbook ...
   ```

   > To continue the restore operation, you can press the *Enter* key or *Y* key. If you want to abort the restore operation, you need to press the *N* key.

   ```
   2017-02-02 21:25:23 INFO Starting Cisco VIM restore...
   2017-02-02 21:25:23 INFO Cisco VIM restore: estimated run time is approx. 45 mins...
   2017-02-02 21:25:23 INFO Please see progress log for restore at
   /var/log/mercury/installer/restore_2017-02-02_21:25:23.log
   2017-02-02 21:25:27 ERROR Error: Backup id is not the one expected
   Error: Found hashID file only in controller(s): controller-2, controller-3 Management backup
   files are ok (as per controller-2)
   Management backup files are ok (as per controller-3)
   The management node changed after the last backup was stored. Do you still want to proceed restoring
   this management node? [
   Y/n] n
   Aborting the restore operation as per user request
   ```

Resolving Low Disk Space

Installing releases on Cisco VIM Software Hub server is not allowed, if the free disk space is less than 20%. Hence, use a utility to remove docker images from the container registry running on the Cisco VIM Software Hub server. You can find the cleanup script at the following location:

```
/root/cvim_sds-<last-tag>/sds/registry_cleanup.py
```

Example of running the cleanup script:

```
# ./registry_cleanup.py -h
usage: registry_cleanup.py [-h] (--list | --delete DELETE | --unused_tags)
[-u USERNAME] [-p PASSWORD] [-r REGISTRY]
List/Delete image tags in the registry
optional arguments:
        -h, --help Show this help message and exit
        --list List Image Tags in Registry
        --delete DELETE Delete Images of provided tags from registry
        --unused_tags List unused Tags in SDS registry
        -u USERNAME, --username USERNAME
        Registry Username
        -p PASSWORD, --password PASSWORD
        Registry Password
        -r REGISTRY, --registry REGISTRY
        Registry URL
```

The cleanup script requires three mandatory parameters namely Registry URL, Registry username, and Registry password. The script supports the following three options:

- List Image Tags: The option lists all the images and corresponding tags present in the docker registry.
- Unused Tags: This option lists all the releases present on the Cisco VIM Software Hub server but not used by any Cisco VIM pod. By default, the pods are registered with the Cisco VIM Software Hub server. When a pod is installed, updated, roll backed, or upgraded, the release information is sent to Cisco VIM Software Hub. You can use this command to identify the releases that can be safely removed from the Cisco VIM Software Hub server.
- Delete Tags: You can specify the releases that you want to remove from the docker registry. The script removes these images and frees the disk space.

A sample snippet of the command template is listed below:

```
#./registry_cleanup.py -u <username> -p <password> -r https://<sds_domian_name>/ --list
#./registry_cleanup.py -u <username> -p <password> -r https://<sds_domian_name>/ --delete
3.2.0
```

Manually Updating Packages

Cisco VIM Software Hub installs the repositories within docker containers, so that all the packages to be installed are obtained from those repositories. These repositories are updated when you install a later version of Cisco VIM release on the Cisco VIM Software Hub server. Once the repositories are updated, all the packages except httpd package and its dependencies are updated. When httpd is updated, all downstream connections are disrupted and the Cisco VIM pod installation must be restarted. Hence, updating httpd is deferred.

To update httpd and its dependent packages, you can use the update script found in the tools directory. Ensure that you run this script during the maintenance phase so that none of the Cisco VIM pods are currently attempting to get artifacts from the Cisco VIM Software Hub server.
Run the following command to execute the update script:

```
# cd /root/cvim_sds-<last-tag> # directory of last installed release and execute the following command.
# ./update_httpd.sh
```

Troubleshooting

Troubleshooting

Cisco NFVI Node

Cisco NFVI Node

Displaying Cisco NFVI Node Names and IP Addresses

Complete the following steps to display the Cisco NFVI node names and IP addresses.

1. Log into the Cisco NFVI build node.
2. The openstack-configs/mercury_servers_info file displays the node name and the address as follows.

```
# more openstack-configs/mercury_servers_info Total nodes: 5
Controller nodes: 3
+------------------+--------------+--------------+--------------+-----------------+---------+
| Server           | CIMC                   | Management          | Provision         |
Tenant                   | Storage |
+------------------+--------------+--------------+--------------+-----------------+---------+
| test-c-control-1 | 10.10.223.13 | 10.11.223.22 | 10.11.223.22 | 169.254.133.102 | None         |
|                                  |                           |              |
|                 |         |
| test-c-control-3 | 10.10.223.9  | 10.11.223.23 | 10.11.223.23 | 169.254.133.103 | None         |
|                                  |              |
|                                |                                    |                 |
| test-c-control-2 | 10.10.223.10 | 10.11.223.24 | 10.11.223.24 | 169.254.133.104 | None         |
|                                  |                           |
|                                 |                                      |                    |
+------------------+--------------+--------------+--------------+-----------------+---------+
Compute nodes: 2
+------------------+--------------+--------------+--------------+-----------------+---------+
| Server                    | CIMC                   | Management          | Provision         |
Tenant                   | Storage |
+------------------+--------------+--------------+--------------+-----------------+---------+
| test-c-compute-1 | 10.10.223.11 | 10.11.223.25 | 10.11.223.25 | 169.254.133.105 | None         |
|                                  |                           |
|                                 |                                      |                 |
| test-c-compute-2 | 10.10.223.12 | 10.11.223.26 | 10.11.223.26 | 169.254.133.106 | None         |
|                                  |                           |
|                                 |                                      |                      |
+
```


During Cisco NFVI deployment, SSH public keys for each node are added to .../.ssh/authorized_keys. Hence, you can login from the build node into each of the Cisco NFVI nodes without passwords. For some reason, if you need account information, see the *openstack -configs/secrets.yaml* file on the build node.

Verifying Cisco NFVI Node Interface Configurations

Complete the following steps to verify the interface configuration of Cisco NFVI nodes:

1. SSH into the target node, for example, one of the Cisco VIM controllers:

```
[root@mgmt-node~]# ssh root@control-server-1
[root@control-server-1 ~]#
```

2. Enter the *ip a* command to get a list of all interfaces on the node:

```
[root@control-server-1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN link/loopback 00:00:00:00:00:00
```

```
brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
2: enp8s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000 link/ether
54:a2:74:7d:42:1d brd ff:ff:ff:ff:ff:ff
3: enp9s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000 link/ether
54:a2:74:7d:42:1e brd ff:ff:ff:ff:ff:ff
```

Displaying Cisco NFVI Node Network Configuration Files

Complete the following steps to view the Cisco NFVI node network configuration files:

1. SSH into the target node, for example, one of the Cisco VIM controllers:

```
[root@mgmt-node~]# ssh root@control-server-1
[root@control-server-1 ~]#
```

2. List all the network configuration files in the */etc/sysconfig/network-scripts* directory, for example:

```
[root@control-server-1 ~]# ls /etc/sysconfig/network-scripts/
ifcfg-a                 ifcfg-enp15s0                ifcfg-mx0                ifdown-
ib                ifup                        ifup-ppp
ifcfg-a0                ifcfg-enp16s0                ifcfg-mx1                ifdown-ippp
ifup-aliases         ifup-routes
ifcfg-a1                ifcfg-enp17s0                ifcfg-p                ifdown-ipv6         ifup-
bnep                ifup-sit
ifcfg-br_api         ifcfg-enp18s0                ifcfg-p0                ifdown-isdn         ifup-
eth                ifup-Team
ifcfg-br_mgmt         ifcfg-enp19s0                ifcfg-p1                ifdown-post         ifup-
ib                ifup-TeamPort
ifcfg-e                 ifcfg-enp20s0                ifcfg-t                ifdown-ppp
ifup-ippp                ifup-tunnel
ifcfg-e0                ifcfg-enp21s0                ifcfg-t0                ifdown-routes
ifup-ipv6                ifup-wireless
ifcfg-e1                ifcfg-enp8s0                ifcfg-t1                ifdown-
sit                ifup-isdn                init.ipv6-global
ifcfg-enp12s0         ifcfg-enp9s0                ifdown                        ifdown-Team
ifup-plip                network-functions
ifcfg-enp13s0         ifcfg-lo                        ifdown-bnep         ifdown-TeamPort ifup-
plusb                network-functions-ipv6
ifcfg-enp14s0         ifcfg-mx                        ifdown-eth                ifdown-tunnel
ifup-post
```

Viewing Cisco NFVI Node Interface Bond Configuration Files

Complete the following steps to view the Cisco NFVI node interface bond configuration files:

1. SSH into the target node, for example, one of the Cisco VIM controllers:

```
[root@mgmt-node~]# ssh root@control-server-1
[root@control-server-1 ~]#
```

2. List all of the network bond configuration files in the */proc/net/bonding/* directory:

```
[root@control-server-1 ~]# ls
/proc/net/bonding/ a bond0 e mx p t
```

3. To view more information about a particular bond configuration, enter:

```
[root@control-server-1 ~]# more /proc/net/bonding/a
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)
Bonding Mode: load balancing (xor)
Transmit Hash Policy: layer3+4 (1)
```

```
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
```

Viewing Cisco NFVI Node Route Information

Complete the following steps to view Cisco NFVI node route information. Note that this is not the HAProxy container running on the controller. The default gateway must point to the gateway on the management network using the br_mgmt bridge.

1. SSH into the target node, for example, one of the Cisco VIM controllers:

```
[root@mgmt-node~]# ssh root@control-server-1
[root@control-server-1 ~]#
```

2. View the routing table (default gateway) of the Cisco NFVI node:

```
server-1 ~]# route -n
Kernel IP routing table
Destination                 Gateway                 Genmask                 Flags         Metric
Ref                 Use Iface
0.0.0.0                         10.23.221.33         0.0.0.0                 UG
0          0                                  0 br_mgmt
10.23.221.32                 0.0.0.0                 255.255.255.240 U                 0
0                               0 br_mgmt
17.16.3.0                       0.0.0.0                 255.255.255.0         U
0          0                                  0 t
169.254.0.0                 0.0.0.0                 255.255.0.0         U
1016          0                                  0 br_api
169.254.0.0                 0.0.0.0                 255.255.0.0         U                 1017
0                            0 e
169.254.0.0                    0.0.0.0                 255.255.0.0         U
1019          0                                  0 br_mgmt
169.254.0.0                 0.0.0.0                 255.255.0.0         U
1020          0                                  0 p
169.254.0.0                 0.0.0.0                 255.255.0.0         U
1021          0                                  0 t
172.17.0.0                        0.0.0.0                 255.255.0.0         U
0          0                                  0 docker0
```

Viewing Linux Network Namespace Route Information

Complete the following steps to view the route information of the Linux network namespace that the HAProxy container uses on a Cisco NFVI controller node. The default gateway must point to the gateway on the API network, using the API interface in the Linux network namespace.

1. SSH into the target node, for example, one of the Cisco VIM controllers:

```
[root@mgmt-node~]# ssh root@control-server-1
[root@control-server-1 ~]#
```

2. Enter the *ip netns* command to find the name of the network namespace:

```
[root@control-server-2 ~]# ip netns 17550 (id: 0)
```

3. Enter the *ip netns exec* command to view the routing table (default gateway) of the Linux network namespace:

```
[root@control-server-2 ~]# ip netns exec 17550 route -n
Kernel IP routing table
Destination                 Gateway                 Genmask                 Flags         Metric
Ref                 Use Iface
0.0.0.0                         172.29.86.1         0.0.0.0                 UG
0                 0                          0 api
10.23.221.32                 0.0.0.0                 255.255.255.240 U                 0
```

```
0                       0 mgmt
172.29.86.                      0 0.0.0.0               255.255.255.0         U
0               0                       0 api
```

Pre-checks for Storage Removal

Pre-checks for Storage Removal

Upon completion of the pod management operations like add-storage, ensure that any subsequent operation such as remove-storage is done on the same storage node after accounting for all of the devices and their corresponding OSDs have been marked in the persistent crush map as shown in the output of the ceph osd crush tree.

Execute the following command on the storage node where a remove-storage pod operation is performed to get a list of all the devices configured for ceph osds:

```
[root@storage-3 ~]$ df | grep -oh ceph-[0-9]*
[root@storage-3 ~]$ df | grep -oh ceph-[0-9]*
ceph-1
ceph-5
ceph-7
ceph-10
```

Login to any of the controller nodes and run the following commands within the ceph mon container:

```
$ cephmon
$ ceph osd crush tree
```

From the json output, locate the storage node to be removed and ensure that all the devices listed for ceph osds have corresponding osd entries for them by running the following commands:

```
        {
                                        "id": -3,
                                        "name": "storage-3",
                                        "type": "host",
                                        "type_id": 1,
                                        "items": [
                                                {
                                                        "id": 1,
                                                        "name": "osd.1",
                                                        "type": "osd",
                                                        "type_id": 0,
                                                        "crush_weight": 1.091095,
                                                        "depth": 2
                                                },
                                                {
                                                        "id": 5,
                                                        "name": "osd.5",
                                                        "type": "osd",
                                                        "type_id": 0,
                                                        "crush_weight": 1.091095,
                                                        "depth": 2
                                                },
                                                {
                                                        "id": 7,
                                                        "name": "osd.7",
                                                        "type": "osd",
                                                        "type_id": 0,
                                                        "crush_weight": 1.091095,
                                                        "depth": 2
                                                },
                                                {
                                                        "id": 10,
                                                        "name": "osd.10",
                                                        "type": "osd",
                                                        "type_id": 0,
                                                        "crush_weight": 1.091095,
                                                        "depth": 2
                                                }
                                        ]
                                },
```

⚠ If ToR_TYPE is Cisco NCS 5500, you must manually remove all the sub-interfaces that were manually configured on the NCS switch, as Cisco VIM automation does not unconfigure/configure the sub-interfaces for which the VLANs were not defined in the *setup_data.yaml*. If manual removal of sub-interface is not done, remove-compute operation is initiated.

General Troubleshooting Procedures

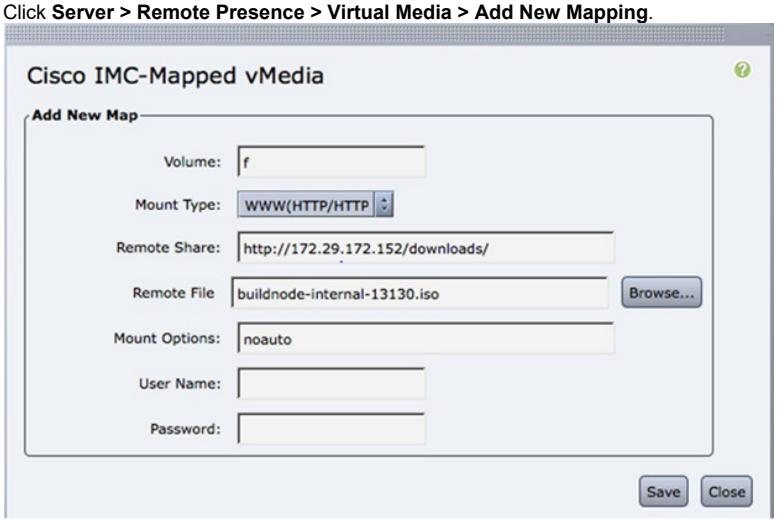
General Troubleshooting Procedures

Managing CIMC and ISO Installation

When you are remote, it is good to map the ISO through the CIMC Mapped vMedia.

To add new mapping:

1. Click **Server > Remote Presence > Virtual Media > Add New Mapping**.

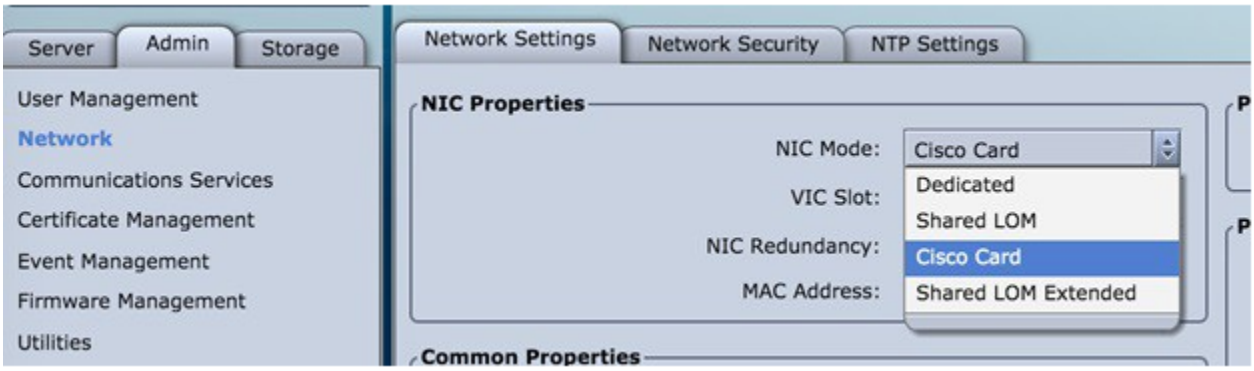


2. Enter the **Volume**, **Mount Type**, **Remote Share**, **Remote File**, **User name**, and **Password**.
3. Click **Save**. The CIMC pulls the ISO directly from the HTTP server.

Management Node Installation Failure

The management node installation fails, if the CIMC is configured for Cisco Card mode.

Choose the dedicated mode in the following screen:

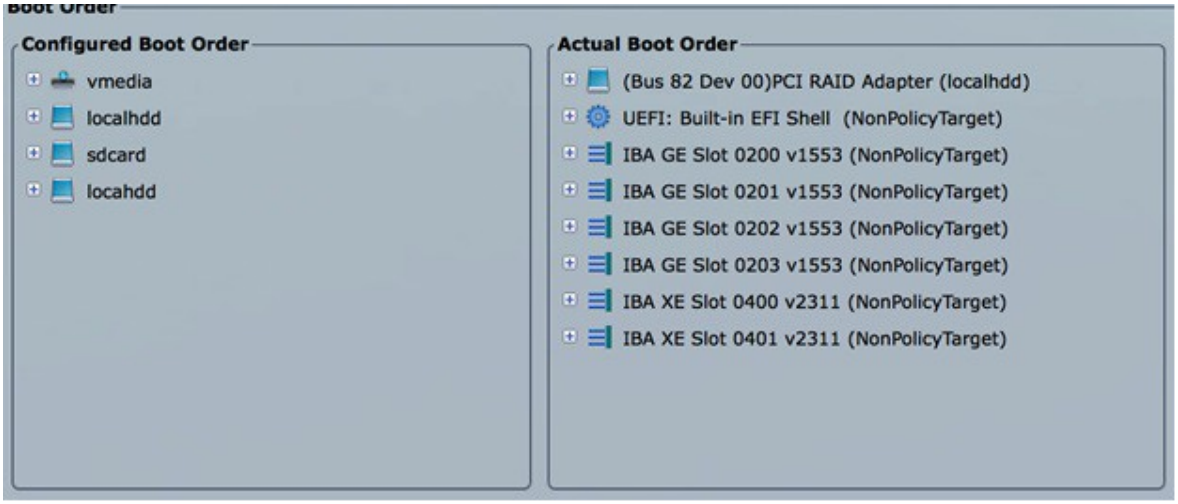


The selected method that is shown in the preceding screen is the incorrect mode.

Configuring Boot Order

The management node does not come up post reboot. It must boot from hard drive to check for the actual boot order.

Choose **Server > BIOS > Configure Boot Order > Boot Order**.



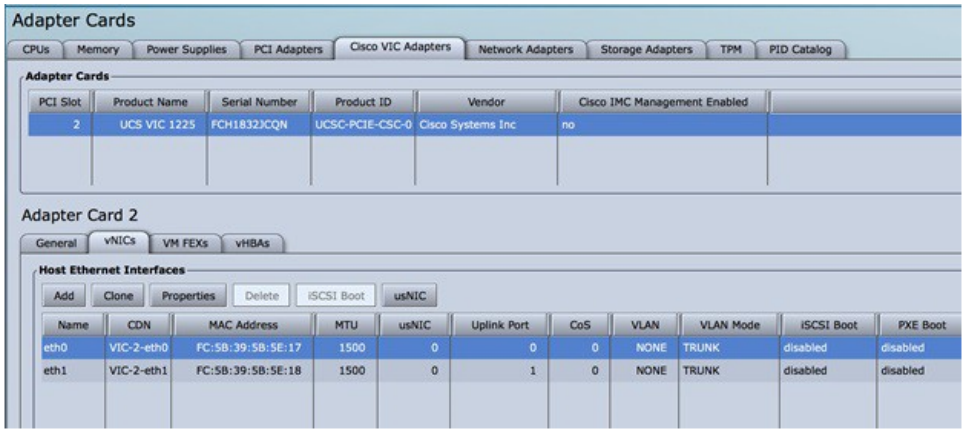
PXE Failure Issue During Baremetal Step

Perform the following steps in case of PXE boot failure:

1. Check the log file */var/log/mercury/mercury_baremetal_install.log* and connect to failing node CIMC KVM console to find out more on PXE boot failure reason.
2. Ensure all validations (step 1) and hardware validations (step 3) pass.
3. Check log file */var/log/mercury/<UUID>/mercury_baremetal_install.log*.
4. Connect to KVM console of failing node(s), to find out more on PXE boot failure.
5. Check L2/L3 network connectivity between failing node(s) and management node.
6. Check for VPC configuration and port-channel status of failing node(s) and ensure *no lacp suspend-individual* is configured on the port-channel.
7. Check if the actual PXE boot order does not differ from the boot-order configured.
8. Perform tcpdump on the management node interface br_mgmt, to watch for UDP port 67 (dhcp) or UDP pot 69 (tftp) tcpdump -I br_mgmt port 67 or port 69 # on the management node.
9. Perform tcpdump on the management node management interfacebr_mgmt on TCP 80 tcpdump -I br_mgmt port 80 # on the management node.
10. Check the apache log to watch the management IP address of failing node (if static allocated) tail *-f/var/log/cobblerhttpd/access_log* # on the management node.
11. For authorization required error messages during bare metal (Step 4) with CIMC operations such as hardware validations or cleaning up vNIC, check whether the maximum allowed simultaneous connection (4) are in use.

    All four connections are run when the third-party application monitoring CIMC does not properly close CIMC. This makes Cisco VIM installer not to login using xmlapi with valid username and password. Check Cisco IMC logs on CIMC (**Server > Faults and Logs > Cisco IMC Logs**) to know the reason for which the user is denied the access (maximum session, incorrect credentials). The workaround is to disable third-party monitoring, wait at least 10 minutes and then perform Cisco VIM operations.
12. In case none of the nodes are getting DHCP address, DHCP requests arrive at the management node without giving any response. To check CIMC VIC adapter settings, choose **Server > Inventory > Cisco VIC Adapters > vNICs | VLAN & VLAN** mode. Ensure that the VLANs (both id and mode) configured does not match with that of N9K switch.

Option	Description
CIMC	Trunk : None
Switch	Access : vlan_mgmt



Connecting to Docker Container

To connect to the docker container, do the following:

```
# generally, aliases are created for all containers
# use alias to identify those
alias | grep in_container
# checking specific alias by name alias cobbler

# check docker containers
# alias created by CVIM
dp
# list docker containers
docker ps -a
# list docker images
docker images

# connecting to container
docker exec -it my_cobbler_<tag_id> /bin/bash

# connecting to docker container as privileged user
docker exec -it -u root my_cobbler_<tag_id> /bin/bash

# systemctl files
systemctl -a | egrep "docker-.*.service"

# check specific service
systemctl status mercury-restapi -l
systemctl status docker-vmtp

# restart specific service
systemctl restart docker-vmtp
```

Connection/Installation Problems

Connection/Installation Problems

Container Download Problems

- Check installer logs log file */var/log/mercury/mercury_buildorchestration.log* for any build node orchestration failures including stuck *registry-populate local registry*. Downloading the Docker container from your management node can be slow.
- Check the network connectivity between the management node and the remote registry in *defaults.yaml* on the management node (*grep "^registry:" openstack-configs/defaults.yaml*).
- Verify if the valid remote registry credentials are defined in *setup_data.yaml* file.
- A proxy server is required to pull the container images from remote registry. If a proxy is required, exclude all IP addresses for your setup including management node.

Cisco IMC Connection Problems during Bare Metal Installation

The cause may be Cisco IMC has too many connections, so the installer cannot connect to it. Clear the connections by logging into your Cisco IMC, selecting the **Admin>Sessions** tab and clearing the connections.

API VIP Connection Problems

Verify if the active HAProxy container is running in one of the controller nodes. On that controller within the HAProxy container namespace, verify whether the IP address is assigned to the API interface. Also, verify whether your ToR and the network infrastructure connecting your ToR are provisioned with API network segment VLAN.

HAProxy Services Downtime after Initial Installation or HA Failover

The HAProxy web interface is accessible on TCP port 1936.

```
http://<external_lb_vip_address>:1936/
Username: haproxy
Password: <HAPROXY_PASSWORD> from secrets.yaml file
```

After initial installation, the HAProxy web interface can report to several OpenStack services with downtime depending on when that OpenStack service is installed after HAProxy installation. The counters are not synchronized between HAProxy active and standby. After HA proxy failover, the downtime timers vary based on the uptime of new active HAproxy container.

Management Node Problems

Service Commands

To identify all the services that are running, enter:

```
$ systemctl -a | grep docker | grep service
On controller ignore status of:
docker-neutronlb
On compute ignore status of:
docker-neutronlb, docker-keystone
```

To start a service on a host, enter:

```
$ systemctl start <service_name>
```

To stop a service on a host, enter:

```
$ systemctl stop <service_name>
```

To restart a service on a host, enter:

```
$ systemctl restart <service_name>
```

To check service status on a host, enter:

```
$ systemctl status <service_name>
```

Management Node Recovery Scenarios

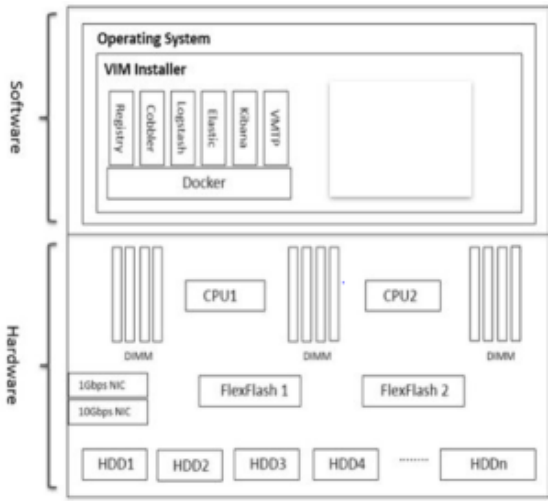
Management Node Recovery Scenarios

Management Node Architecture

The Cisco NFVI management node hosts the Cisco VIM Rest API service, Cobbler for PXE services, ELK for Logging to Kibana dashboard services, and VMTP for cloud validation. As the maintenance node does not have redundancy, understanding its point of failure and recovery scenarios are important. Managing node recovery scenarios are described in the following steps.

The management node architecture includes a Cisco UCS C240 M4 server with dual CPU socket. It has a 1-Gbps on-board (LOM) NIC and a 10-Gbps Cisco VIC mLOM. HDDs are used in 8,16, or 24 disk configurations.

The following figure shows the high-level maintenance node of the hardware and software architecture.



Different management node hardware or software failures can cause Cisco NFVI service disruptions and outages. Some failed services can be recovered through manual intervention. In cases if the system is operational during a failure, double faults cannot be recoverable.

The following table lists the management node failure scenarios and their recovery options.

Scenario #	Failure or Trigger	Recoverable	Operational Impact
1	Failure of 1 or 2 active HDD	Yes	No
2	Simultaneous failure of more than 2 active HDD	No	Yes
3	Spare HDD failure: 4 spare for 24 HDD; or 2 spare for 8 HDD	Yes	No
4	Power outage/hard reboot	Yes	Yes
5	Graceful reboot	Yes	Yes
6	Docker daemon start failure	Yes	Yes

7	Service container (Cobbler, ELK) start failure	Yes	Yes
8	One link failure on bond interface	Yes	No
9	Two link failures on bond interface	Yes	Yes
10	REST API service failure	Yes	No
11	Graceful reboot with Cisco VIM Unified Management	Yes	Yes. CLI alternatives exist during reboot.
12	Power outage or hard reboot with Cisco VIM Unified Management	Yes	Yes
13	VIM Unified Management Container reinstallation	Yes	Yes. CLI alternatives exist during reinstall.
14	Cisco VIM Unified Management Container reboot	Yes	Yes. CLI alternatives exist during reboot.
15	Intel 1350 1Gbps LOM failure	Yes	Yes
16	Cisco VIC 1227 10-Gbps mLOM failure	Yes	Yes
17	DIMM memory failure	Yes	No
18	One CPU failure	Yes	No

Scenario 1: Failure of One or Two Active HDDs

The management node uses 8,16, or 24-HDDs. The HDDs are configured with RAID 6, to enable data redundancy and storage performance and to overcome any unforeseen HDD failures.

- When 8 HDDs are installed, 7 are active disks and one is spare disk.
- When 16 HDDs are installed, 14 are active disks and two are spare disks.
- When 24 HDDs are installed, 20 are active disks and four are spare disks.

With RAID 6 up, two simultaneous active HDD failures can occur. When an HDD fails, the system begins automatic recovery by moving the spare disk to active state and rebuilding the new active HDD. It takes approximately 4 hours to rebuild the new disk and move to synchronized state. During this operation, the system is fully functional without causing any impact. However, you must monitor the system to ensure that more failures do not occur to enter into a double fault situation.

You can use the *storcli* commands to check the disk and RAID state as shown in the following commands:

Make sure that the node is running with hardware RAID by checking the *storcli* output and comparing to the one preceding.

```
[root@mgmt-node ~]# /opt/MegaRAID/storcli/storcli64 /c0 show
<...snip...>
TOPOLOGY:
========
-----------------------------------------------------------------------------
DG Arr Row EID:Slot DID Type State BT                Size         PDC         PI SED         DS3
FSpace TR
-----------------------------------------------------------------------------
0         -         -         -                  -         RAID6 Optl         N           4.087 TB  dflt
N         N         dflt         N                  N
0         0         -          -      -          RAID6 Optl         N           4.087 TB  dflt         N
N         dflt         N                 N <== RAID
6 in optimal state
0         0         0         252:1         1         DRIVE Onln         N         837.258 GB  dflt
N         N         dflt         -                  N
0         0         1         252:2         2         DRIVE Onln         N         837.258 GB  dflt
N         N         dflt         -                  N
0         0         2         252:3         3         DRIVE Onln         N         930.390 GB  dflt
N         N         dflt         -                  N
0         0         3         252:4         4         DRIVE Onln         N         930.390 GB  dflt
N         N         dflt         -                  N
0         0         4         252:5         5         DRIVE Onln         N         930.390 GB  dflt
N         N         dflt         -                  N
0         0         5         252:6         6         DRIVE Onln         N         930.390 GB  dflt
N         N         dflt         -                  N
0         0         6         252:7         7         DRIVE Onln         N         930.390 GB  dflt
N         N         dflt         -                  N
0         -         -         252:8         8         DRIVE DHS          -         930.390 GB   -
-         -          -           -                  N
-----------------------------------------------------------------------------
<...snip...>
PD LIST:
=======
```

```
---------------------------------------------------------------------------
EID:Slt DID State         DG                Size         Intf         Med         SED PI         SeSz
Model                 Sp
---------------------------------------------------------------------------
252:1         1         Onln         0         837.258 GB         SAS         HDD         N         N
512B ST900MM0006  U <== all disks
functioning
252:2         2         Onln         0         837.258 GB         SAS         HDD         N         N
512B ST900MM0006  U
252:3         3         Onln         0         930.390 GB         SAS                HDD         N
N         512B ST91000640SS U
252:4         4         Onln         0         930.390 GB         SAS                HDD         N
N         512B ST91000640SS U
252:5         5         Onln         0         930.390 GB         SAS         HDD         N         N
512B ST91000640SS U
252:6         6         Onln         0         930.390 GB         SAS                HDD         N
N         512B ST91000640SS U
252:7         7         Onln         0         930.390 GB         SAS                HDD         N
N         512B ST91000640SS U
252:8         8         DHS          0         930.390 GB         SAS         HDD         N         N
512B ST91000640SS D
---------------------------------------------------------------------------
[root@mgmt-node ~]# /opt/MegaRAID/storcli/storcli64 /c0 show
<...snip...>
TOPOLOGY :
========
-----------------------------------------------------------------------------------
DG         Arr Row EID:Slot DID         Type State BT                 Size         PDC          PI SED
DS3         FSpace TR
-----------------------------------------------------------------------------------
0         -         -         -                 -                 RAID6 Pdgd N         4.087 TB
dflt         N         N dflt         N                 N <== RAID 6
in degraded state
0         0         -         -                 -                 RAID6 Dgrd N         4.087 TB
dflt         N         N dflt         N                 N
0         0         0         252:8         8                 DRIVE Rbld Y         930.390 GB
dflt         N         N dflt         -                 N
0         0         1         252:2         2                 DRIVE Onln N         837.258 GB
dflt         N         N dflt         -                 N
0         0         2         252:3         3                 DRIVE Onln N         930.390 GB
dflt         N         N dflt         -                 N
0         0         3         252:4         4                 DRIVE Onln N         930.390 GB
dflt         N         N dflt         -                 N
0         0         4         252:5         5                 DRIVE Onln N         930.390 GB
dflt         N         N dflt         -                 N
0         0         5         252:6         6                 DRIVE Onln N         930.390 GB
dflt         N         N dflt         -                 N
0         0         6         252:7         7                 DRIVE Onln N         930.390 GB
dflt         N         N dflt         -                 N
-----------------------------------------------------------------------------------
<...snip...>
PD LIST :
=======
---------------------------------------------------------------------------
EID:Slt         DID State         DG                Size                Intf         Med SED PI SeSz
Model                 Sp
---------------------------------------------------------------------------
252:1                 1         UGood         -         837.258 GB                SAS         HDD N         N
512B ST900MM0006         U <== active disk
in slot 1 disconnected from drive group 0
252:2                 2         Onln         0         837.258 GB                SAS         HDD N         N
512B ST900MM0006         U
252:3                 3         Onln         0         930.390 GB                SAS         HDD N         N
512B ST91000640SS U
252:4                 4         Onln         0         930.390 GB                SAS         HDD N         N
512B ST91000640SS U
252:5                 5         Onln         0         930.390 GB                SAS         HDD N         N
512B ST91000640SS U
252:6                 6         Onln         0        930.390 GB                SAS         HDD N         N
512B ST91000640SS U
252:7                 7         Onln         0        930.390 GB                SAS         HDD N         N
```

```
512B ST91000640SS U
252:8                8         Rbld         0         930.390 GB                SAS         HDD N         N
512B ST91000640SS U <== spare disk
in slot 8 joined drive group 0 and in rebuilding state
-------------------------------------------------------------------------------
[root@mgmt-node ~]# /opt/MegaRAID/storcli/storcli64 /c0/e252/s8 show rebuild
Controller = 0
Status = Success
Description = Show Drive Rebuild Status Succeeded.
------------------------------------------------------------
Drive-ID                Progress%                Status         Estimated Time Left
------------------------------------------------------------
/c0/e252/s8                   20         In progress 2 Hours   28 Minutes <== spare disk in slot 8 rebuild
status
------------------------------------------------------------
```

To replace the failed disk and add it back as a spare:

```
[root@mgmt-node ~]# /opt/MegaRAID/storcli/storcli64 /c0/e252/s1 add hotsparedrive dg=0
Controller = 0
Status = Success
Description = Add Hot Spare Succeeded.
[root@mgmt-node ~]# /opt/MegaRAID/storcli/storcli64 /c0 show
<...snip...>
TOPOLOGY :
========
-----------------------------------------------------------------------------------
DG Arr Row         EID:Slot         DID Type State BT                 Size         PDC PI SED DS3
FSpace         TR
-----------------------------------------------------------------------------------
0         -         -         -                           -         RAID6 Pdgd N           4.087 TB dflt
N         N dflt         N                N
0         0         -         -                           -         RAID6 Dgrd N           4.087 TB dflt
N         N dflt         N                N
0        0         0         252:8                8         DRIVE Rbld Y         930.390 GB dflt N         N
dflt         -                 N
0         0         1         252:2                2         DRIVE Onln N         837.258 GB dflt N         N
dflt         -                 N
0         0         2         252:3                3         DRIVE Onln N         930.390 GB dflt N         N
dflt         -                 N
0         0         3         252:4                4         DRIVE Onln N         930.390 GB dflt N         N
dflt         -                 N
0         0         4         252:5                5         DRIVE Onln N         930.390 GB dflt N         N
dflt         -                 N
0         0         5         252:6                6         DRIVE Onln N         930.390 GB dflt N         N
dflt         -                 N
0         0         6         252:7                7         DRIVE Onln N         930.390 GB dflt N         N
dflt         -                 N
0         -         -         252:1                1         DRIVE DHS  -         837.258 GB         -
-         -         -         -                 N
-----------------------------------------------------------------------------------
<...snip...>
PD LIST :
=======
-------------------------------------------------------------------------------
EID:Slt DID State         DG                Size         Intf         Med SED PI         SeSz
Model                         Sp
-------------------------------------------------------------------------------
252:1         1         DHS         0         837.258 GB         SAS         HDD N         N         512B
ST900MM0006         U <== replacement
disk added back as spare
252:2         2         Onln         0         837.258 GB         SAS         HDD N         N         512B
ST900MM0006         U
252:3         3         Onln         0         930.390 GB         SAS         HDD N         N         512B
ST91000640SS         U
252:4         4         Onln         0         930.390 GB         SAS         HDD N         N         512B
ST91000640SS         U
252:5         5         Onln         0         930.390 GB         SAS         HDD N         N         512B
ST91000640SS         U
252:6         6         Onln         0         930.390 GB         SAS         HDD N         N         512B
```

```
ST91000640SS         U
252:7         7         Onln         0         930.390 GB         SAS         HDD N         N         512B
ST91000640SS         U
252:8         8         Rbld         0         930.390 GB         SAS         HDD N         N         512B
ST91000640SS         U
------------------------------------------------------------------------------
```

Scenario 2: Simultaneous Failure of More than Two Active HDDs

If more than two HDD failures occur at the same time, the management node goes into an unrecoverable failure state because RAID 6 allows for recovery of up to two simultaneous HDD failures. To recover the management node, reinstall the operating system.

Scenario 3: Spare HDD Failure

When the management node has 24 HDDs, four are designated as spares. Failure of any of the disks does not impact the RAID or system functionality. Cisco recommends replacing these disks when they fail (see the steps in Scenario 1) to serve as standby disks and so when an active disk fails, an auto-rebuild is triggered.

Scenario 4: Power Outage or Reboot

If a power outage or hard system reboot occurs, the system boots up, and come back to operational state. Services running on the management node during down time gets disrupted. See the steps in Scenario 9 for the list of commands to check the services status after recovery.

Scenario 5: System Reboot

If a graceful system reboot occurs, the system boots up and come back to operational state. Services running on the management node during down time gets disrupted. See the steps in Scenario 9 for the list of commands to check the services status after recovery.

Scenario 6: Docker Daemon Start Failure

The management node runs the services using Docker containers. If the Docker daemon fails to come up, it causes services such as ELK, Cobbler, and VMTP to go into down state. You can use the *systemctl* command to check the status of the Docker daemon, for example:

```
# systemctl status docker
docker.service - Docker Application Container Engine
Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2016-08-22 00:33:43 CEST; 21h ago
Docs: http://docs.docker.com
Main PID: 16728 (docker)
```

If the Docker daemon is in down state, use the *systemctl restart docker* command to restart the Docker service. Run the commands that are listed in Scenario 9 to verify that all the Docker services are active.

Scenario 7: Service Container (Cobbler, ELK) Start Failure

As described in Scenario 8, all the services run as Docker containers on the management node. To find all services running as containers, use the *docker ps –a* command. If any services are in Exit state, use the *systemctl* command and grep for Docker to find the exact service name, for example:

```
# systemctl | grep docker- | awk '{print $1}'
docker-cobbler-tftp.service
docker-cobbler-web.service
docker-cobbler.service
docker-container-registry.service
docker-elasticsearch.service
docker-kibana.service
docker-logstash.service
docker-vmtp.service
```

If any services need restarting, use the *systemctl* command. For example, to restart a Kibana service:

```
# systemctl restart docker-kibana.service
```

Scenario 8: One link failure on the bond Interface

management node is set up with two different networks: br_api and br_mgmt. The br_api interface is the external. It is used for accessing outside services such as the Cisco VIM REST API, Kibana, and Cobbler. The br_mgmt interface is internal. It is used for provisioning and to provide management connectivity to all OpenStack nodes (control, compute and storage). Each network has two ports that are bonded to provide redundancy. If one port fails, the system remains completely functional through the other port. If a port fails, check for physical network connectivity, and remote switch configuration to debug the underlying cause of the link failure.

Scenario 9: Two Link Failures on the Bond Interface

As described in Scenario 10, each network is configured with two ports. If both ports are down, the system is not reachable and management node services could be disrupted. After the ports are back up, the system is fully operational. Check the physical network connectivity and the remote switch configuration to debug the underlying link failure cause.

Scenario 10: REST API Service Failure

The management node runs the REST API service for Cisco VIM clients to reach the server. If the REST service is down, Cisco VIM clients cannot reach the server to trigger any server operations. However, with the exception of the REST service, other management node services remain operational.

To verify the management node REST services are fully operational, use the following command to check that the httpd and mercury-restapi services are in active and running state:

```
# systemctl status httpd
httpd.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2016-08-22 00:22:10 CEST; 22h ago
# systemctl status mercury-restapi.service
mercury-restapi.service - Mercury Restapi
Loaded: loaded (/usr/lib/systemd/system/mercury-restapi.service; enabled; vendor preset:
disabled)
Active: active (running) since Mon 2016-08-22 00:20:18 CEST; 22h ago
```

A tool is also provided so that you can check the REST API server status and the location of the folder it is running from. To execute run the following command:

```
# cd installer-<tagid>/tools
#./restapi.py -a status
  Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h
  ago
     REST API launch directory:/root/installer-<tagid>/
```

Confirm the server status is active and check that the restapi launch folder matches the folder where the installation was launched. The restapi tool also provides the options to launch, tear down, and reset password for the restapi server as shown in the following command:

```
# ./restapi.py -h
usage: restapi.py [-h] --action ACTION [--yes] [--verbose]
REST API setup helper
optional arguments:
-h, --help                          show this help message and exit
--action ACTION, -a ACTION
                                         setup - Install and Start the REST API server.
                                         teardown - Stop and Uninstall the REST API
server.
                                         restart - Restart the REST API server.
                                         regenerate-password - Regenerate the password for
REST API server.
                                         reset-password - Reset the REST API password with
user given password.
                                         status - Check the status of the REST API server
--yes, -y                           Skip the dialog. Yes to the action.
--verbose, -v                 Perform the action in verbose mode.
```

If the REST API server is not running, execute *ciscovim* to show the following error message:

```
# cd installer-<tagid>/
# ciscovim -setupfile ~/Save/<setup_data.yaml> run
```

If the installer directory or the REST API state is not correct or points to an incorrect REST API launch directory, go to the installer-*<tagid>/tools* directory and execute:

```
# ./restapi.py -action setup
```

To confirm that the REST API server state and launch directory is correct run the following command:

```
# ./restapi.py -action status
```

Scenario 11: Graceful Reboot with Cisco VIM Unified Management

Cisco VIM Unified Management runs as a container on the management node. After a graceful reboot of the management node, the VIM Unified Management and its associated database containers comes up. So there is no impact on recovery.

Scenario 12: Power Outage or Hard Reboot With VIM Unified Management

The Cisco VIM Unified Management container comes up automatically following a power outage or hard reset of the management node.

Scenario 13: Cisco VIM Unified Management Reinstallation

If the management node which is running the Cisco VIM Unified Management fails and cannot come up, you must uninstall and reinstall the Cisco VIM UM. After the VM Unified Management container comes up, add the relevant bootstrap steps as listed in the install guide to register the pod. VIM Unified Management then automatically detects the installer status and reflects the present status appropriately.

To clean up and reinstall Cisco VIM UM run the following command:

```
# cd /root/installer-<tagid>/insight/
# ./bootstrap_insight.py -a uninstall -o standalone -f </root/insight_setup_data.yaml>
```

Scenario 14: VIM Unified Management Container reboot

On Reboot of the VIM Unified Management container, services continue to work as it is.

Scenario 15: Intel (I350) 1Gbps LOM failure

The management node is set up with an Intel (I350) 1-Gbps LOM for API connectivity. Two 1-Gbps ports are bonded to provide connectivity redundancy. No operational impact occurs if one of these ports goes down. However, if both ports fail, or the LOM network adapter fails, the system cannot be reached through the API IP address. If this occurs you must replace the server because the LOM is connected to the system motherboard. To recover the management node with a new server, complete the following steps. Make sure the new management node hardware profile, matches the existing server and the Cisco IMC IP address is assigned.

1. Shut down the existing management node.
2. Unplug the power from the existing and new management nodes.
3. Remove all HDDs from existing management node and install them in the same slots of the new management node.
4. Plug in the power to the new management node, but do not boot the node.
5. Verify the configured boot order is set to boot from local HDD.
6. Verify the Cisco NFVI management VLAN is configured on the Cisco VIC interfaces.
7. Boot the management node for the operating system to begin.After the management node is up, the management node bond interface is down due to the incorrect MAC address. It points to old node network card MAC address.
8. Update the MAC address under */etc/sysconfig/*network-scripts.
9. Reboot the management node. It is fully operational. All interfaces has to be in an up state and be reachable.
10. Verify that Kibana and Cobbler dashboards are accessible.
11. Verify the Rest API services are up. See Scenario 15 for any recovery steps.

Scenario 16: Cisco VIC 1227 10Gbps mLOM failure

The management node is configured with a Cisco VIC 1227 dual port 10-Gbps mLOM adapter for connectivity to the other Cisco NFVI nodes. Two 10 Gbps ports are bonded to provide connectivity redundancy. If one of the 10-Gbps ports goes down, no operational impact occurs. However, if both Cisco VIC 10 Gbps ports fail, the system goes into an unreachable state on the management network. If this occurs, you must replace the VIC network adapters. Otherwise pod management and the Fluentd forwarding service isdisrupted. If you replace a Cisco VIC, update the management and provisioning VLAN for the VIC interfaces using Cisco IMC and update the MAC address in the interfaces under */etc/sysconfig/network-scripts* interface configuration file.

Scenario 17: DIMM Memory Failure

The management node is set up with multiple DIMM memory across different slots. Failure of one or memory modules could cause the system to go into unstable state, depending on how many DIMM memory failures occur. DIMM memory failures are standard system failures like any other Linux system server. If a DIMM memory fails, replace the memory module(s) as soon as possible to keep the system in stable state.

Scenario 18: One CPU Failure

Cisco NFVI management nodes have dual core Intel CPUs (CPU1 and CPU2). If one CPU fails, the system remains operational. However, always replace failed CPU modules immediately. CPU failures are standard system failures such as any other Linux system server. If a CPU fails, replace it immediately to keep the system in stable state.

Compute Node Recovery Scenario

Compute Node Recovery Scenario

The Cisco NFVI compute node hosts the OpenStack services to provide processing, network, and storage resources to run instances. The node architecture includes a Cisco UCS C220 M4/M5 server with dual CPU socket, different NIC combinations, and SSD/HDDs in RAID 1 configuration. The steps below list the mechanism to recover from a failed HDD.

Failure of One Active HDD

With RAID 1, data are shown and allows up to one active HDD failure. When an HDD fails, the node is still functional with no impacts. However, the data are no longer illustrated and losing another HDD results in unrecoverable and operational downtime. The failed disk has to be replaced soon as it takes approximately 2 hours to rebuild the new disk and move to synchronized state.

To check the disk and RAID state, run the *storcli* commands as follows:

Make sure that the node is running with hardware RAID by checking the *storcli* output and comparing to the one that is shown in the following command.

```
[root@compute-node ~]# /opt/MegaRAID/storcli/storcli64 /c0 show
<...snip...>
TOPOLOGY :
========
-----------------------------------------------------------------------------
DG         Arr Row  EID:Slot   DID   Type  State BT         Size     PDC         PI SED DS3 FSpace TR
-----------------------------------------------------------------------------
0          -        -                 -            -      RAID1  Optl  N  837.258 GB dflt         N         N
dflt         N            N <== RAID 1 in
optimal state
0          0        -                 -            -      RAID1  Optl  N  837.258 GB dflt         N         N
dflt         N            N
0          0        0          252:2      9     DRIVE  Onln  N  837.258 GB dflt         N         N
dflt         -      N
0          0        1          252:3      11    DRIVE  Onln  N  837.258 GB dflt         N         N
dflt         -      N
-----------------------------------------------------------------------------
<...snip...>
Physical Drives = 2
PD LIST :
=======
-------------------------------------------------------------------------
EID:Slt         DID State DG                 Size         Intf Med         SED PI SeSz Model                 Sp
-------------------------------------------------------------------------
252:2                9         Onln   0  837.258 GB         SAS  HDD         N         N  512B ST900MM0006 U
<== all disks
functioning
252:3                11         Onln   0  837.258 GB         SAS  HDD         N         N  512B ST900MM0006 U
-------------------------------------------------------------------------
[root@compute-node ~]# /opt/MegaRAID/storcli/storcli64 /c0 show
<...snip...>

TOPOLOGY :
========
-----------------------------------------------------------------------------------------
DG Arr Row  EID:Slot         DID         Type         State         BT                Size         PDC PI SED
DS3 FSpace         TR
-----------------------------------------------------------------------------------------
0          -        -                 -                -                 RAID1         Dgrd         N
837.258 GB dflt  N  N dflt         N                N <== RAID 1 in
degraded state.
0          0        -                 -                -                 RAID1         Dgrd         N
837.258 GB dflt  N  N dflt         N                N
0          0        0                 -                -                 DRIVE         Msng         -
837.258 GB  -          -  -  -         -                N
0          0        1         252:3                11                DRIVE         Onln         N
837.258 GB dflt  N  N dflt         -                N
-----------------------------------------------------------------------------------------
<...snip...>
PD LIST :
```

```
=======
------------------------------------------------------------------------------
EID:Slt         DID         State         DG                 Size         Intf Med SED PI SeSz   Model    Sp
------------------------------------------------------------------------------
252:2                9                 UGood         -         837.258 GB  SAS  HDD  N  N  512B ST900MM0006 U
<== active disk
in slot 2 disconnected from drive group 0
252:3                11                 Onln         0         837.258 GB  SAS  HDD  N  N  512B ST900MM0006 U
------------------------------------------------------------------------------
```

To replace the failed disk and add it back as a spare, run the following command:

```
[root@compute-node ~]# /opt/MegaRAID/storcli/storcli64 /c0/e252/s2 add hotsparedrive dg=0
Controller = 0
Status = Success
Description = Add Hot Spare Succeeded.
[root@compute-node ~]# /opt/MegaRAID/storcli/storcli64 /c0 show
<...snip...>
TOPOLOGY :
========
------------------------------------------------------------------------------
DG         Arr Row   EID:Slot  DID Type  State BT    Size     PDC PI SED DS3 FSpace TR
------------------------------------------------------------------------------
0         -         -             -                 -   RAID1 Dgrd  N  837.258 GB dflt N   N dflt  N      N
0         0         -                 -                 -   RAID1 Dgrd  N  837.258 GB dflt N   N dflt  N      N
0         0         0           252:2         9   DRIVE Rbld  Y  837.258 GB dflt N   N dflt  -      N
0         0         1           252:3         11  DRIVE Onln  N  837.258 GB dflt N   N dflt  -      N
------------------------------------------------------------------------------
<...snip...>
PD LIST :
=======
-------------------------------------------------------------------------
EID:Slt         DID State DG    Size    Intf Med SED PI SeSz    Model   Sp
-------------------------------------------------------------------------
252:2                9         Rbld  0  837.258 GB SAS  HDD  N  N  512B ST900MM0006 U <== replacement
disk in slot 2 joined device group 0 and in rebuilding state
252:3                11  Onln  0  837.258 GB SAS  HDD  N  N  512B ST900MM0006 U
-------------------------------------------------------------------------

[root@compute-node ~]# /opt/MegaRAID/storcli/storcli64 /c0/e252/s2 show rebuild
Controller = 0
Status = Success
Description = Show Drive Rebuild Status Succeeded.

----------------------------------------------------------
Drive-ID         Progress%         Status                       Estimated Time Left
----------------------------------------------------------
/c0/e252/s2         10                 In progress         1 Hours 9 Minutes <== replacement disk in slot 2
rebuild
status
----------------------------------------------------------
```

Technical Support Tools

Technical Support Tools

Running Cisco VIM Technical Support Tool

Cisco VIM includes a tech-support tool that you can use to gather Cisco VIM information to help solve issues working with Cisco Technical Support. The tech-support tool can be extended to execute custom scripts. It can be called after runner is executed at least once. The tech-support tool uses a configuration file that specifies what information to collect.

The configuration file is located in the location: */root/openstack-configs/tech-support/tech_support_cfg.yaml*.

The tech-support tool checks the point where the Cisco VIM installer has executed and collects the output of files or commands that is indicated by the configuration file. For example, if the installer fails at Step 3 (VALIDATION), the tech-support provides information that is listed in the configuration file up to Step 3 (included). You can override this default behavior by adding the *--stage* option to the command.

The tech-support script is located at the *management node /root/installer-{tag-id}/tech-support* directory. To run it after the runner execution, enter the following command:

```
./tech-support/tech_support.py
```

The command creates a compressed tar file containing all the information that is gathered. The file location is displayed in the console at the end of the execution. You need not have to execute the command with any options. However, if you want to override any default behavior, you can use the following options:

```
#/tech_support.py --help
Usage: tech_support.py [options]

Tech-support collects information about your cloud

Options:
-h, --help                                show this help message and exit
--stage=STAGE                          specify the stage where installer left off
--config-file=CFG_FILE
                                          specify alternate configuration file name
--tmp-dir=TMP_DIR                 specify alternate temporary directory name
--file-size=TAIL_SIZE
                                          specify max size (in KB) of each file collected
--host-list=HOST_LIST
                                          List (comma separated) of the hostnames of the servers
                                          to collect info from
--ip-list=IP_LIST                 List (comma separated) of the IPv4 of the hosts to
                                          collect info from
--exclude-mgmt-node         specify if mgmt node info needs to be excluded
--include-cimc                        specify if cimc techsupport needs to be included
--include-hw-diags                specify if hardware diagnostics need to be included
```

Where:

- stage: Tells at which state the installer left off. The possible values are: INPUT_VALIDATION, BUILDNODE_ORCHESTRATION, VALIDATION, BAREMETAL_INSTALL, COMMON_SETUP, CEPH, ORCHESTRATION or VMTP.
- config-file: Provides the path for a specific configuration file. Make sure that your syntax is correct. Look at the default */root/tech-support /openstack-configs/tech_support_cfg.yaml* file as an example on how to create a new config-file or modify the default file.
- tmp-dir: Provides the path to a temp directory tech-support can use to create the compressed tar file. The tech-support tool provides the infrastructure to execute standard Linux commands from packages that are included in the Cisco VIM installation. This infrastructure is extensible and you can add commands, files, or custom bash or Python scripts into the configuration file pane for the tool to collect the output of those commands or scripts. See the *README* pane for more details.
- file-size: Is an integer that specifies (in KB) the maximum file size that tech-support captures and tail the file if needed. By default, this value is set to 10 MB. For example, if no file-size option is provided and the tech-support has to collect */var/log/mercury/data.log* and the data.log is more than 10 MB, tech-support gets the last 10 MB from */var/log/mercury/data.log*.
- host-list: Provides the list of hosts one wants to collect from the tech-support through hostname, defaults to all hosts.
- ip-list: Provides the list of hosts to collect tech-support when their management IPv4 defaults to all hosts.
- exclude-mgmt-node: It is an option not to collect tech-support from the management node.

- include-cimc: Only applied for Cisco servers .This option allows to specify the list of hosts to get the CIMC tech-support. You can use this option along with the *–host-list* and *–ip-list* options.
- include-hw-diags: Only applied for Quanta servers. This option allows to specify the list of hosts to get the hardware support information collected on Quanta servers. It also collects the hardware information of the management node if it is a Quanta server. This option can be used along with the *–host-list* option.

You can avail tech-support for CIMC via this tool. With the given design associated to the CIMC tech-support command, ensure that you do not use *–include-cimc* option by default. It is recommended to use tech-support for CIMC for specific servers where issues are seen. Ensure that you use a maximum of three servers at a time using the below command:

```
#./tech-support.py --include-cimc --host-list=server_hostname_1,server_hostname_2
or
#./tech-support.py -include-cimc --ip-list=cimc_ip_host1,cimc_ip_host2
```


When using the *ip-list* option, provide the list of the management IP addresses. The tech-support can figure out the CIMC IP address from the *setup_data.yaml* file.

Tech-Support Configuration File

Cisco VIM tech-support is a utility tool is designed to collect the VIM pod logs which help users to debug the issues offline. The administrator uses the tech-support configuration files to provide the list of commands or configuration files. The tech support tool of the Cisco VIM gathers list of commands or configuration files for the offline diagnostic or debugging purposes.

By default the tech-support configuration file is located at the */root/openstack-configs/tech-support/tech_support_cfg.yaml* file. Alternatively, you can use a different one by specifying the *-config-file* option. The syntax of this configuration file must be as follows:

The tech-support configuration file section is divided into eight sections which corresponds to each of the installer stages

- INPUT_VALIDATION
- BUILDNODE_ORCHESTRATION
- VALIDATION
- BAREMETAL_INSTALL
- COMMON_SETUP
- CEPH
- ORCHESTRATION
- VMTP

Inside each of these eight sections, there are tags divided on hierarchical levels. At the first level, the tag indicates the host(s) or path on which the command(s) run and from where the file(s) can be collected.

The possible tags are as follows:

- - HOSTS_MANAGEMENT : Run in the Management node only
- - HOSTS_CONTROL : Run in all the Control nodes
- - HOSTS_COMPUTE : Run in all the Compute nodes
- - HOSTS_STORAGE : Run in all the Storage nodes
- - HOSTS_COMMON : Run in all the Compute and Control nodes
- - HOSTS_ALL : Run in all the Compute, Control and Storage nodes

In any of these eight sections, if *HOSTS* tag is not specified then no information is collected for that stage.

For each of the hosts mentioned above there is a second level tag which specifies where to run the command. The possible values of those tags are as follows:

- - SERVER_FILES: Path(s) to the file(s) that tech-support has to collect.
- - SERVER_COMMANDS: Command(s) or script name(s) which has to be executed directly on the server. The command(s) has to be included before in the $PATH. For the scripts, refer to the Custom Scripts paragraph below.
- - CONTAINERS: Indicates the tech-support tool that the command(s) has to be executed and the files to be gathered from inside a container. See the following steps for more specific information of what can be added in this section.

In the CONTAINERS section, indicate the path in which container the commands are executed or gathered from. This is done with a <*container_name*> tag. The following are shown to get the string for the<*container_name*> tag:

- all_containers: Execute inside all containers (regardless of the state).
- <container_name>: Container Name must be the name of a container and it indicates in which container to run the command or gather the information. It runs commands inside the container only if the mentioned container is up (as we cannot run commands on dead containers). Examples of how to get the container name:

Execute *docker ps* and get the name (without any numbers) of the last column of output *docker ps -a*.

For example:

```
CONTAINER ID        IMAGE                                          COMMAND  <snip>  NAMES
81bc4e54cbfb        <registry>/vmtp:4263        /bin/bash"                    vmtp_4263
```

The tech-support runs the linux commands on the server (from packages that is included in RHEL7.3). Add the name of the commands under the *SERVER_COMMANDS* section of the configuration file to run the commands.

However, if the administrator wants to add a custom bash or python script to be executed in some set of servers in the cloud. In such case you need to add the script into the custom-scripts directory on the current directory path */root/openstack-configs/tech-support/* and add the script name into the corresponding *SERVER_COMMANDS* section.

The tech-support tool will scp the script(s) included in the *custom-scripts* directory into the appropriate cloud nodes where it will be executed (as# indicated in this config file) and capture the output (stdout and stderr) and add it to the collection of files collected by the tech-support tool. It is assumed that the scripts are self-standing and independent and needs no external input.

Following is an example of a custom tech-support configuration file. This is just an example of what information the tech-support tool will gather if given the following configuration file:

```
COMMON_SETUP:
        HOSTS_ALL:                 # All compute, control and storage hosts
                SERVER_FILES:
                        - /usr/lib/docker-storage-setup
                SERVER_COMMANDS:
                        - docker info
                        - my_script.sh
                CONTAINERS:
                        all_containers:  #execute in all containers (even if they are in down state)
                          CONTAINER_COMMANDS:
                                - docker inspect
                                - docker logs
                                        logstash:
                                          CONTAINER_FILES:
                                                - /var/log/
                                          CONTAINER_COMMANDS:
                                                - ls -l
```

Given this example of configuration, and assuming that the installer ended in at least the *COMMON_SETUP* state, the tech-support tool will run under all *OpenStack* nodes (Compute, Control and Storage) and it will:

- Gather (if exists) the contents of */usr/lib/docker-storage-setup* file.
- Run *docker info* command and collect the output.
- Run *my_script.sh* and collect the output. The *my_script.sh* is an example of a bash script which the user previously added to the */root/openstack-configs/tech-support/custom-scripts* directory.
- Collect the output of docker inspect and docker logs for all containers.
- Collect the files in */var/log* inside the logstash container (if there is container with that name). This is equivalent to running the following command (where */tmp* indicates a temporary location where the tech-support tool gathers all the information): *docker cp logstash_{tag}:/var/log/ /tmp.*
- Collect the output of the command *docker exec logstash_{{tag}}: ls -l.*

Tech-Support When Servers Are Offline

It is difficult to collect the information from the servers if one or more cloud nodes are not reachable. In this case, you can connect through the **KVM** console into those servers and run the local tech-support tool.

1. To run the local tech-support tool run the following command:

```
/root/tech_support_offline
```

2. Cisco VIM tech_support _offline collects the Logs and other troubleshooting output from the server and place it in the location of the other server:

```
/root/tech_support
```


After the server is reachable, you can use the Cisco VIM tech-support tool which collects all the files under the */root/tech-support/* directory which can be used to debug any issue which are offline.

Running Cisco VIM Software Hub Technical Support Tool

The Cisco VIM Software Hub technical support tool uses a configuration file that specifies the information to be collected. The configuration file is located in the following location:

```
/root/cvim_sds-{tag-id}/openstack-configs/tech-support/tech_support_sds.yaml
```

This tool checks the point where the Cisco VIM Software Hub has executed and collects the output of files or commands indicated by the configuration file. The technical support script is available at the Software Hub node in the following location:

```
/root/cvim_sds-{tag-id}/tech-support/ directory.
```

To run the script, enter the following command:

```
./tech-support/tech_support_sds
```

This command execution creates a compressed tar file containing all the collected information and displays the file location.

Disk and OSD Maintenance Tools

Disk and OSD Maintenance Tools

Manage Physical Drives

You can use the disk-maintenance tool to check the status of all physical drives that are present in running and operational nodes in the following roles (except for third-party servers):

- Management
- Control (all or specific nodes)
- Compute (all or specific nodes)
- Storage

This provides the information about the present status of the physical drives. The status can be Online, Offline, Rebuilding, Unconfigured Good or JBOD states if all disks are ok. If not, the disks that have gone bad are displayed with the slot number and server information, for replacement. When multiple disks are to be replaced, it is recommended to remove or add disk for that node.

- Physically remove and insert a new disk before attempting to replace.
- For smooth operation, wipe out the disk before attempting replace operation.
- Call Cisco TAC if you face any issue. Do not reattempt.

Management Node

To check the status of the *Diskmgmt* log in to the management node and run the *ciscovim* command with the *diskmgmt* option. The design of the *diskmgmt* user interface follows a test job create, list, show, and delete the workflow.

1. Run the *Help* command to see all available command line options:

```
# ciscovim help diskmgmt
usage: ciscovim diskmgmt         [--server <node1,node2,...>] [--id <id>]
                                                    [--locator {on,off}] [--json-display] [-y]
                                                    create|delete|list|show check-disks|replace-disks
                                                    all|management|control|compute

HDD maintenance helper
Positional arguments:
        create|delete|list|show                 The control command to perform
        check-disks|replace-disks                 The identity of the task/action
        all|management|control|compute  The role of the target host(s)
Optional arguments:
--server <node1,node2,...>                          List of specific control/compute host names
                                                                within the target role.
--id <id>                                                       ID used to identify specific item to
                                                                show/delete.
--locator {on,off}                                      Turn on|off locator LED for server with bad
                                                                disks and for the physical

drives.
--json-display                                                  Shows output in JSON format.
-y, --yes                                                       Yes option to perform the action
```

2. Run the following *check-disk* operation command to create *check-disks* operation for all control nodes in the pod. The system responds with a message indicating the Time, ID and when it was created.

```
# ciscovim diskmgmt create check-disks control
+------------+--------------------------------------+
| Field      | Value                                                                    |
+------------+--------------------------------------+
| action          | check-disks                              |
| command          | create                                                                    |
| created_at | 2018-03-07T21:12:20.684648+00:00         |
| id                  | 0c6d27c8-bdac-493b-817e-1ea8640dae57 |
| locator          | False                                                                    |
| result          |                                                                                  |
```

```
| role                    | control                                                                    |
| servers          | None                                                              |
| status           | not_run                                                             |
| updated_at | None                                                            |
+------------+--------------------------------------+
```

3. Run the *ciscovim diskmgmt list* command to monitor the currently running task and completed tasks. The list command can filter based on the role. Use *all* command to list all the tests implemented in the database.

```
# ciscovim diskmgmt list check-disks control
+--------------------------------------+-------------+---------+----------+---------------------------+
| ID                                                                  | Action          | Role    |
Status   | Created
+--------------------------------------+-------------+---------+----------+---------------------------+
| 861d4d73-ffee-40bf-9348-13afc697ee3d | check-disks | control | Complete | 2018-03-05 14:44:47+00:00
|
| 0c6d27c8-bdac-493b-817e-1ea8640dae57 | check-disks | control | Running  | 2018-03-07 21:12:20+00:00
|
+--------------------------------------+-------------+---------+----------+---------------------------+
[root@F24-Michigan ~]# ciscovim diskmgmt list check-disks compute
+--------------------------------------+-------------+---------+----------+---------------------------+
| ID                                                                  | Action      | Role    |
Status   | Created
|
+--------------------------------------+-------------+---------+----------+---------------------------+
| 0be7a55a-37fe-43a1-a975-cbf93ac78893 | check-disks | compute | Complete | 2018-03-05 14:45:45+00:00
|
+--------------------------------------+-------------+---------+----------+---------------------------+
[root@F24-Michigan ~]# ciscovim diskmgmt list check-disks all
+--------------------------------------+-------------+---------+----------+---------------------------+
| ID                                                                  | Action      | Role    |
Status   | Created
|
+--------------------------------------+-------------+---------+----------+---------------------------+
| cdfd18c1-6346-47a2-b0f5-661305b5d160 | check-disks | all     | Complete | 2018-03-05 14:43:50+00:00
|
| 861d4d73-ffee-40bf-9348-13afc697ee3d | check-disks | control | Complete | 2018-03-05 14:44:47+00:00
|
| 0be7a55a-37fe-43a1-a975-cbf93ac78893 | check-disks | compute | Complete | 2018-03-05 14:45:45+00:00
|
| 0c6d27c8-bdac-493b-817e-1ea8640dae57 | check-disks | control | Complete | 2018-03-07 21:12:20+00:00
|
+--------------------------------------+-------------+---------+----------+---------------------------+
```

4. Run the following command to show the detailed results of a *diskmgmt check-disks* operation:

```
# ciscovim diskmgmt show check-disks control --id 0c6d27c8-bdac-493b-817e-1ea8640dae57
+----------------------------+----------------------+------------------------------+---------
+--------------------------+
| Message                    | Host                 | Role                         | Server  |
State                    |
+----------------------------+----------------------+------------------------------+---------
+--------------------------+
| Raid Health Status         | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 |
Optimal                  |
|                            | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 |
Optimal                  |
|                            | f24-michigan-micro-3 | block_storage control compute | 7.7.7.5 |
Optimal                  |
|                            |                      |                              |
|                          |
| VD Health Status           | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 |
Optimal                            |
|                            | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 |
Optimal                  |
|                                          | f24-michigan-micro-3 | block_storage control compute |
7.7.7.5 | Optimal                    |
|                                          |
```

```
|                                                |         |                                |
| RAID Level and Type        | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 | Type-
HW; Level - RAID1  |
|                            | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 | Type-
HW; Level - RAID1  |
|                            | f24-michigan-micro-3 | block_storage control compute | 7.7.7.5 | Type-
HW; Level - RAID1  |
|                            |                      |                               |
|                          |
| Number of Physical Disks   | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 |
8                        |
|                            | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 |
8                        |
|                            | f24-michigan-micro-3 | block_storage control compute | 7.7.7.5 |
8                        |
| Number of Virtual Disks    | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 |
1                        |
|                            | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 |
1                        |
|                            | f24-michigan-micro-3 | block_storage control compute | 7.7.7.5 |
1                        |
| Boot Drive Disk Media-Type | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 |
HDD                      |
|                            | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 |
HDD                      |
|                            | f24-michigan-micro-3 | block_storage control compute | 7.7.7.5 |
SSD                      |
+----------------------------+----------------------+-------------------------------+---------
+--------------------------+
State Keys:
DHS-Dedicated Hot Spare|UGood-Unconfigured Good|GHS-Global Hotspare
UBad-Unconfigured Bad|Onln-Online|Offln-Offline
Rbld-Rebuilding|JBOD-Just a Bunch Of Disks
```

5. Run the following command to delete the *diskmgmt check-disks*:

```
Delete a diskmgmt check-disks result:
```


Cisco recommends you to delete the tests that are not in use.

Compute/Control Node

All the compute/control nodes must run with hardware RAID and typically have two HDDs or SSDs. If the nodes are running with HDDs and has one of the HDD in failed state, see Compute Node Recovery Scenario on how to recover the node.

OSD-Maintenance Tool (Storage Node)

You can use the OSD maintenance tool to check the status of all OSDs that are present in running and operational block storage nodes. This tool gives you the detailed information about the status of the OSDs whether they are Up or Down, in addition to which HDD corresponds to which OSD, including the slot number and server hostname.

- If it is down, run the cluster recovery and recheck as the OSD is discovered after *check_osds* is performed.
- If still down, wait for 30 minutes before attempting replace, for *ceph-mon* to sync.
- Physically remove and insert a new disk before attempting replace.
- For smooth operation, wipe out the disk before attempting replace operation.
- Need a dedicated journal SSD for each storage server where *osdmgmt* is attempted.
- You can replace only one OSD at a time. Space out each replace OSD by 30 minutes - time for *ceph-mon* to sync.
- Call TAC if any issue is hit. Do not reattempt

To check the status of the *osdmgmt* tool log in the management node and run the *ciscovim* command with the *osdmgmt* option. The *osdmgmt* user interface allows you to create, list, show, and delete a workflow.

- Use *ciscovim osdmgmt create* command to initiate a check and replace OSD operation
- Use *ciscovim osdmgmt list* command to view summary and status of current OSD operations
- Use *ciscovim osdmgmt show ... --id <ID>* command to view detail OSD operation results
- Use '*ciscovim osdmgmt delete … --id <ID>* command to delete the results.

Examples of usage of this tool:

1. Run the *Help* command to see all the options:

```
# ciscovim help osdmgmt
usage: ciscovim osdmgmt         [--server <node1,node2,...>] [--detail] [--id <id>]
                                                             [--osd <osd_name>] [--locator {on,off}]
                                                             [--json-display] [-y]
                                                             create|delete|list|show check-osds|replace-osd
OSD maintenance helper
Positional arguments:
        create|delete|list|show         The control command to perform
        check-osds|replace-osd                 The identity of the task/action
Optional arguments:
        --server <node1,node2,...>         List of specific block_storage hostnames
        --detail                                      Display full OSD details
--id <id>                                              ID used to identify specific item to
                                                             show/delete.
--osd <osd_name>                                  Name of down OSD to replace. Eg. 'osd.xx'
--locator {on,off}                                  Turn on|off locator LED for server with bad OSDs
                                                             and for the physical drives.
--json-display                                         Show output will be in JSON format.
-y, --yes                                             Yes option to perform the action
--+------------+----------+-----------+--------------------------+-----------+
```

2. To check the *osds* run the following command:

```
# ciscovim osdmgmt create check-osds
+------------+--------------------------------------+
| Field          | Value                                                                  |
+------------+--------------------------------------+
| action     | check-osds                                                          |
| command    | create                                                                 |
| created_at | 2018-03-08T21:11:13.611786+00:00         |
| id         | 5fd4f9b5-786a-4a21-a70f-bffac70a3f3f |
| locator    | False                                                                  |
| osd        | None                                                                |
| result     |                                                                                |
| servers    | None                                                                |
| status     | not_run                                                                |
| updated_at | None                                                                |
+------------+--------------------------------------+
```

3. Monitor the *osdmgmt* check operations using *te list* command. Cisco Vim *Osd mgmt list* commands are used to monitor the currently running test. It also helps you to view the tests that are run/ completed.

```
# ciscovim osdmgmt list check-osds
+--------------------------------------+------------+----------+----------------------------+
| ID                                   | Action     | Status   | Created                    |
+--------------------------------------+------------+----------+----------------------------+
| 5fd4f9b5-786a-4a21-a70f-bffac70a3f3f | check-osds | Complete | 2018-03-08 21:11:13+00:00 |
| 4efd0be8-a76c-4bc3-89ce-142de458d844 | check-osds | Complete | 2018-03-08 21:31:01+00:00 |
+--------------------------------------+------------+----------+----------------------------+
```

4. To show the detailed results of *osdmgmt check-osds operation*, run the following command:

```
# ciscovim osdmgmt show check-osds --id 5fd4f9b5-786a-4a21-a70f-bffac70a3f3f
+--------------------+----------------------+-------------------------------+---------+---------+
| Message            | Host                 | Role                          | Server  | State   |
+--------------------+----------------------+-------------------------------+---------+---------+
| Overall OSD Status | f24-michigan-micro-3 | block_storage control compute | 7.7.7.5 | Optimal |
|                    | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 | Optimal |
|                    | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 | Optimal |
| Number of OSDs     | f24-michigan-micro-3 | block_storage control compute | 7.7.7.5 | 5             |
|                    | f24-michigan-micro-1 | block_storage control compute | 7.7.7.7 | 5       |
|                    | f24-michigan-micro-2 | block_storage control compute | 7.7.7.6 | 5             |
+--------------------+----------------------+-------------------------------+---------+---------+
```

```
+----------------------+--------+--------+----+-----------+-----------+--------------------------
+-----------+
| Host                 | OSDs   | Status | ID | HDD Slot  | Path      | Mount                    |
Journal |
+----------------------+--------+--------+----+-----------+-----------+--------------------------
+-----------+
| f24-michigan-micro-3 | osd.0         | up          | 0  | 4 (JBOD)  | /dev/sda1 | /var/lib/ceph/osd
/ceph-0  | /dev/sdf1 |
|                      | osd.1  | up     | 1  | 5 (JBOD)  | /dev/sdb1 | /var/lib/ceph/osd/ceph-1  | /dev
/sdf2 |
|                      | osd.3  | up     | 3  | 7 (JBOD)  | /dev/sdc1 | /var/lib/ceph/osd/ceph-3  | /dev
/sdf3 |
|                      | osd.5  | up     | 5  | 8 (JBOD)  | /dev/sdd1 | /var/lib/ceph/osd/ceph-5  | /dev
/sdf4 |
|                      | osd.6  | up     | 6  | 6 (JBOD)  | /dev/sde1 | /var/lib/ceph/osd/ceph-6  | /dev
/sdf5 |
| f24-michigan-micro-1 | osd.2  | up     | 2  | 5 (JBOD)  | /dev/sda1 | /var/lib/ceph/osd/ceph-2  | /dev
/sdf1 |
|                      | osd.7  | up     | 7  | 7 (JBOD)  | /dev/sdb1 | /var/lib/ceph/osd/ceph-7  | /dev
/sdf2 |
|                      | osd.9  | up     | 9  | 8 (JBOD)  | /dev/sdc1 | /var/lib/ceph/osd/ceph-9  | /dev
/sdf3 |
|                      | osd.11 | up     | 11 | 6 (JBOD)  | /dev/sdd1 | /var/lib/ceph/osd/ceph-11 | /dev
/sdf4 |
|                      | osd.13 | up     | 13 | 4 (JBOD)  | /dev/sde1 | /var/lib/ceph/osd/ceph-13 | /dev
/sdf5 |
| f24-michigan-micro-2 | osd.4  | up          | 4  | 8 (JBOD)  | /dev/sda1 | /var/lib/ceph/osd/ceph-4  |
/dev/sdf1 |
|                      | osd.8  | up     | 8  | 5 (JBOD)  | /dev/sdb1 | /var/lib/ceph/osd/ceph-8  | /dev
/sdf2 |
|                      | osd.10 | up          | 10 | 4 (JBOD)  | /dev/sdc1 | /var/lib/ceph/osd/ceph-10 |
/dev/sdf3 |
|                      | osd.12 | up          | 12 | 6 (JBOD)  | /dev/sdd1 | /var/lib/ceph/osd/ceph-12 |
/dev/sdf4 |
|                      | osd.14 | up          | 14 | 7 (JBOD)  | /dev/sde1 | /var/lib/ceph/osd/ceph-14 |
/dev/sdf5 |
+----------------------+--------+--------+----+-----------+-----------+--------------------------
+-----------+
```

5. To delete the *check-disk osds*, run the following command:

```
# ciscovim osdmgmt delete check-osds --id 5fd4f9b5-786a-4a21-a70f-bffac70a3f3f
Perform the action. Continue (Y/N)Y
Delete of UUID 5fd4f9b5-786a-4a21-a70f-bffac70a3f3f Successful
[root@F24-Michigan ~]# ciscovim osdmgmt list check-osds
+--------------------------------------+------------+----------+---------------------------+
| ID                                   | Action     | Status   | Created                   |
+--------------------------------------+------------+----------+---------------------------+
| 4efd0be8-a76c-4bc3-89ce-142de458d844 | check-osds | Complete | 2018-03-08 21:31:01+00:00 |
+--------------------------------------+------------+----------+---------------------------+
```

Utility Tool

Utility Tool

Utility to Resolve Cisco VIM Hardware Validation Failures

The Cisco VIM Hardware Validation utility tool is used to perform hardware validation during the installation of **UCS C-series** servers. It captures the user and environmental hardware validation errors that occur during the installation process. The tool enables you to fix these errors that are based on the inputs you provide at the Command Line Interface (CLI). It validates the updated configurations to verify if the changes are applied properly. After the error is resolved, you can resume the installation from the point of failure.

The ciscovim hardware-mgmt user interface allows you to test the job validate orresolve-failures(create), list, show, and delete workflow.

Hardware-mgmt user workflow:

1. Use "*ciscovim hardware-mgmt validate* …" command to initiate a validation.
2. Use "*ciscovim hardware-mgmt list* …" command to view summary/status of current test jobs.
3. Use "*ciscovim hardware-mgmt show* … *--id <ID>*" command to view detail test results.
4. Use "*ciscovim hardware-mgmt delete* … *--id <ID>*" to delete test results.

A database of results is maintained so that the user can keep the results of *multiple hardware-mgmt* operations and view them at any time.

You cannot use the utility for the following tasks:

- Configuring BIOS settings for the B-series pods.
- Upgrading or changing the firmware version.
- Resolving hardware failures other than lom, hba, flexflash, pcie_slot, power, and vnic_pxe_boot.

Command Usage

To capture the list of failures that can be resolved by using the utility, go to the *install* directory and execute the *help* command:

```
# cd <installer-id>/clouddeploy
# python hw_validations.py -help .
```

The following shows the output of the *help* command.

```
usage: hw_validations.py [-h] [--resolve-failures RESOLVE_FAILURES]
[--validate VALIDATE_OF] [-y] [--host HOSTS]
[--file SETUP_FILE_LOCATION]
UCS Hardware Validations
optional arguments:
-h, --help show this help message and exit
--resolve-failures RESOLVE_FAILURES, -rf RESOLVE_FAILURES
                                              all - Fix all the failures.
                                              lom - Fix LOM port(s) status failures.
                                              hba - Fix HBA port status failures.
                                              flexflash - Fix Flexflash failures.
                                              pcie_slot - Fix PCIe slot status failures.
                                              power - Fix Power failures.
                                              vnic_pxe_boot - Fix Vnic PXE_Boot statusfailures
-y, -yes
--host HOSTS Comma separated list of hostnames
--file SETUP_FILE_LOCATION, -f SETUP_FILE_LOCATION
                        Provide a valid 'setup_data.yaml' file
```

Command Syntax

```
hw_validations.py [-h] [--resolve-failures RESOLVE_FAILURES] [--validate VALIDATE_OF] [-y]
[--host HOSTS] [--file SETUP_FILE_LOCATION]
```

The following table provides the description of the parameters of the command.

Optional	Description
[-h], --help	Provides detailed information about the command.
[--resolve-failures RESOLVE_FAILURES], -rf RESOLVE_FAILURES	Enables you to specify the failure that you want to resolve. The optional arguments are as follows:
[-y]	Yes
[--host HOSTS]	Enables you to specify the hostname of the server for which you want to resolve failures. You cannot specify the IP address or CIMC IP address of servers as arguments. You can specify a list of hostnames as comma-separated arguments. If the -host option is not specified, the failures of all the servers that are specified in the *setup_data.yaml* file are resolved.
[--file SETUP_FILE_LOCATION] [-f SETUP_FILE_LOCATION]	Enables you to specify the name of a *setup_data.yaml* file.

Examples of Command Usage

The following table provides the commonly used commands along with their examples.

Purpose	Syntax	Example
To resolve all failures.	python hw_validations.py --resolve-failures all -y	python hw_validations.py --resolve-failures all -y
To simultaneously resolve one or more failures.	python hw_validations.py --resolve-failures <failure-1>,<failure-2> -y	To resolve the lom and hba status failures: python hw_validations.py --resolve-failures lom,hba -y
To resolve the errors by using the setup_data.yaml file.	python hw_validations.py --resolve-failures <failure-1>,<failure-2> -y --file <location-of-yaml file>	To resolve the LOM status failures by using ~- file: python hw_validations.py --resolve-failures lom,hba -y --file ~/save/setup_data.yaml
To resolve failures on a particular server as specified in the setup_data.yaml file by using the **--** *host* option.	python hw_validations.py --resolve-failures <failure-1> -y --host <name-of-host-server-1>, <name-of-host-server-2>	To resolve the PCIe slot failures on hiccup-controller-1 server as specified in the setup_data.yaml: python hw_validations.py --resolve-failures pcie_slot -y --host hiccup-controller-1

Cisco VIM Client Debug Option

Cisco VIM Client Debug Option

The **--debug** option enables you to get verbose logging on the ciscovim client console. You can use verbose logging to troubleshoot issues with the ciscovim client.

The debug option has the following parts:

- Curl Command: Curl command can be used for debugging. It can be executed standalone. Curl Command also displays the REST API Endpoint and the Request Payload.
- Response of REST API.

Examples of Using debug Option to get list of passwords

```
# ciscovim --debug list-password-keys
2018-05-28 22:13:21,945 DEBUG [ciscovimclient.common.httpclient][MainThread] curl -i -X GET
-H 'Content-Type: application/json' -H 'Authorization: ****' -H 'Accept: application/json'
-H 'User-Agent: python-ciscovimclient' --cacert /var/www/mercury/mercury-ca.crt
https://172.31.231.17:8445/secrets
2018-05-28 22:13:21,972 DEBUG [ciscovimclient.common.httpclient][MainThread]
HTTP/1.1 200 OK
content-length: 1284
x-xss-protection: 1
x-content-type-options: nosniff
strict-transport-security: max-age=31536000
server: WSGIServer/0.1 Python/2.7.5
cache-control: no-cache, no-store, must-revalidate, max-age=0
date: Tue, 29 May 2018 05:13:21 GMT
x-frame-options: SAMEORIGIN
content-type: application/json; charset=UTF-8
{u'HEAT_KEYSTONE_PASSWORD': '****', u'CINDER_KEYSTONE_PASSWORD': '****',
u'METADATA_PROXY_SHARED_SECRET': '****', u'WSREP_PASSWORD': '****', u'ETCD_ROOT_PASSWORD':
'****', u'HEAT_DB_PASSWORD': '****', u'CINDER_DB_PASSWORD': '****', u'KEYSTONE_DB_PASSWORD':
'****', u'NOVA_DB_PASSWORD': '****', u'GLANCE_KEYSTONE_PASSWORD': '****',
u'CLOUDPULSE_KEYSTONE_PASSWORD': '****', u'VPP_ETCD_PASSWORD': '****', u'COBBLER_PASSWORD':
'****', u'DB_ROOT_PASSWORD': '****', u'NEUTRON_KEYSTONE_PASSWORD': '****',
u'HEAT_STACK_DOMAIN_ADMIN_PASSWORD': '****', u'KIBANA_PASSWORD': '****',
u'IRONIC_KEYSTONE_PASSWORD': '****', u'ADMIN_USER_PASSWORD': '****', u'HAPROXY_PASSWORD':
'****', u'NEUTRON_DB_PASSWORD': '****', u'IRONIC_DB_PASSWORD': '****', u'GLANCE_DB_PASSWORD':
'****', u'RABBITMQ_ERLANG_COOKIE': '****', u'NOVA_KEYSTONE_PASSWORD': '****',
u'CPULSE_DB_PASSWORD': '****', u'HORIZON_SECRET_KEY': '****', u'RABBITMQ_PASSWORD': '****'}
+----------------------------------+
| Password Keys                    |
+----------------------------------+
| ADMIN_USER_PASSWORD              |
| CINDER_DB_PASSWORD               |
| CINDER_KEYSTONE_PASSWORD         |
| CLOUDPULSE_KEYSTONE_PASSWORD     |
| COBBLER_PASSWORD                 |
| CPULSE_DB_PASSWORD               |
| DB_ROOT_PASSWORD                 |
| ETCD_ROOT_PASSWORD               |
| GLANCE_DB_PASSWORD               |
| GLANCE_KEYSTONE_PASSWORD         |
| HAPROXY_PASSWORD                 |
| HEAT_DB_PASSWORD                 |
| HEAT_KEYSTONE_PASSWORD           |
| HEAT_STACK_DOMAIN_ADMIN_PASSWORD |
| HORIZON_SECRET_KEY               |
| IRONIC_DB_PASSWORD               |
| IRONIC_KEYSTONE_PASSWORD         |
| KEYSTONE_DB_PASSWORD             |
| KIBANA_PASSWORD                  |
```

```
| METADATA_PROXY_SHARED_SECRET            |
| NEUTRON_DB_PASSWORD                        |
| NEUTRON_KEYSTONE_PASSWORD            |
| NOVA_DB_PASSWORD                        |
| NOVA_KEYSTONE_PASSWORD                    |
| RABBITMQ_ERLANG_COOKIE                    |
| RABBITMQ_PASSWORD                            |
| VPP_ETCD_PASSWORD                            |
| WSREP_PASSWORD                                |
+----------------------------------+
```

Examples of Using debug option to get list of nodes

```
# ciscovim --debug list-nodes
2018-05-28 22:13:31,572 DEBUG [ciscovimclient.common.httpclient][MainThread] curl -i -X GET
-H 'Content-Type: application/json' -H 'Authorization: ****' -H 'Accept: application/json'
-H 'User-Agent: python-ciscovimclient' --cacert /var/www/mercury/mercury-ca.crt
https://172.31.231.17:8445/nodes
2018-05-28 22:13:31,599 DEBUG [ciscovimclient.common.httpclient][MainThread]
HTTP/1.1 200 OK
content-length: 2339
x-xss-protection: 1
x-content-type-options: nosniff
strict-transport-security: max-age=31536000
server: WSGIServer/0.1 Python/2.7.5
cache-control: no-cache, no-store, must-revalidate, max-age=0
date: Tue, 29 May 2018 05:13:31 GMT
x-frame-options: SAMEORIGIN
content-type: application/json; charset=UTF-8
{u'nodes': {u'status': u'Active', u'uuid': u'6b1ea6ee-b15b-41ca-9d79-3bb9ec0002bc',
u'setupdata': u'fe78b5f9-5a46-447c-9317-2bf7362c1e81', u'node_data': {u'rack_info':
{u'rack_id': u'RackD'}, u'cimc_info': {u'cimc_ip': u'172.29.172.81'}, u'management_ip':
u'21.0.0.10'}, u'updated_at': u'2018-05-25T11:14:46+00:00', u'reboot_required': u'No',
u'mtype': u'control', u'install': u'372aa3c1-1ab0-4dd0-a8a8-1853a085133c', u'power_status':
u'PowerOnSuccess', u'install_logs':
u'https://172.31.231.17:8008//edd3975c-8b7c-4d3c-93de-a033ae10a6b6', u'created_at':
u'2018-05-21T13:25:50+00:00', u'name': u'gg34-2'}}
+-----------+--------+---------+---------------+
| Node Name | Status | Type    | Management IP |
+-----------+--------+---------+---------------+
| gg34-1    | Active | control | 21.0.0.12           |
| gg34-2    | Active | control | 21.0.0.10     |
| gg34-3    | Active | control | 21.0.0.11     |
| gg34-4    | Active | compute | 21.0.0.13     |
+-----------+--------+---------+---------------+
```

Example of Getting Response from REST API using Curl Commands

```
Get the REST API Password.
# cat /opt/cisco/ui_config.json
{
"Kibana-Url": "http://172.31.231.17:5601",
"RestAPI-Url": "https://172.31.231.17:8445",
"RestAPI-Username": "admin",
"RestAPI-Password": "********************",
"RestDB-Password": "********************",
"BuildNodeIP": "172.31.231.17"
}
Form the Curl Command.
curl -k -u <RestAPI-Username>:<RestAPI-Password> <RestAPI-Url>/<Endpoint>
E.g. To get Nodes Info of Cloud
curl -k -u admin:**** http://172.31.231.17:5601/v1/nodes
```

Examples of Response of REST APIs

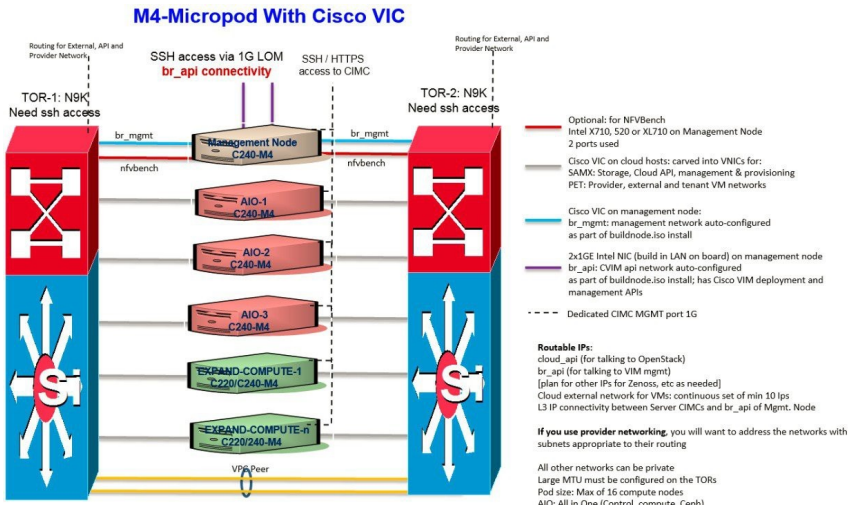
```
API "/"
# curl -k -u admin:**** https://172.31.231.17:8445/
{"default_version": {"id": "v1", "links": [{"href": "http://127.0.0.1:8083/v1/", "rel":
"self"}]}, "versions": [{"id": "v1", "links": [{"href": "http://127.0.0.1:8083/v1/", "rel":
"self"}]}], "name": "Virtualized Infrastructure Manager Rest API", "description":
"Virtualized Infrastructure Manager Rest API is used to invoke installer from API."}
API "/v1/setupdata/"
# curl -k -u admin:**** https://172.31.231.17:8445/v1/setupdata/
{"setupdatas": [. . .]}
API "/v1/nodes"
# curl -k -u admin:**** https://172.31.231.17:8445/v1/nodes
{"nodes": [{"status": "Active", "uuid": "0adabc97-f284-425b-ac63-2d336819fbaf", "setupdata":
"fe78b5f9-5a46-447c-9317-2bf7362c1e81", "node_data": "{\"rack_info\": {\"rack_id\":
\"RackC\"}, \"cimc_info\": {\"cimc_ip\": \"172.29.172.75\"}, \"management_ip\":
\"21.0.0.13\"}", "updated_at": "2018-05-21T15:11:05+00:00", "reboot_required": "No", "mtype":
"compute", "install": "372aa3c1-1ab0-4dd0-a8a8-1853a085133c", "power_status":
"PowerOnSuccess", "install_logs":
"https://172.31.231.17:8008//edd3975c-8b7c-4d3c-93de-a033ae10a6b6", "created_at":
"2018-05-21T13:25:50+00:00", "name": "gg34-4"}, . . . . ]}
API "/v1/secrets"
# curl -k -u admin:**** https://172.31.231.17:8445/v1/secrets
{"HEAT_KEYSTONE_PASSWORD": "5oNff4jWsvAwnWk1", "CINDER_KEYSTONE_PASSWORD": "Hq4i6S5CnfQe7Z2W",
"RABBITMQ_ERLANG_COOKIE": "XRMHBQHTLVJSVWDFKJUX", "METADATA_PROXY_SHARED_SECRET":
"XNzrhosqW4rwiz7c", "WSREP_PASSWORD": "z1oQqhKd1fXDxJTV", "ETCD_ROOT_PASSWORD":
"LMLC8gvi1IA3KiIc", "HEAT_DB_PASSWORD": "J8zt8ldMvdtJxAtG", "CINDER_DB_PASSWORD":
"BVX3y2280DSx2JkY", "KEYSTONE_DB_PASSWORD": "55fVNzxR1VxCNOdh", "NOVA_DB_PASSWORD":
"Rk1MK1OIJgsjGZal", "IRONIC_KEYSTONE_PASSWORD": "9tYZgIw6SZERZ1dZ", "ADMIN_USER_PASSWORD":
"DjDQrk4QT7pgHy94", "GLANCE_KEYSTONE_PASSWORD": "w4REb8uhrHquCfRm", "HAPROXY_PASSWORD":
"oB0v7VJoo2IfB8OW", "CLOUDPULSE_KEYSTONE_PASSWORD": "q6QVvxBQhrqv6Zhx", "NEUTRON_DB_PASSWORD":
"FZVMWgApcZR4us5q", "IRONIC_DB_PASSWORD": "dq3Udmu95DWyX1jy", "GLANCE_DB_PASSWORD":
"O7vQ2emuPDrrvD4x", "KIBANA_PASSWORD": "azHHhP4ewxpZVwcg", "VPP_ETCD_PASSWORD":
"NLyIAvECMW2qI7Bp", "NOVA_KEYSTONE_PASSWORD": "JUfMNGz0BZG7JwXV", "NEUTRON_KEYSTONE_PASSWORD":
"QQ0lo8Q87BjFoAYQ", "CPULSE_DB_PASSWORD": "DaFthNtpX2RvwTSs", "COBBLER_PASSWORD":
"XoIJ9mbWcmVyzvvN", "HORIZON_SECRET_KEY":
"NHkA0qwHIWUSwhPZowJ8Ge3RyRd6oM8XjOT8PHnZdckxgm3kbb1MSltsw0TAQJnx", "DB_ROOT_PASSWORD":
"seqh5DRIKP6ZsKJ8", "HEAT_STACK_DOMAIN_ADMIN_PASSWORD": "Vu6LexEadAxscsvY",
"RABBITMQ_PASSWORD": "LBoYoxuvGsMsl1TX"}
API "/v1/nodes/mgmt._node"
# curl -k -u admin:**** https://172.31.231.17:8445/v1/nodes/mgmt_node
{"api_ip": "172.31.231.17", "mgmt_ip": "21.0.0.2"}
```

Wiring Diagrams

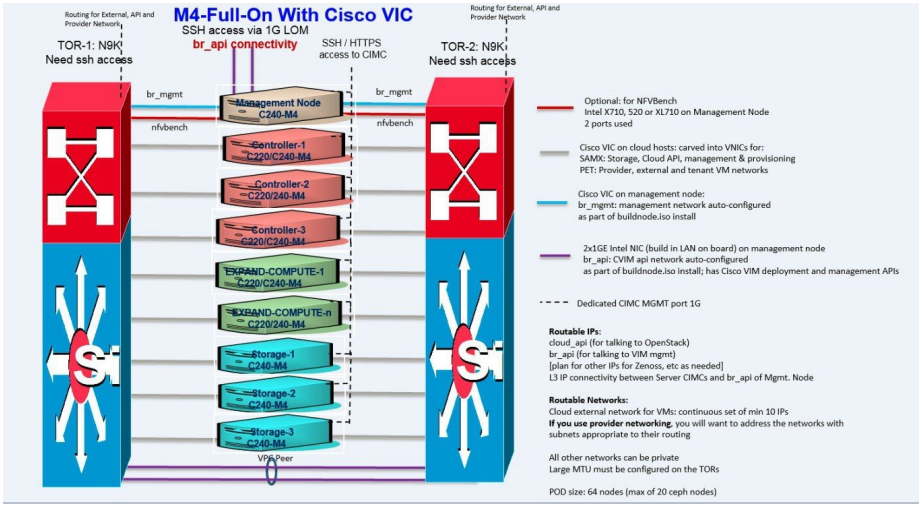
Wiring Diagrams

Following are the wiring diagrams of Cisco VIM:

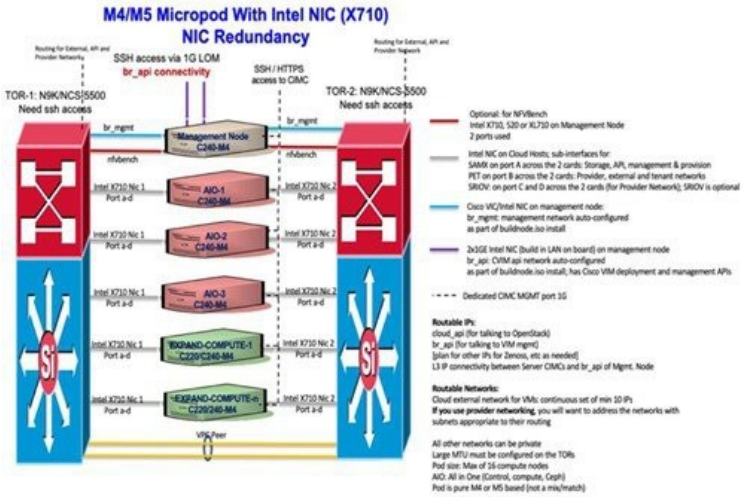
M4-Micropod with Cisco VIC



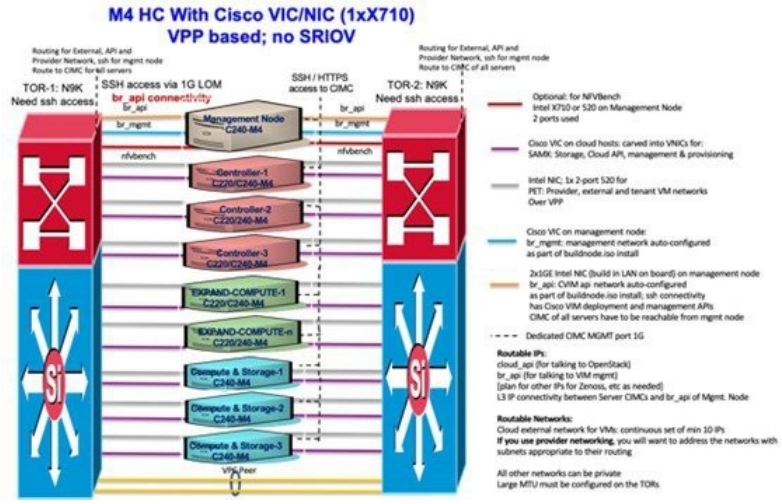
M4-Full-On with Cisco VIC



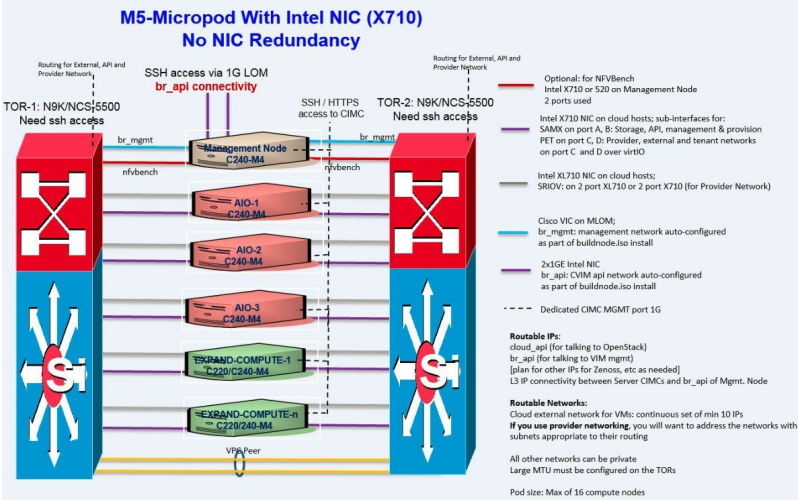
M4/M5 Micropod with Intel NIC (X710) - NIC Redundancy



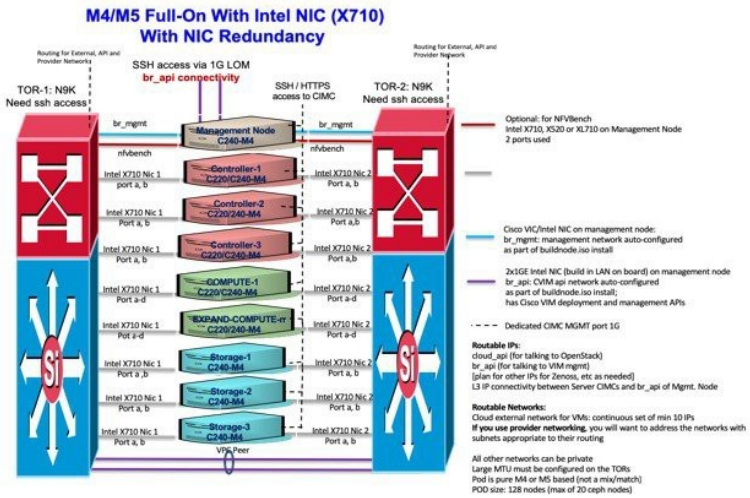
M4 Hyperconverged with VPP based Cisco VIC/NIC (1xX710) (no SRIOV)



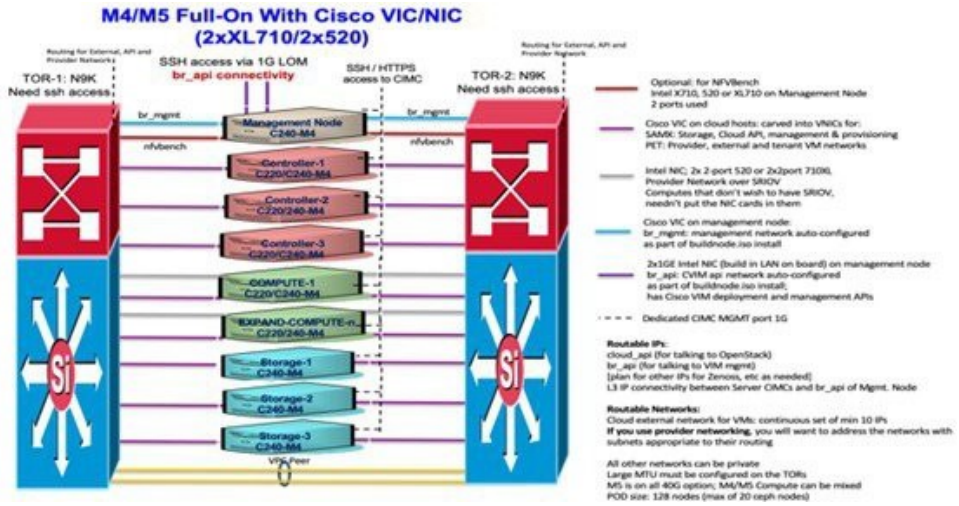
M5-Micropod with Intel NIC (X710) - No NIC Redundancy



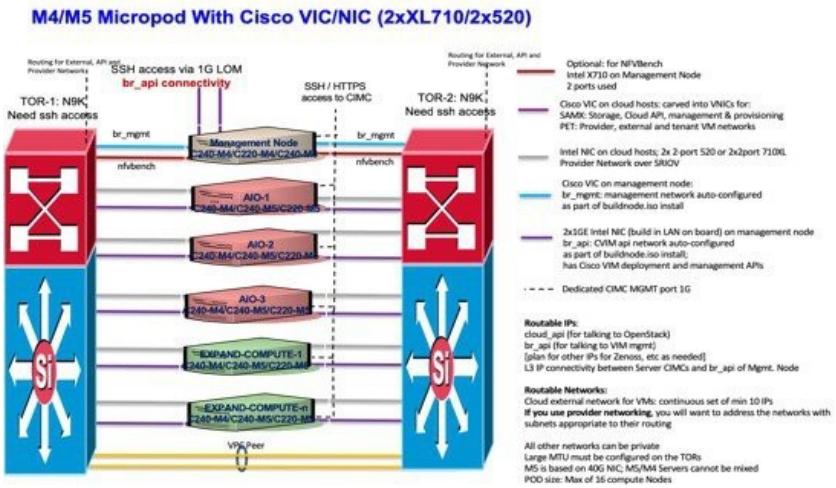
M4/M5 Full-On with Intel NIC (X710) and with NIC Redundancy



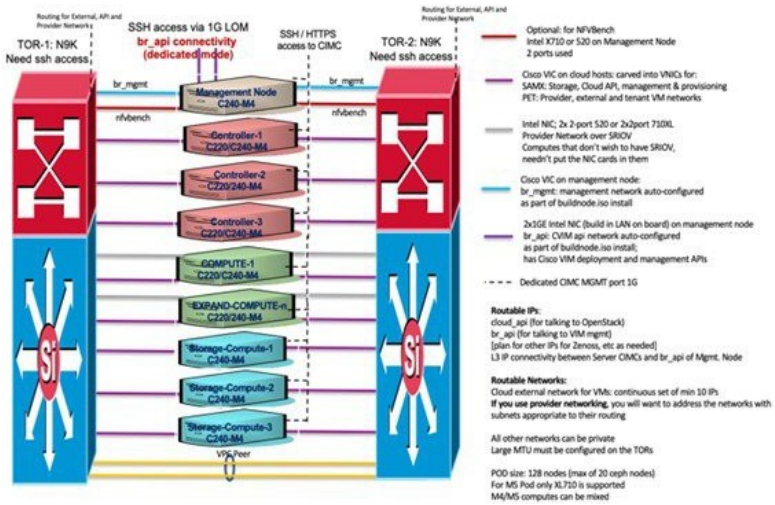
M4/M5 Full-On with Cisco VIC/NIC (2xXL710/2x520)



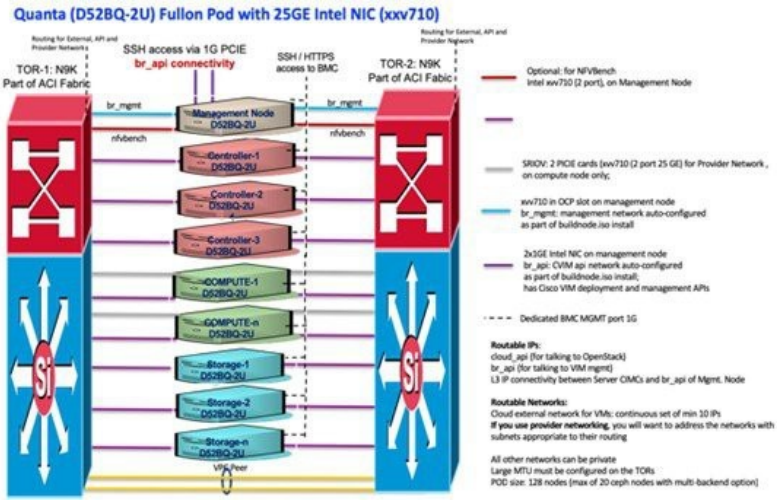
M4/M5 Micropod with Cisco VIC/NIC (2xXL710/2x520)



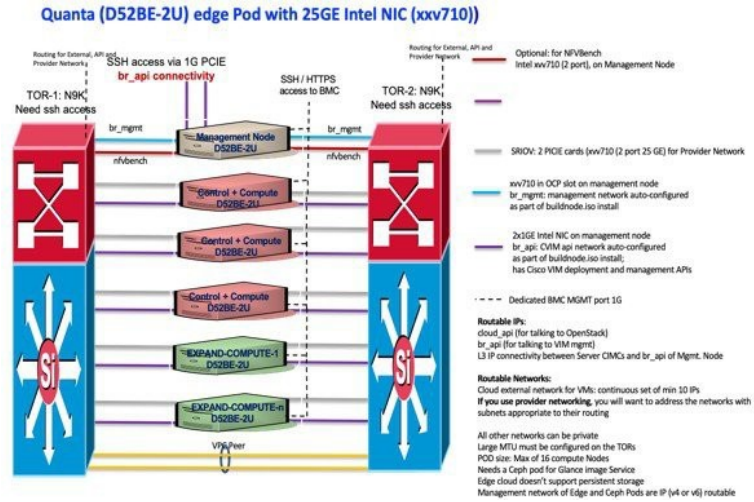
M4/M5-HC with Cisco VIC/NIC (2xXL710/2x520)



Quanta (D52BQ-2U 3UPI) Fullon Pod with 25GE Intel NIC (xxv710)



Quanta (D52BE-2U) Edge Pod with 25GE Intel NIC (xxv710)



Quanta (D52BQ-2U 3UPI) Ceph Pod with 25GE Intel NIC (xxv710)

Quanta (D52BQ-2U) ceph Pod with 25GE Intel NIC (xxv710))