HP Helion OpenStack Carrier Grade 2.1 Beta

Contents

HP Helion OpenStack® Carrier Grade 2.1 Beta..... 3
Overview..... 3
Non-KVM Region Overview..... 8
KVM Region Overview..... 9
Technical Overview..... 9
Services Overview..... 15
Release Notes..... 21
Applying Customer-Specific Branding (optional)..... 26
Installation..... 27
Deploying the Denver Template..... 27
Configuring SR-IOV or PCI Passthrough Networking..... 66
Best Practices..... 75
Administration..... 80
KVM Region Administrator Guide..... 80
Centralized Logging..... 80
Backup and Restore..... 84
Restart MySQL and RabbitMQ..... 100
Patching and Update Process..... 101
API and SDK Reference..... 103
Lifecycle Manager CLI Reference..... 105
Operations..... 109
Operations Guide..... 111
Troubleshooting..... 198
Installation Troubleshooting..... 200
Open Source and Third-Party Software License Agreements..... 209
HP Helion OpenStack Carrier Grade: Open Source and Third-Party Software License Agreement.... 209
Software License Terms..... 209
HP Helion OpenStack Carrier Grade: Software License Terms..... 209

HP Helion OpenStack® Carrier Grade 2.1 Beta

HP Helion OpenStack Carrier Grade is a carrier-grade distribution of OpenStack, the leading open source cloud computing platform.

HP Helion OpenStack Carrier Grade provides communications service providers (CSPs) with an open source based cloud platform that meets their demanding reliability requirements.

Installing HPE OpenStack Carrier Grade

Use the following links to begin installing HPE OpenStack Carrier Grade:

- *HP Helion OpenStack Carrier Grade 2.1 Beta: Installation* on page 27

  Start with this document for complete instructions on how to install your HP Helion OpenStack cloud, including system requirements, prerequisites, and deployment models

Learning about HP Helion OpenStack Carrier Grade

Use the following links to review some high-level overview information about HP Helion OpenStack Carrier Grade:

- *HP Helion OpenStack Carrier Grade 2.1 Beta: Overview* on page 3
- *HP Helion OpenStack Carrier Grade 2.1 Beta: Release Notes* on page 21

Getting started with HP Helion OpenStack Carrier Grade

Use the following links and tools to begin working with HP Helion OpenStack Carrier Grade:

- *Administrator Guide*

  The *KVM-Region Administrator Guide* is addressed to HP Helion OpenStack Carrier Grade administrators responsible for the following areas:

  - Creating and maintaining resources used by end users (tenants), such as virtual machines, storage pools, network objects, and access credentials.
  - Operating and maintaining components of the HP Helion OpenStack Carrier Grade product, such as clusters, nodes, system software, licensing files, and backup and restore facilities

  The Administer Guide also contains specific tasks, such as logging, backup/restore, switch configuration, and configuring a multiple data center environment.
- *Operations Guide*

  The Operations Guide introduces the Horizon interface with specific information on how to use Horizon to operate HP Helion OpenStack Carrier Grade on a day-to-day basis.
- *Services Overview*

  These topics describe the supported OpenStack Service and contain links to the respective OpenStack CLI and API documentation.
- *API and SDK Reference*

  The API and SDK reference provides links to supported API and custom OpenStack API extensions. The page also links to the HP Helion OpenStack Carrier Grade Software Development Kit (SDK) documentation.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Overview

HCG ties together Open Source services into a highly available, resilient framework with high performance components that meets the needs and demands of CSPs

HP Helion OpenStack Carrier Grade brings together the flexibility and scalability of the IT cloud, and the high-availability and performance demanded by the Telecommunications industry, into a unique carrier grade, industry-leading solution. HP Helion OpenStack Carrier Grade is aligned with the ETSI-NFV architecture.

HP Helion OpenStack Carrier Grade includes two Linux host operating systems, server virtualization (KVM), network virtualization (vSwitch and SDN controllers), an installer and cloud lifecycle management framework, fault and performance management, and high-availability framework for the OpenStack control plane.

HP Helion OpenStack Carrier Grade is based on HP Helion OpenStack 2.0 but with significantly enhanced and optimized functionality, availability, scale and performance to meet the needs of NFV cloud deployments.

HP Helion OpenStack Carrier Grade includes following key components:

- OpenStack—core services including Horizon, Nova, Neutron, Cinder, Glance, Swift, Keystone, Ceilometer, and Heat.
- Compute node software package that includes:
  - Carrier-grade Linux (host operating system [OS] running on the compute nodes)
  - Carrier-grade KVM (for virtualization of the compute node)
  - Carrier-grade virtual switch, data plane development kit (DPDK)-enabled high-performance virtual switch
- Management and middleware—composed of high-availability (HA) management; operations, administration, and maintenance (OAM); software image management; and fault and performance management
- Guest software development kit (SDK) for inclusion in the guest OS of the virtual network functions (VNF) for performance acceleration and improving the HA framework above and beyond standard VIMs.

Primary Users

Telecom companies desiring cloud-based Network Function Virtualization (NFV).

Standard Features

Feature	Description
Availability and reliability	• Advanced self-healing • No single point of failure
Platform for high performance VNFs	• Near-line rate networking throughout for VNFs like vEPC, vBRAS, vIMS, vFW, vRouter etc. • Bare metal compute performance
Manageability	• In-service upgrade capabilities • Enhanced security • Inventory management • Advanced resource scheduling and orchestration capabilities
High Availability/ Disaster Recovery	• NIC Bonding at the server level • HA for KVM instance • Compute Node failure detection and Auto-evacuation in the KVM region • Live Migration in the KVM region

Core HP Helion OpenStack Carrier Grade Capabilities

Core capabilities unique to HP Helion OpenStack Carrier Grade include:

Backup and Restore

HP Helion OpenStack Carrier Grade includes a backup and restore application called Attis which you can use to backup and restore essential system files and components of the non-KVM cloud. Attis is automatically installed on each of the controller nodes in the non-KVM region. For more information, see *Backup and Restore Configuration Files and MySQL Clusters*.

For information on backing up and restoring the KVM region, see the *KVM-Region Administrator Guide*.

Multiple NIC Support

When launching a VM instance, you can specify multiple network interfaces.

Centralized Logging

The HP Helion OpenStack Carrier Grade Centralized Logging feature collects logs on a central system, rather than leaving the logs scattered across the network. The administrator can use a single Kibana interface to view log information in charts, graphs, tables, histograms, and other forms. For more information, see *Centralized Logging*.

Installation Options

HP Helion OpenStack Carrier Grade has four deployment models, depending on your system configuration. Specific installation templates are included in the download package to facilitate the deployment of your cloud.

You can find more information on the deployment options in the *Technical Overview*.

- KVM-based cloud only (using the Denver template)

External storage

You can integrate either HPE Storevirtual (VSA) or HP StoreServ (3PAR) storage in the KVM region.

- With HPE StoreVirtual VSA storage

  HPE StoreVirtual VSA software is a Virtual Storage Appliance that provides the complete array functionality on top of a Linux KVM environment without external hardware. VSA eliminates the need for external shared storage required to implement Block Storage features.
- With HPE StoreServ (3PAR) storage

  HPE 3PAR StoreServ is a storage array that supports Fibre Channel (FC) as well as iSCSI protocol.

You must install 3PAR or VSA before starting the HP Helion OpenStack installation and are independent of HP Helion OpenStack Carrier Grade.

Unbonded or Bonded NIC configuration

The HP Helion OpenStack Carrier Grade installation allows for network interface card bonding (bonded NIC).

Service Overviews

HP Helion OpenStack Carrier Grade is comprised of a number of services, including several OpenStack and HP Helion OpenStack services.

For more information, see *Services Overview*.

High-Performance Networking

HP Helion OpenStack Carrier Grade provides significantly improved network performance over the default OpenStack solution through a guest application on a virtual machine.

Virtual switching is a key function within data centers based on Software Defined Networking (SDN) as well as telecom infrastructures that leverages Network Functions Virtualization (NFV).

In the NFV scenario, for example, the virtual switch (vSwitch) is responsible for switching network traffic between the core network and the virtualized applications or Virtual Network Functions (VNFs) that are running in Virtual Machines (VMs). Based on your deployment model, you will use either:

Accelerated vSwitch (AVS). AVS is integrated into the servers in the KVM region. AVS is an optimization of Open vSwitch (OVS) technology for NFV environments. Open vSwitch is a multilayer software switch licensed

under the open source Apache 2 license. AVS provides connectivity between virtual machines on the same compute node, and between virtual machines and external networks. AVS is for customers who are focused on Virtualized Infrastructure Manager (VIM) key features like line rate performance and high availability.

AVS supports a variety of network connectivity options with the hosted virtual machines, as follows:

- Unmodified guests can use Linux networking and virtio drivers. This provides a mechanism to bring existing applications into the production environment immediately.
- Guest applications can be modified to leverage the Accelerated Virtual Port (AVP) drivers provided with the HP Helion OpenStack Carrier Grade. AVP ports provide increased throughput over plain virtio drivers when connected to the AVS.
- For the highest performance, guest applications can also be modified to make use of the Intel DPDK libraries and the AVP poll-mode drivers provided by the HP Helion OpenStack Carrier Grade to connect with the AVS Switch.

In addition to AVS, HP Helion OpenStack Carrier Grade incorporates DPDK-Accelerated Neutron Virtual Router L3 Forwarding (AVR). Accelerated forwarding is used between directly attached tenant networks and subnets, as well as for gateway, SNAT, and floating IP functionality.

AVS is included in the Denver deployment of HP Helion Carrier Grade. The *Technical Overview* describes these deployments.

High-Availability Extensions

HP Helion OpenStack Carrier Grade (in the KVM region) provides a number of extensions to OpenStack to deliver highly available hosting of virtual machines, including:

1:1 OpenStack controller services

Automatic configuration of the OpenStack controller services in 1:1 active/standby mode across two controller nodes.

Fast detection of compute host failures

Implemented by using a highly efficient and highly scalable heartbeat protocol between the controller and compute nodes.

Fast recovery of virtual machines instances upon detection of a compute node failure

Extensions to Nova services that automatically re-schedule impacted virtual machine instances to available alternative compute nodes in the cluster.

Fast recovery of tenant network services upon detection of a compute node failure

Extensions to Neutron that automatically re-schedule impacted network services such as DHCP, L3 Routing, and User/Meta data server, for all affected tenant networks. This covers tenant networks spanning multiple compute nodes.

Fast and enhanced detection of virtual machines failures

Failure of any KVM/QEMU instance is automatically reported by the death process notification.

Additionally, modified guests can make use of the HP Helion OpenStack Carrier Grade Guest Heartbeat Library to register application-specific health check callbacks with the virtual machine. This registration allows Nova compute extensions on the host compute node to monitor the health of the guest application. The frequency of the health checks is determined at registration time. The semantics of the health check, that is, determining when the application is in a good or a bad state, is under the control of the application itself.

Automatic recovery of failed virtual machine instances

Extensions to Nova that automatically re-start a failed virtual machine on the same compute node. If the re-start operation fails, the virtual machine is re-scheduled to use an alternative compute node.

Virtual machine server groups

Named groups of virtual machines instances to which a common set of attributes are applied, including:

- compute node affinity or anti-affinity
- maximum number of virtual machine instances
- best effort or strict affinity policy

Virtual machines in the same server group can use a server group messaging API for low-bandwidth communications.

In a typical use of a virtual machine server group, guest applications in active/standby pairs are deployed on different compute nodes to protect them from hardware failures.

Live migration support with DPDK-accelerated networking

Live migration support for virtual machines using the HP Helion OpenStack Carrier Grade high-performance networking options.

Graceful shutdown (and other operations) of virtual machines

Nova extensions that turn the default shutdown operation of virtual machines into an ACPI shutdown. Guest applications can therefore register shutdown scripts using standard ACPI mechanisms to execute operations such as closing files, updating persistent databases, or cleanly disconnecting from subscribed services.

Optionally, guest applications can use the HP Helion OpenStack Carrier Grade Guest Heartbeat Library to register to receive process management requests such as shutdown, live-migrate, pause, auto-scale, and others. The guest applications can then reject the requests based upon application-specific state directives, or prepare for a graceful execution.

Link Aggregation (LAG) support

Support for LAG, also known as Aggregate Ethernet, on controller and compute nodes for link protection.

Protected HA Middleware

HP Helion OpenStack Carrier Grade HA middleware is protected by a process monitor that uses death process notification to detect and respawn critical HA processes.

Performance Management Extensions

The Ceilometer service in the HP Helion OpenStack Carrier Grade features improved performance, scalability, and usability. It has been extended to support a CSV-formatted file backend that provides a more traditional Telco Northbound interface for performance management.

Heat Extensions

The OpenStack Heat orchestration service is enhanced to include:

- Support for several missing resource types in the public reference implementation
- Helpful example templates illustrating real reference scenarios

Virtual Machine Performance

HP Helion OpenStack Carrier Grade provides an improved execution environment for virtual machines that contributes to their overall performance when deployed on the compute nodes in the KVM region. Enhancements to the execution environment include:

- Low-latency, bounded delivery of virtual interrupts, and availability of low-latency high resolution timers.
- Option to allocate 2 MB or 1 GB huge memory pages to reduce swapping and TLB lookup misses.
- Improved resource tracking of VMs that use dedicated CPUs, to ensure successful migration and evacuation.
- Support for affining guest NUMA nodes to specific host NUMA nodes.
- Capability to specify specific CPU models to be used by a virtual machine in order to leverage advanced features of the CPU architecture.

Guest VLANs

HP Helion OpenStack Carrier Grade guests can make use of VLANs to encapsulate IP traffic from a single or multiple IP subnets on a virtual Ethernet interface. This capability facilitates the porting of current user applications running on dedicated physical servers using VLANs to a virtualized environment.

HP Helion OpenStack Carrier Grade tenants can define multiple IP subnets on a single tenant network, get their traffic encapsulated on VLAN IDs of their choice, and still benefit from the underlying functionality provided by the AVS and the overall virtualized network infrastructure.

Ethernet Interface Types

You can connect a VM directly to a physical interface using PCI passthrough or SR-IOV. You can choose either method by selecting `pci-sriov` or `pci-passthrough` as the network type when creating interfaces.

PCI Passthrough. A passthrough Ethernet interface is a physical PCI Ethernet NIC on a compute node to which a virtual machine is granted direct access. This minimizes packet processing delays but at the same time demands special operational considerations. For all purposes, a PCI passthrough interface behaves as if it were physically attached to the virtual machine.

Instructions for configuring SR-IOV are available after for installation, see *Configuring PCI-Passthrough*

SR-IOV. A Single-Root I/O Virtualization (SR-IOV) Ethernet interface is a physical PCI Ethernet NIC that implements hardware-based virtualization mechanisms to expose multiple virtual network interfaces that can be used by one or more virtual machines simultaneously.

When compared with a PCI Passthtrough Ethernet interface, an SR-IOV Ethernet interface:

- Provides benefits similar to those of a PCI Passthtrough Ethernet interface, including lower latency packet processing;
- scales up more easily in a virtualized environment by providing multiple Virtual Functions (VF) that can be attached to multiple virtual machine interfaces;
- shares the same limitations, including the lack of support for LAG, QoS, ACL, and live migration;
- has the same requirements regarding the VLAN configuration of the access switches;
- provides a similar configuration workflow when used on HP Helion OpenStack Carrier Grade.

Instructions for configuring SR-IOV are available after for installation, see *Configuring SR-IOV*.

Power Management

A cloud orchestration service that monitors and manages the resource usage on the compute nodes to power down servers during periods of low usage. This service contributes to saving power and operational costs.

By continuously monitoring the resource usage, the power management service can de-fragment the service cloud by live-migrating virtual machine instances onto a smaller set of compute nodes. Unused hosts can then be manually powered down.

As the cloud usage levels rise, unused compute nodes can be manually powered on to host new virtual machine instances.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Non-KVM Region Overview

For installation and maintenance, HP Helion OpenStack Carrier Grade consists of three logical or conceptual *regions*: Non-KVM, KVM, and the optional baremetal.

A server in the Non-KVM region hosts the lifecycle manager, which contains the installation scripts and configuration files to deploy and maintain HP Helion OpenStack Carrier Grade; and HP Helion OpenStack, a commercial-grade distribution of OpenStack.

Note: These regions do not function as OpenStack regions.

Lifecycle Manager

All four deployment models install the lifecycle manager into the non-KVM region.

The Non-KVM environment includes a full installation of a lifecycle manager, an application that is used to deploy HP Helion OpenStack Carrier Grade and can be used for ongoing operations and maintenance of the system.

- **Physical Node Preparation.** The lifecycle manager can configure nodes prior to installation of a base operating system, including node discovery/inventory, BIOS configuration, (specifically setting PXE boot on primary interface), GRUB settings, RAID setup for local disks, iLO/IPMI set up and firmware upgrades.

- **OS Install.** The lifecycle manager takes a PXE bootable node and installs a base operating system.
- **Cloud Configuration.** The lifecycle manager can provide detailed information about the cloud topology, such as the structure of control plane, assignment of services to nodes, and service configuration. You can also specify environment-specific configurations.
- **OS Configuration.** The lifecycle manager can automatically execute operating system configuration values, such as NIC assignments, NTP settings, DNS settings, NIC bonding, sysctl settings, VLAN creation and so forth. The lifecycle manager uses the Ansible data model output and server playbooks to automatically apply the per-node configurations.
- **Helion Operation & Maintenance.** The lifecycle manager is responsible for the deploy, upgrade and maintenance lifecycle of the HP Helion OpenStack Carrier Grade system.

HP Helion OpenStack

All four deployment models install HP Helion OpenStack into the non-KVM region.

HPE Helion OpenStack2.0 is the latest OpenStack-based infrastructure-as-a-service cloud platform release from HP. It is based on the OpenStack Kilo release and implements core services and features of Kilo while providing new installation and management features.

HP Helion OpenStack offers many services based on the different OpenStack projects to provide the functionality you need. Visit the *HP Helion OpenStack Services Overview page* for a complete list of services.

HP Helion OpenStack® Carrier Grade 2.1 Beta: KVM Region Overview

For installation and maintenance, HP Helion OpenStack Carrier Grade consists of three logical or conceptual *regions*: Non-KVM, KVM, and baremetal.

Note: These regions do not function as OpenStack regions.

The HP Helion OpenStack Carrier Grade KVM region is a high-performance, high-availability, cloud operating system that enables telecommunications operators to use Commercial-off-the-shelf (COTS) hardware to manage Virtualized Network Functions (VNF) within a carrier grade Network Function Virtualization (NFV) architecture.

The KVM region includes the critical run-time components and lifecycle development tools, services, and developer support needed to successfully build and deploy a virtualized network running multiple VMs.

- TL 9000 design methodology to guarantee six nines reliability
- Full 10 G line rate accelerated virtual switching running unmodified guest applications
- 10 microsecond deterministic interrupt latency to support virtualization in the most stringent customer-provided equipment (CPE) and access sections of the network
- Accelerated live VM migration, including the share nothing model, which is faster than enterprise software
- 500 km geographical redundancy over a standard IP network; more over dedicated fiber
- Detection of failed controllers, hosts, or VMs 60x faster than enterprise Linux; automatic recovery, with no single point of failure
- Fully integrated telecom-grade security, including complete AAA access control
- Involvement in trials with the European Telecommunications Standards Institute (ETSI) and other standards bodies

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Denver Deployment Technical Overview

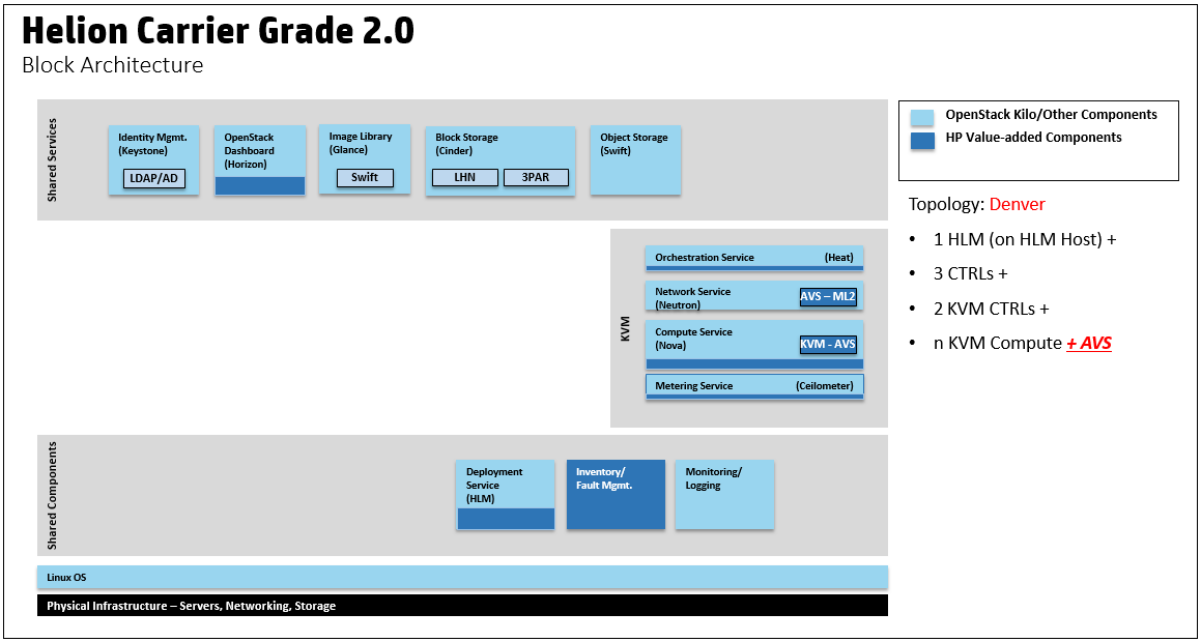
This page introduces deployment and network architectures of the Denver deployment of HPE Helion OpenStack Carrier Grade. During the installation, use the `denver` template that comes with the installation package.

Note: The Denver deployment is for proof-of-concept (POC) only and is not intended for production environments.

Services overview

HP Helion OpenStack Carrier Grade is comprised of several integrated OpenStack services. Each service works through an API (application programming interface) that allows services to work together and allows users to interact with the services. For a complete description of these services, see the *Services Overview* page.

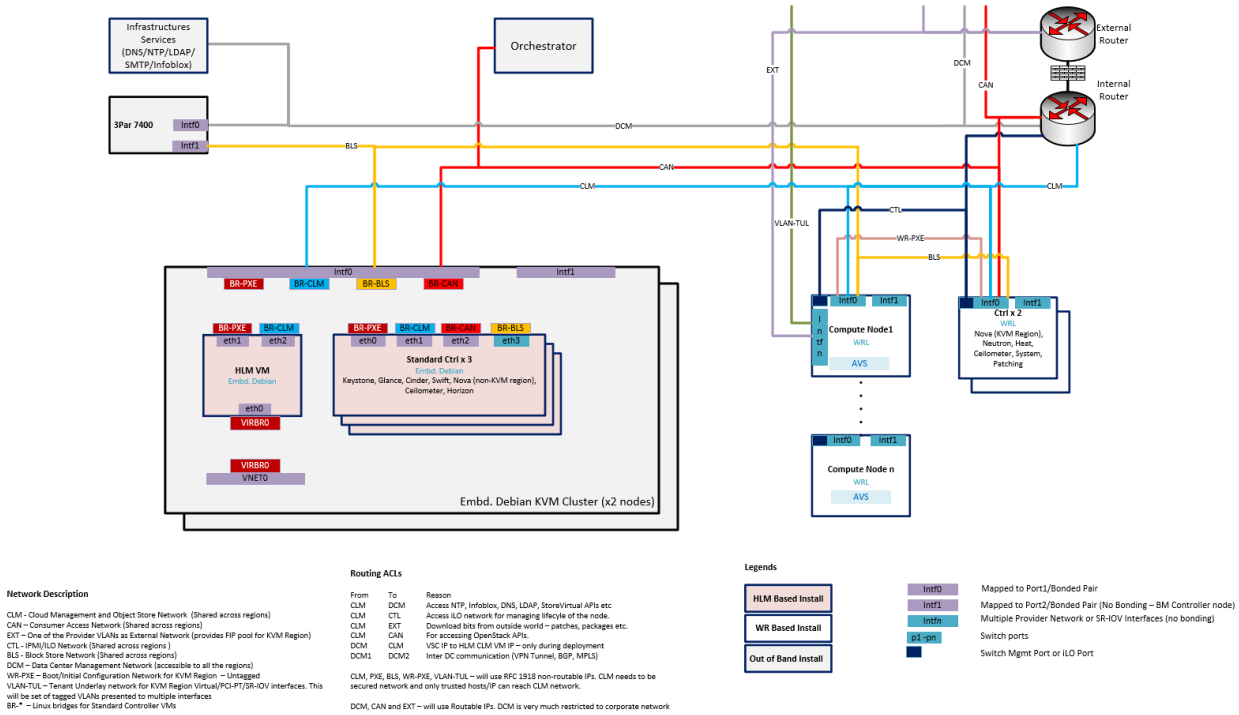
Network/Component Architecture



- *Deployment architecture*
- *Network architecture*

Deployment architecture

The following diagram depicts a simplified deployment scenario of HP Helion OpenStack Carrier Grade.



Note: Use the browser tools to expand and zoom in on the image as needed. Many browsers allow you to view only the image and have tools to zoom.

The following sections describe essential aspects of this diagram.

Network architecture

The following information describes the network configuration, which must be configured by the network administrator.

Network	Description
CLM	Cloud Management Network. Shared between the Non-KVM and KVM regions.
CAN	Consumer Access Network Shared between the Non-KVM and KVM regions.
EXT	Provider VLAN as an External network (provides that FIP pool for the KVM region).
CTL	IPMI/iLO network. Shared between the Non-KVM and KVM regions.
BLS	Block Storage Network. Shared between the Non-KVM and KVM regions.
DCM	Data Center Management network (accessible to KVM region) and route across multiple data centers.
WR- PXE	Boot/initial configuration network for non-KVM region controllers. Untagged
VLAN-TUL	Tenant Underlay Network for the KVM region Virtual/ PCI-PT/SR-IOV interfaces. This is a set of tagged VLANs presented to multiple interfaces.

Network	Description
BR*	Linux bridges for standard controller VMs.

Interfaces

The following are the interfaces being used, based on the technical architecture diagram. You can use more than two interfaces and specific networks to physical networks.

- Intf0 is mapped to Port1/Bonded Pair
- Intf1 is mapped to Port2/Bonded Pair
- Intf*n* are Multiple Provider Networks or SR-IOV interfaces (no bonding).

Also note the following required interfaces:

- Switch ports
- Switch management port or iLO port

Routing ACLs

Configure the following routing access lists.

From	To	Reason
CLM	DCM	Access NTP, DNS, LDAP, StoreVirtual APIs, and so forth
CLM	CTL	Access iLO network for managing the lifecycle of the node
CLM	EXT	Access external public network
CLM	CAN	Access OpnStack APIs
DCM	CLM	VSC IP to lifecycle manager CLM VM IP - only during deployment
DCM1	DCM2	Inter-datacenter communications (VLAN tunnel, BGP, MPLS)

CLM, PXE, BLS, WR-PXE, VLAN-TUL should use RFC 1918 non-routable IPs to prevent access to these networks from DCM, CTL, or EXT.

DCM, CAN, and EXT should use routable IP addresses. DCM should be restricted to the corporate network.

Service Architecture Diagram

For service architecture diagrams with interface details, see *Service Architecture Diagrams*

Regions

For installation and maintenance, HP Helion OpenStack Carrier Grade consists of two logical or conceptual *regions*: Non-KVM and KVM. You will see these terms used in the installation process. The *Deployment Architecture diagram* shows an illustration of these two zones.

Non-KVM

The Non-KVM region contains the lifecycle manager, to deploy and maintain HP Helion OpenStack Carrier Grade; and HP Helion OpenStack, a commercial-grade distribution of OpenStack.

KVM

The KVM region is the heart of HP Helion OpenStack Carrier Grade. The KVM region consists of a software platform, providing ultra-reliability and exceptional performance efficiencies for telecommunications networks.

Components

- **Lifecycle manager** The lifecycle manager deploys and manages HP Helion OpenStack Carrier Grade.
- **Non-KVM Region Controller**. Standard IaaS control plane to enable cloud-to-cloud communication.
- **StoreVirtual/3PAR**: Hardware storage array used as backend for Cinder. Support for 3PAR has a similar architecture as StoreVirtual on iSCSI, not Fibre.
- **KVM Region Controller**: Real-time control plane for compute and networking. Contains modified versions of most of the OpenStack components.
- **KVM Region Compute**: Realtime compute node with networking components.
- **Orchestrator**: This could be any application consuming the cloud services.

Data

Data name	Confidentiality	Integrity	Availability	Backup?	Description
Cloud Definition	Confidential	High	Low	Yes	Control plane and network topology and mapping to data center (input to HLM)
Cloud Configuration	Confidential	High	Low	Yes	Configuration of services in cloud (output from HLM)
MySQL database	Confidential	High	High	Yes	Contains user preferences. Backup to Swift daily.
Logs	Confidential	High	Medium	Yes	Logs from all services
Credentials	Confidential	High	High	Yes	Inter-service authentication uses the credentials for each service

Ethernet Interfaces

All hosts in the server connect to at least the internal management network using an Ethernet interface. The ports used for this connection must support network booting and must be configured to be used as the primary booting device for normal operations.

Typically this means that they must be on-board ports, since in most BIOS/UEFI implementations only on-board ports can be configured for network booting. You can use ports on a 10 GB NIC instead, if these ports fulfill these requirements.

The following table illustrates the number and type of Ethernet ports required in two different installation scenarios.

NOTE: The following table assumes that each interface is connected to a single network. An Ethernet interface can be shared by more than one network.

Personality	Basic Scenario	LAG Scenario
Controller Node	• One 10G on-board interface (Internal management network)	• Two 10G on-board interfaces (Internal management network)

Personality	Basic Scenario	LAG Scenario
Compute Node	• One 10G on-board interface (Internal management network) • Two 10G (Intel 82599) interfaces per Provider Network	• Two 10G on-board interfaces (Internal management network) • Two 10G (Intel 82599) interfaces per Provider Network

In the basic scenario, a single Ethernet port is used to attach the host to each of the networks. In the LAG scenario, two Ethernet ports are used for each connection.

Board Management Modules

For out-of-band reset and power-on/power-off capabilities, DL360 or DL380 servers equipped with HPE iLO (Integrated Lights Out) board management modules are required. Each module must be connected using port-based VLAN to a switch that has access to the internal management network.

USB Interface

For the controller, a USB interface is required for backup and restore operations, and for software installation if a DVD is not available.

Network Requirements

The networking environment incorporates several types of network:

- the internal management network
- the OAM network
- one or more provider networks
- an optional infrastructure network
- an optional board management network.

Operational requirements for each network are described in the following sections.

Internal Management Network

The internal management network must be implemented as a single, dedicated, Layer 2 broadcast domain for the exclusive use of each server cluster. Sharing of this network by more than one server cluster is not a supported configuration.

During the server software installation process, several network services such as DHCP, and PXE, are expected to run over the internal management network. These services are used to bring up the different hosts to an operational state. Therefore, it is mandatory that this network be operational and available in advance, to ensure a successful installation.

On each host, the internal management network can be implemented using a 10 Gb Ethernet port. In either case, requirements for this port are:

- must be capable of PXE-booting
- can be used by the motherboard as a primary boot device

CAN/OAM Network

You should ensure that the following services are available on the CAN/OAM Network:

- DNS Service - Needed to facilitate the name resolution of servers reachable on the CAN/OAM Network.

  The server can operate without a configured DNS service. However, a DNS service should be in place to ensure that links to external references in the current and future versions of the web administration interface work as expected.

- NTP Service - The Network Time Protocol (NTP) can be optionally used by the server controller nodes to synchronize their local clocks with a reliable external time reference. However, it is strongly suggested that this service be available, among other things, to ensure that system-wide log reports present a unified view of the day-to-day operations.

The server compute nodes always use the controller nodes as the time server for the entire cluster.

Provider Network

There are no specific requirements for network services to be available on the provider network. However, you must ensure that all network services required by the guests running in the compute nodes are available. For configuration purposes, the compute nodes themselves are entirely served by the services provided by the controller nodes over the internal management network.

Infrastructure Network

This is an optional network.

As with the internal management network, the infrastructure network must be implemented as a single, dedicated, Layer 2 broadcast domain for the exclusive use of each server cluster.

Sharing of this network by more than one server cluster is not a supported configuration.

The infrastructure network can be implemented as a 10 Gb Ethernet network. In its absence, all infrastructure traffic is carried over the internal management network.

Board Management Network

Board Management CTL (IPMI Control) Network External access to the board management network, the board management modules are assigned IP addresses accessible from the OAM network, and the controller uses the OAM network to connect to them.

Next Step

Review the *Support Matrix*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Services Overview

HP Helion OpenStack Carrier Grade is comprised of several integrated services. Each service works through an API (application programming interface) that allows services to work together and allows users to interact with the services.

This page contains the following information:

- *Service User Accounts*
- *OpenStack Services*
- *Dashboard services*
- *For more information*

In addition to the APIs, you can interact with the most services through a graphic user interface (dashboard or console) or a command line interface (CLI).

Service User Accounts

The HP Helion OpenStack Carrier Grade installation process creates a **service user** account for each installed service. Service user accounts require elevated privileges to validate end user tokens. It is therefore strongly recommended that you do ***not*** add these service user accounts to any project because this could allow project users to access services they should not have permission to access.

The service user accounts include, but are not limited to, the following:

- Nova
- Neutron
- Glance
- Cinder
- Heat
- Keystone
- Ceilometer

OpenStack Services

The following services are foundation technologies used by the HP Helion OpenStack Carrier Grde.

Compute Operations (Nova). The Compute service manages the hypervisors and virtual machines in your environment.

See *Overview of the Compute service*.

Networking Operations (Neutron). The Networking Operations service is a virtual networking service that leverages the OpenStack Neutron service to provide network connectivity and addressing to HP Helion OpenStack Carrier Grade devices.

See *Overview of the Network Operations service*.

Image Operations (Glance)

The Image Operations service is a web service for managing virtual machine images.

See *Overview of the Image Operations service*

Metering (Ceilometer). The Metering service enables a single infrastructure to collect measurements throughout your cloud environment.

See *Overview of the Metering service*.

Orchestration (Heat). The Orchestration service provides a template-based orchestration for describing a cloud application. A Heat template is a *YAML* file that describes the infrastructure for a cloud application. Templates contain vendor-independent specifications for launching a particular service or application.

See *Overview of the Orchestration service*.

Volume Operations (Cinder). The Volume Operations service enables you to attach storage volumes to the virtual instances in your cloud environment. The service provides persistent block level storage devices for use with your Compute instances.

See *Overview of the Volume Operations service*.

Identity Management (Keystone). The Identity Management service enables you to create and administer users and security groups, and control access to your cloud environment.

See *Overview of the Identity Management service*.

Ironic. HP Helion OpenStack leverages the OpenStack Ironic service during the installation for provisioning of the controller and KVM compute host in a baremetal deployment.

See *Overview of the Ironic Service*

Dashboard services

HP Helion OpenStack Carrier Grade uses the following services or software to present user interfaces to aspects of HP Helion OpenStack

Horizon. The Horizon service is the basis of the *HP Helion OpenStack Carrier Grade Dashboard* for creating and managing HP Helion OpenStack Carrier Grade resources. The Horizon dashboard is developed by HPE for use with HP Helion OpenStack

You can use the Horizon dashboard to view, allocate, and manage all virtual resources within a cloud. See *Horizon Service Overview*.

For more information

For information on how to operate your cloud we suggest you read the *Administrator Guide*

For more information on installing the command-line interface for interacting with services, see *installing the OpenStack command-line clients*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Compute Service (Nova) Overview

The HP Helion OpenStack Carrier Grade Compute service leverages the OpenStack Nova compute service to instantiate virtual machine instances on publicly accessible physical machines hosted in your cloud environment.

The Compute service allows you to work with **flavors**, which are unique combinations of disk space, memory capacity, and CPU; **images**, which are collections of files used as a base installation, typically operating systems such as Ubuntu 10.10; and **servers**, which are virtual instances created by combining a flavor and an image.

A variety of flavors and images are provided by the Compute service to create a wide mix of servers.

Working with the Compute Service

To perform tasks using the Compute service, you can use the dashboard, API or CLI.

Using the dashboards

You can use the *HP Helion OpenStack Carrier Grade Dashboard* to work with the Compute service.

Using the API

You can use a low-level, raw REST API access to the HPE Compute service. See the *OpenStack Compute API v2.0 Reference*.

Using the CLI

You can use the command-line interface software to access HPE Compute. See the *OpenStack Command Line Interface Reference*.

For more information on installing the CLI, see *Install the OpenStack command-line clients*.

For more information

For information on how to operate your cloud we suggest you read the *Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Networking Service (Neutron) Overview

The HP Helion OpenStack Carrier Grade Networking servi ce is a virtual networking service that leverages the OpenStack Neutron service to provide network connectivity and addressing to HP Helion OpenStack Carrier Grade devices.

The Networking service also provides an API to configure and manage a variety of network services.

You can use the Networking service to connect guest servers or you can define and configure your own virtual network topology.

Working with the Networking service

To perform tasks using the Networking service, you can use the dashboard, API or CLI.

Using the dashboards

You can use *HP Helion OpenStack Carrier Grade Dashboard* to work with the Networking service.

Using the API

You can use a low-level, raw REST API to access the Networking service. See the *OpenStack Networking API v2.0 Reference*.

Using the CLI

You can use any of several command-line interface software to access the Networking service. See the *OpenStack Command Line Interface Reference*.

For more information on installing the CLI, see *Install the OpenStack command-line clients*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Image Operations (Glance) Service Overview

Based on OpenStack Glance, the HP Helion OpenStack Carrier Grade Image Operations service is a web service for managing virtual machine images. It provides a set of RESTful APIs that enables querying/updating of image metadata as well as retrieval of the actual image data.

With the Image Operations service you can work with image files, which are virtual disk image files that the *Compute* service can use to create a virtual machine.

Each image has a name, an unique identifier (UUIDs in hexadecimal string notation) and a specific disc and container format.

Working with the Image Operations Service

To perform tasks using the Image Operations service, you can use the dashboard, API or CLI.

Using the dashboards

You can use the *Horizon dashdoard* to work with the Image Operations service.

Using the API

You can use a low-level, raw REST API access to HPE Image Operations service. See the *OpenStack Image Service API v2.0 Reference*.

Using the CLI

You can use any of several command-line interface software to access the Image Operations service. See the *OpenStack Command Line Interface Reference*.

For more information on installing the command-line interface for interacting with services, see *installing the OpenStack command-line clients*.

--.

For more information

For information on how to operate your cloud we suggest you read the *Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Block Storage Volume Operations (Cinder) Overview

The HP Helion OpenStack Carrier Grade Block Storage Volume Operations uses the OpenStack Cinder service to manage storage volumes, including creating volumes, creating volume snapshots, and configuring volumes.

Once created, you can easily disconnect block storage volumes from one instance and attach them to another. You can also create snapshots of these volumes.

Working with the Volume Operations Service

To perform tasks using the Volume Operations service, you can use the dashboard, API or CLI.

Using the dashboards

You can use the *HP Helion OpenStack Carrier Grade Dashboard* to work with the Volume Operations service.

Using the API

You can use a low-level, raw REST API for access to the Volume Operations service. See the *OpenStack Block Storage API v2.0 Reference*.

Using the CLI

You can use any of several command-line interfaces to access the Volume Operations service. See *OpenStack Command Line Interface Reference*.

For more information on installing the command-line interface for interacting with services, see *installing the OpenStack command-line clients*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Orchestration Service (Heat) Overview

The HP Helion OpenStack Carrier Grade Orchestration service leverages OpenStack Heat to provide template-based orchestration for describing a cloud application. It executes OpenStack API calls to generate running cloud applications.

Working with the Orchestration Service

To perform tasks using the Orchestration service, you can use the dashboard, API or CLI.

Using the dashboards

You can use the *HP Helion OpenStack Carrier Grade Dashboard* to work with the Compute service.

Using the API

You can use a low-level, raw REST API access to the Orchestration service. See the *OpenStack Orchestration API v1 Reference*.

Using the CLI

You can use any of several command-line interface software to access the Orchestration service. See the *OpenStack Command Line Interface Reference*.

For more information on installing the command-line interface for interacting with services, see *installing the OpenStack command-line clients*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Identity Service (Keystone) Overview

Based on Openstack Keystone, the HP Helion OpenStack Carrier Grade Identity service provides one-stop authentication using the Keystone V2 or V3 API.

The Identity service enables you to create and configure users, specify user roles and credentials, and issue security tokens.

The Identity service validates that incoming requests are being made by the user who claims to be making the call.

Users have a login and may be assigned tokens to access resources. Users can scope their authentication to a project (or, tenant) which then limits where and how their tokens can be used to interact with services. User roles, which are sets of rights and privileges, can be assigned to control access to projects.

The Identity service confirms that incoming request are being made by the user who claims to be making the call by validating a set of claims that the user is making. These claims are initially in the form of a set of credentials (username and password, or user access keys). After initial confirmation, the Identity service will issue a token that the user can provide to demonstrate that their identity has been authenticated when making subsequent requests.

Working with the Identity Service

To perform tasks using the Identity service, you can use the or .

To perform tasks using the Compute service, you can use the dashboard, API or CLI.

Using the dashboards

You can use the *HP Helion OpenStack Carrier Grade Dashboard* to work with the Identity service.

Horizon does not support Keystone v3 or domains by default. However, you can manually configure Horizon to use v3. For more information see: *Configuring Horizon for Keystone v3*.

Using the API

You can use a low-level, raw REST API access to the Identity service. See the *OpenStack Identity API v3*.

Using the CLI

You can use the command-line interface software to access the Identiry service. See the *OpenStack Identity service command-line client*.

For more information on installing the CLI, see *Install the OpenStack command-line clients*.

For more information

For information on how to operate your cloud we suggest you read the *Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Metering Service (Ceilometer) Overview

Note: The deployment of the Helion OpenStack v1.1 Metering service is considered experimental and targeted at developers investigating integration of external software applications with the Ceilometer API for showback, chargeback, and billing applications only. Only a limited set of metrics are available in the Helion OpenStack v1.1 release.

The HP Helion OpenStack Metering service leverages the OpenStack Ceilometer service. A metering service takes specified measurements of both physical and virtual resources, including physical servers and network devices such as switches and firewalls. No matter what purpose the data is used for, this service provides a reliable, consistent method for data collection.

Installation

The metering service is automatically installed as part of the Helion OpenStack installation process. It may be necessary to install the command-line interface (*CLI*) separately to perform various administrative tasks.

The initial default configuration enables a limited subset of all potential meters, collecting a few essential measurements from the Nova, Cinder, Glance, and Neutron services only. With these measurements, the Ceilometer API can begin collecting basic Helion OpenStack usage and status information.

Additional metrics collection for all of the Helion OpenStack infrastructure services, as well as other application and platform services, are targeted for future Helion OpenStack releases.

Working with Ceilometer

All the Ceilometer processes have a unified configuration file that can be found at */etc/ceilometer/ceilometer.conf* on the specific overcloud controller you are logged in to.

Access to Ceilometer is through the command-line interface *(CLI)*, or the low-level *REST API*. A Ceilometer Horizon dashboard panel is not available at this time.

For more information

For information on how to operate your cloud we suggest you read the *Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Ironic Service Overview

HP Helion OpenStack leverages the OpenStack Ironic service during the installation for provisioning of the controller and KVM compute host in a baremetal deployment.

Ironic is an OpenStack service to provision baremetal, not virtual, machines by leveraging common technologies such as PXE boot and IPMI to cover a wide range of hardware. Supporting pluggable drivers allows vendor-specific functionality to be added.

For more information

For information on Ironic, see OpenStack *Ironic's developer documentation*.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Horizon Service Overview

Horizon is the OpenStack service that serves as the basis for the HP Helion OpenStack Carrier Grade web interface or **dashboard**.

The dashboard provides a web-based user interface to HP Helion OpenStack Carrier Grade services including Compute, Volume Operations, Networking, and Identity.

The Horizon dashboard includes several tabs, including **Project**, **Admin**, **System** tabs. These tabs provide administrators and users with a graphical interface to access, provision and automate cloud-based resources.

For more information

For information on using the dashboards, see *How to Use the Helion Dashboard*.

For more information

For information on how to operate your cloud we suggest you read the *Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Release Notes

Thank you for your interest in HPE Helion OpenStack This document provides an overview of the features contained within HPE Helion OpenStack version 2.0, including known issues and workarounds, and where to find further information on the product release.

For more information on using HP Helion OpenStack Carrier Grade, see the *HP Helion OpenStack Carrier Grade Installation Guide*, the *HP Helion OpenStack Carrier Grade Administrator Guide* and the *HP Helion OpenStack Operations Guide*. For information on using the HP Helion OpenStack Carrier Grade Developer API, including API definitions and usage descriptions, see the *HP Helion OpenStack Carrier Grade API and SDK Reference*.

See:

- *Changes in this release* on page 22
- *Usage Caveats* on page 22

- *Known Problems and Limitations* on page 23

Changes in this release

The following enhancements were added for the HP Helion OpenStack Carrier Grade 2.0 release:

- Reduced control plane
- Support for restarting MySQL and RabbitMQ clusters after failure

Differences from HCG 2.0 Architecture

HP Helion OpenStack Carrier Grade 2.1 Architecture is built upon HP Helion OpenStack Carrier Grade 2.0 with the following key differences:

- **Virtual control planes.** The HP Helion OpenStack controllers are deployed onto virtual machines on a single host system. The controllers and the lifecycle manager are deployed on the same host system. In HP Helion OpenStack Carrier Grade, each of these components required a separate server.

Usage Caveats

Backup files in cloud directories can cause installation to fail

During the HP Helion OpenStack Carrier Grade installation, you will need to create and edit a number of JSON configuration files. You should create backups of these files, in the event you need to reinstall. Create the backups in a directory on `/root/` directory or on a remote system. Do not store backups of the JSON files inside your cloud directory or any where inside the `/var/hlm/clouds` directory.

VMs reported as ACTIVE before compute nodes are recovered

During a system recovery (for example, after a site power outage), when the controller is available but before the compute nodes are available, the Nova service shows an **Active** status for VMs . Until the compute nodes are available, this should be an **Error** status.

Controller swact raises spurious ssh security warning

On ssh login to the active controller after a controller swact, a security warning appears, saying the host identification has changed. This occurs because the ssh keys are not currently synchronized across controllers. It can be disregarded.

Mismatch of interface settings in LAG group

If the interfaces in a LAG group have mismatched speed or duplex settings, they are marked as incompatible by the system. To prevent this, ensure both interfaces in a LAG group use the same speed and duplex settings.

Storage or compute node must be re-added after MAC address change on management interface

For a compute or storage node, any change to the management interface configuration that results in a change of MAC address requires the node to be re-installed. The management interface MAC address can change if the physical Ethernet port is changed (for example, from eth1 to eth2), or if a LAG configuration is changed in a way that removes the Ethernet port associated with the LAG MAC address (for example, if the interface originally used for PXE boot is removed or replaced).

Instance cannot be launched with a specified port ID

Use of the `--port-id` parameter when launching an instance results in command failure.

Live migration resets uptime

When a VM is live-migrated, the uptime reported for the VM is reset to 0.

Interface network type cannot be changed directly from SRIOV to data

For an interface using network type "SRIOV," the network type must be changed to "none" before it can be changed to "data."

Glance image deletion does not release storage space

The storage space used by a glance image is not released when the image is deleted. To free the space for other uses, a glance-api restart is required.

Known Problems and Limitations

VMware VMK No Memory Error

When powering on the ESX Compute Proxy VM, you might receive a `VMK_NO_MEMORY` error. This is a known problem with HP server and ESXi 5.x.

To fix this issue, upgrade to HP AMS version 10.0.1 and above. See *Fixing the VMware VMK_NO_MEMORY Error*.

Use the CLI with the KVM Region

When working with the servers in the KVM region, do not use the Horizon interface. Please use the *OpenStack command-line interface CLI commands*.

Potential Vulnerability with Intel® LAN Products with SR-IOV

In Intel® LAN products with SR-IOV capability, the potential exists where, under specific conditions, Virtual Machines (VMs) can cause network congestion spreading, a well-known side-effect of Ethernet flow control, which could affect other VMs as well as the Hypervisor itself.

For more information, see the *bulletin in the Intel Security Center*.

Do not change OpenStack Service default passwords

Changing the default password for Swift, Glance, Cinder results in failing of their respective cloud admin operations.

Floating IP not working when SNAT is enabled

When router is configured either centralized (server default) or distributed , it is seen that Floating IP is not working.

To fix this issue, log onto `controller-0` for the KVM region and execute the following command to disable SNAT on the router:

```
neutron router-update <router-name> --external_gateway_info type=dict
 network_id=<network-id>,enable_snat=False
```

Unable to create new users through the Horizon UI

After logging into the Horizon interface as an `admin` user, an error occurs when you click **Create User** under the **Idenity** section.

You can create users with the OpenStack Keystone CLI commands. For axample:

```
keystone user-create --name <user-name> [--tenant <tenant>][--pass [<pass>]]
 [--email <email>][--enabled <true|false>]
```

For more information, see *OpenStack Command-Line Interface Reference*.

Unable to create new project through the Horizon Identity UI

After logging into the Horizon interface as an `admin` user, an error occurs when you click **Create Project** under the **Idenity** section.

You can create projects with the OpenStack Keystone CLI commands. For axample:

```
keystone tenant-create --name <tenant-name>
                [--description <tenant-description>]
                [--enabled <true|false>]
```

For more information, see *OpenStack Command-Line Interface Reference*.

Cinder Volume Backup is not working upon cloud deployment

Cinder Volume Backup is not working upon installation of HP Helion OpenStack Carrier Grade 2.0 The `cinder.backup.driver` file is not present in /etc/cinder/cinder.conf.

Bonding on the control interface is not supported

Due to an issue in `config_region` script, bonding on the control interface (hosts PXE, CLM, BLS, CAN networks) is not supported. A patch to support this feature is actively being worked upon.

Because of this issue, the data interface on the compute node does support balanced-xor bonding mode and Active/Standby modes.

StoreVirtual Cluster VIP not available on storage network.

If you cannot ping a specific virtual IP address on a StoreVirtual server, locate the host with the associated IP and reboot that server.

VXLAN not certified

The VXLAN feature has not been certified for HP Helion OpenStack Carrier Grade.

Cinder Block Storage snapshot feature not working

For HP Helion OpenStack Carrier Grade cloud using 3PAR iSCSI configured as the Cinder block storage service. The Cinder volume snapshot feature might not function properly if following entries are enabled in the `/etc/cinder/cinder.conf` file.

```
hp3par_snapshot_retention=48
hp3par_snapshot_expiration=72
```

To correct this issue, edit the `/etc/cinder/cinder.conf` file to disable these entries by commenting-out the entries, as follows:

```
#hp3par_snapshot_retention=48
#hp3par_snapshot_expiration=72
```

The `hp3par_snapshot_retention` entry is the time in hours to retain a snapshot.

The `hp3par_snapshot_expiration` entry is the time in hours when a snapshot expires and is deleted.

LDAP conflict causing error with templates

When deploying templates, such as `VMAutoScaling.yaml` you might receive a n error similar to the following:

```
Error: Can’t find role heat_stack_user
```

The problem is due to an inconsistency in the HP Helion OpenStack Carrier Grade LDAP implementation. To fix this problem, you should disable LDAP in Keystone and create few roles as mentioned below.

How you fix the problem depends upon whether your he HP Helion OpenStack Carrier Grade cloud is currently deployed.

If the cloud is not deployed

1. If the HP Helion OpenStack Carrier Grade cloud is not deployed, before deploying edit the `definition.json` file to set `ldap_enabled` to 0.

   ```
   "ldap_enabled": 0,
   ```

   This setting causes the cloud to deploy with SQL as Keystone backend instead of LDAP.
2. After you deploy the cloud, create the following roles in the Keystone by logging on to one of the controller nodes:

a. Source the stackrc file:

```
source stackrc
```

b. Execute the following command to create the heat_stack_owner role:

```
keystone role-create --name heat_stack_owner
```

c. Execute the following command to create the heat_stack_owner role:

```
keystone role-create --name heat_stack_user
```

If the cloud is currently deployed

1. After the cloud is deployed, on each controller, modify the `/etc/keystone/keystone.conf` to comment-out the LDAP entry and uncomment SQL driver, as shown:

```
[identity]
driver = keystone.identity.backends.sql.Identity
#driver = keystone.identity.backends.ldap.Identity
```

2. Create the following roles in the Keystone by logging on to one of the controller nodes:

   a. Source the stackrc file:

```
source stackrc
```

   b. Execute the following command to create the heat_stack_owner role:

```
keystone role-create --name heat_stack_owner
```

   c. Execute the following command to create the heat_stack_owner role:

```
keystone role-create --name heat_stack_user
```

Non-shared services do not work from Horizon dashboard

1. Go to each controller node in the non-KVM region and replace `user.py` file in the following location: `/opt/stack/venvs/horizon/lib/python2.7/site-packages/openstack_auth/user.py`
2. Restart apache2 service

LAG for the KVM region control plane does not work

Link aggregation groups (LAG) are not supported in the KVM region control plane. This is a known limitation that is scheduled to be corrected with the HP Helion OpenStack Carrier Grade GA release. A LAG is a mechanism that allows multiple parallel Ethernet network connections between two hosts to be used as a single logical connection.

SR-IOV limitations

- SR-IOV is supported only for Intel 82599.
- The maximum number of VFs per NIC is 32.
- SR-IOV and PCI passthrough cannot both be used on the same provider network.
- SR-IOV is not supported on Mellanox NICs.

Interface or interface consolidation limitations

- VLAN over bonded interface without an assigned network type is not supported.
- Addition of an infrastructure interface after installation is not functional.
- Consolidation of the infrastructure network over the OAM network is not supported.
- Stacked VLANs are not supported. On a consolidated management or infrastructure interface, a VLAN provider network can be associated directly with the untagged interface; however, flat or VXLAN provider networks must be associated with a consolidated VLAN data interface.

- Interface profiles cannot be created for VLAN interface types.
- The `system host-if-modify-ports` command is deprecated.

Mellanox CX-3 NICs limitations

- Mellanox CX-3 NIC is supported for use in the AVS vSwitch only.
- For a Mellanox CX3, all ports must be used ether for data interfaces, or for non-data interfaces. It is not possible to use some ports for data interfaces and others for non-data interfaces on the same Mellanox CX3 NIC.
- Jumbo frames are not supported on Mellanox NICs.
- SR-IOV, PCI-Passthrough are not supported on Mellanox NICs.

Installation does not fully utilize disks greater than two terabytes

HP Helion OpenStack Carrier Grade in the KVM region can be installed on disks greater than 2 TB, but only 2 TB of the disk is useable.

Guest heartbeat and notification features are not fully validated.

Heartbeat and notification services for VMs are not fully validated.

Cinder API version generates a log warning

The V1 API for Cinder in use by this version of HP Helion OpenStack Carrier Grade is deprecated, resulting in log warnings.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Applying Customer-Specific Branding (optional)

You can optionally apply customer-specific branding by including a branding tarball.

For more information on creating the branding tarball, see the instructions in the `wrs-branding-1.0.0.tgz` in the HP Helion OpenStack Carrier Grade SDK tarball.

This component contains instructions and examples for adding custom branding to the Horizon GUI. You can modifythe existing style sheet, font, and image files to develop your own branding, and then apply the branding by installinga tarball that includes the modified files along with a manifest.

The branding tarball can be applied at various stages. The steps for each stage are described below.

Note:

The recommended method is to install the tarball before running the controller configuration script.

1. Log into the active controller using the CLI.
2. Delete any previous tarball from the `/opt/branding` directory.
3. Copy the new branding tarball to the `/opt/branding` directory.
4. Install the branding.

   To install the branding as part of initial system configuration, run the configuration controller script.

   If you have already run the controller configuration script, you can install the branding as follows:

   a. Ensure that any previous tarballs are deleted from the `/opt/branding` directory.
   b. Ensure that the new branding tarball is copied to the `/opt/branding` directory.
   c. Execute the following command:

      ```
      sudo service horizon restart
      ```

      This processes the branding files on the active controller.
   d. Lock the inactive controller.
   e. Unlock the inactive controller.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Installation

This document describes the process for installing HP Helion OpenStack Carrier Grade.

About the installation

The HP Helion OpenStack Carrier Grade installation installs a virtual machine for the lifecycle manager VM, creates a base HP Helion OpenStack cloud, and deploys a carrier grade cloud.

After installation, you can interact with the HP Helion OpenStack cloud using the *Horizon graphical interface* or using the CLIs of the respective *services* to manage hypervisors and provision virtual machines.

Before you begin

Before you begin, make sure you review the Technical Overview and Support Matrix for your deployment model:

- *Technical Overview*
- *Support Matrix*

KVM Topology using the Denver Deployment

If installing the Denver template, you are installing the KVM region and HP Helion OpenStack Carrier Grade *Accelerated vSwitch (AVS)* networking.

You can also integrate HPE Storevirtual (VSA) or HPE StoreServ (3PAR) storage in the KVM region.

You must install 3PAR or VSA before starting the HP Helion OpenStack installation and are independent of HP Helion OpenStack Carrier Grade. During the installation, you will integrate the storage into HP Helion OpenStack Carrier Grade. See the installation instructions for the 3PAR and/or VSA parameters you will need.

Start *installing the Denver deployment*.

Installation Troubleshooting

Check with the *Installation Troubleshooting page* for tips and work-arounds in case you run into issues while installing.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Deploying the Denver Template

This document describes the process for installing HP Helion OpenStack Carrier Grade.

About the installation

The HP Helion OpenStack Carrier Grade Denver Deployment installs the lifecycle manager, creates a base HP Helion OpenStack cloud, configures network virtualization through Accelerated vSwitch (AVS), and deploys a carrier grade cloud.

After installation, you can interact with the HP Helion OpenStack cloud using the *Horizon graphical interface* or using the CLIs of the respective *services*.

KVM Topology using the *denver* template

If installing the `denver` template, you are installing the KVM region and HP Helion OpenStack AVS networking.

You can also integrate HPE Storevirtual (VSA) or HPE StoreServ (3PAR) storage in the KVM region.

You must install 3PAR or VSA before starting the HP Helion OpenStack installation and are independent of HP Helion OpenStack Carrier Grade. During the installation, you will integrate the storage into HP Helion OpenStack Carrier Grade. See the installation instructions for the 3PAR and/or VSA parameters you will need.

Unbonded or Bonded NIC configuration

During the installation, specific steps might be different, based on whether you are installing into a single NIC or bonded NIC environment.

Installation information

Before starting the installation, review the following topics:

Use the following process to install HP Helion OpenStack Carrier Grade.

- *Technical Overview* for information on the HP Helion OpenStack Carrier Grade environment.
  - Review the Cloud Topologies to decide appropriate topology for your use case.
  - Review the deployment architecture for different hypervisors
  - Review the network architecture for networking needs
- *Technical Specifications* for dimensions and limits of the current versrion of HP Helion OpenStack Carrier Grade.
- *Support Matrix* to make sure your environment meets the minimum requirements.

Installation process

Use the following process to install HP Helion OpenStack Carrier Grade.

1. Perform any required or optional *installation prerequisites*.
2. *Prepare the network for installation*
3. Install *the Lifecycle Manager*.
4. Install the *HPE Helion OpenStack cloud*. These components will be installed into what is called the *Non-KVM region*.
5. Launch the *Helion user interface*.
6. Install the *carrier grade cloud*. The carrier grade cloud is deployed into what is called the *KVM region.*
7. After the deployment is complete, do a full backup of the deployment. This will make it easier to recover should you encounter a problem. For more information, see *Backup and Restore Configuration Files*.

First Step

Perform the *prerequisite steps* required to install HP Helion OpenStack Carrier Grade.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Denver Deployment Technical Overview

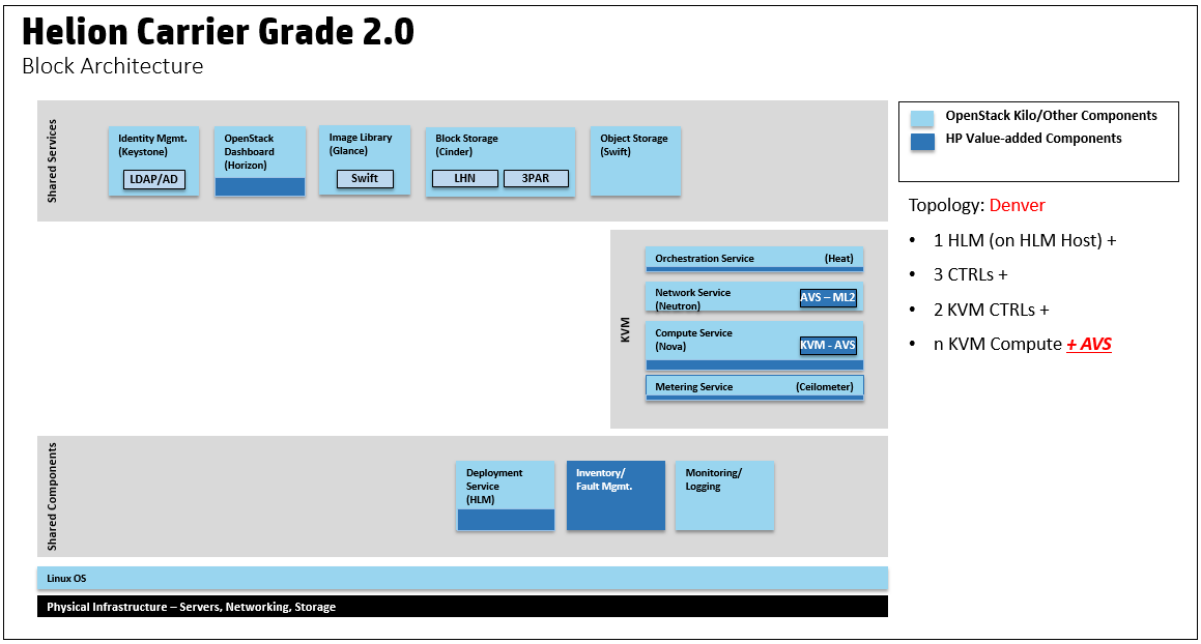
This page introduces deployment and network architectures of the Denver deployment of HPE Helion OpenStack Carrier Grade. During the installation, use the `denver` template that comes with the installation package.

Note: The Denver deployment is for proof-of-concept (POC) only and is not intended for production environments.

Services overview

HP Helion OpenStack Carrier Grade is comprised of several integrated OpenStack services. Each service works through an API (application programming interface) that allows services to work together and allows users to interact with the services. For a complete description of these services, see the *Services Overview* page.

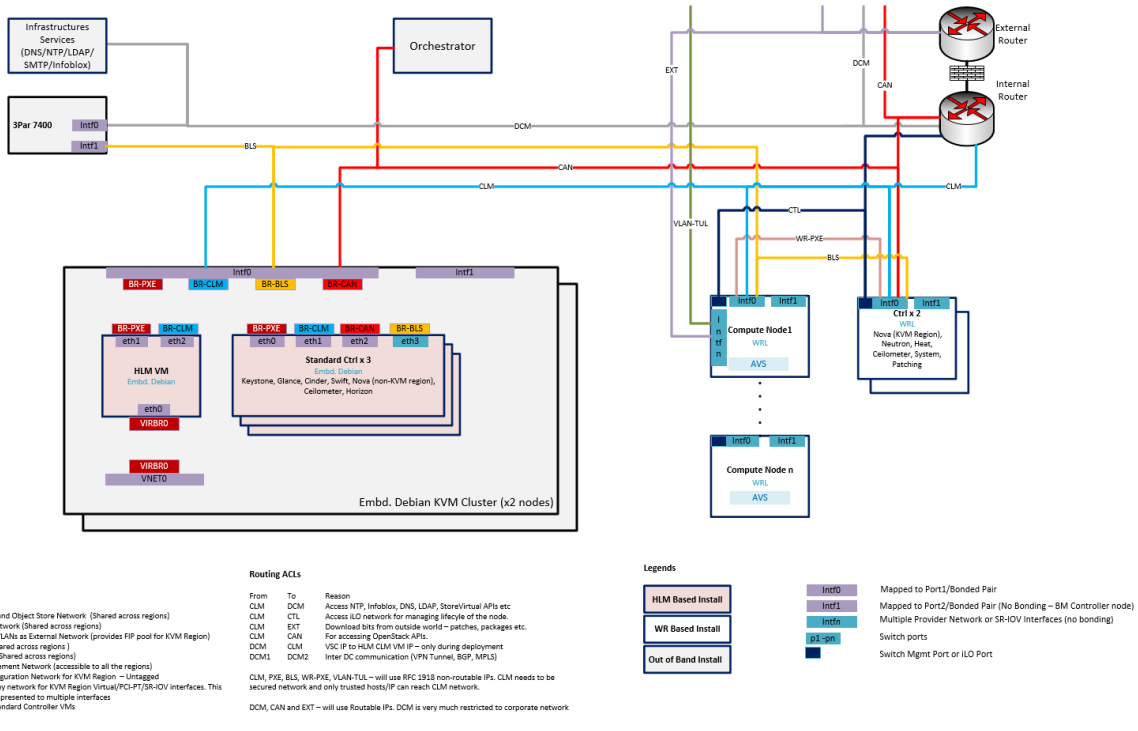
Network/Component Architecture



- *Deployment architecture*
- *Network architecture*

Deployment architecture

The following diagram depicts a simplified deployment scenario of HP Helion OpenStack Carrier Grade.



Note: Use the browser tools to expand and zoom in on the image as needed. Many browsers allow you to view only the image and have tools to zoom.

The following sections describe essential aspects of this diagram.

Network architecture

The following information describes the network configuration, which must be configured by the network administrator.

Network	Description
CLM	Cloud Management Network. Shared between the Non-KVM and KVM regions.
CAN	Consumer Access Network Shared between the Non-KVM and KVM regions.
EXT	Provider VLAN as an External network (provides that FIP pool for the KVM region).
CTL	IPMI/iLO network. Shared between the Non-KVM and KVM regions.
BLS	Block Storage Network. Shared between the Non-KVM and KVM regions.
DCM	Data Center Management network (accessible to KVM region) and route across multiple data centers.
WR- PXE	Boot/initial configuration network for non-KVM region controllers. Untagged
VLAN-TUL	Tenant Underlay Network for the KVM region Virtual/ PCI-PT/SR-IOV interfaces. This is a set of tagged VLANs presented to multiple interfaces.
BR*	Linux bridges for standard controller VMs.

Interfaces

The following are the interfaces being used, based on the technical architecture diagram. You can use more than two interfaces and specific networks to physical networks.

- Intf0 is mapped to Port1/Bonded Pair
- Intf1 is mapped to Port2/Bonded Pair
- Intf*n* are Multiple Provider Networks or SR-IOV interfaces (no bonding).

Also note the following required interfaces:

- Switch ports
- Switch management port or iLO port

Routing ACLs

Configure the following routing access lists.

From	To	Reason
CLM	DCM	Access NTP, DNS, LDAP, StoreVirtual APIs, and so forth
CLM	CTL	Access iLO network for managing the lifecycle of the node
CLM	EXT	Access external public network
CLM	CAN	Access OpnStack APIs

From	To	Reason
DCM	CLM	VSC IP to lifecycle manager CLM VM IP - only during deployment
DCM1	DCM2	Inter-datacenter communications (VLAN tunnel, BGP, MPLS)

CLM, PXE, BLS, WR-PXE, VLAN-TUL should use RFC 1918 non-routable IPs to prevent access to these networks from DCM, CTL, or EXT.

DCM, CAN, and EXT should use routable IP addresses. DCM should be restricted to the corporate network.

Service Architecture Diagram

For service architecture diagrams with interface details, see *Service Architecture Diagrams*

Regions

For installation and maintenance, HP Helion OpenStack Carrier Grade consists of two logical or conceptual *regions*: Non-KVM and KVM. You will see these terms used in the installation process. The *Deployment Architecture diagram* shows an illustration of these two zones.

Non-KVM

The Non-KVM region contains the lifecycle manager, to deploy and maintain HP Helion OpenStack Carrier Grade; and HP Helion OpenStack, a commercial-grade distribution of OpenStack.

KVM

The KVM region is the heart of HP Helion OpenStack Carrier Grade. The KVM region consists of a software platform, providing ultra-reliability and exceptional performance efficiencies for telecommunications networks.

Components

- **Lifecycle manager** The lifecycle manager deploys and manages HP Helion OpenStack Carrier Grade.
- **Non-KVM Region Controller**. Standard IaaS control plane to enable cloud-to-cloud communication.
- **StoreVirtual/3PAR**: Hardware storage array used as backend for Cinder. Support for 3PAR has a similar architecture as StoreVirtual on iSCSI, not Fibre.
- **KVM Region Controller**: Real-time control plane for compute and networking. Contains modified versions of most of the OpenStack components.
- **KVM Region Compute**: Realtime compute node with networking components.
- **Orchestrator**: This could be any application consuming the cloud services.

Data

Data name	Confidentiality	Integrity	Availability	Backup?	Description
Cloud Definition	Confidential	High	Low	Yes	Control plane and network topology and mapping to data center (input to HLM)
Cloud Configuration	Confidential	High	Low	Yes	Configuration of services in cloud (output from HLM)
MySQL database	Confidential	High	High	Yes	Contains user preferences.

Data name	Confidentiality	Integrity	Availability	Backup?	Description
					Backup to Swift daily.
Logs	Confidential	High	Medium	Yes	Logs from all services
Credentials	Confidential	High	High	Yes	Inter-service authentication uses the credentials for each service

Ethernet Interfaces

All hosts in the server connect to at least the internal management network using an Ethernet interface. The ports used for this connection must support network booting and must be configured to be used as the primary booting device for normal operations.

Typically this means that they must be on-board ports, since in most BIOS/UEFI implementations only on-board ports can be configured for network booting. You can use ports on a 10 GB NIC instead, if these ports fulfill these requirements.

The following table illustrates the number and type of Ethernet ports required in two different installation scenarios.

NOTE: The following table assumes that each interface is connected to a single network. An Ethernet interface can be shared by more than one network.

Personality	Basic Scenario	LAG Scenario
Controller Node	• One 10G on-board interface (Internal management network)	• Two 10G on-board interfaces (Internal management network)
Compute Node	• One 10G on-board interface (Internal management network) • Two 10G (Intel 82599) interfaces per Provider Network	• Two 10G on-board interfaces (Internal management network) • Two 10G (Intel 82599) interfaces per Provider Network

In the basic scenario, a single Ethernet port is used to attach the host to each of the networks. In the LAG scenario, two Ethernet ports are used for each connection.

Board Management Modules

For out-of-band reset and power-on/power-off capabilities, DL360 or DL380 servers equipped with HPE iLO (Integrated Lights Out) board management modules are required. Each module must be connected using port-based VLAN to a switch that has access to the internal management network.

USB Interface

For the controller, a USB interface is required for backup and restore operations, and for software installation if a DVD is not available.

Network Requirements

The networking environment incorporates several types of network:

- the internal management network
- the OAM network
- one or more provider networks

- an optional infrastructure network
- an optional board management network.

Operational requirements for each network are described in the following sections.

Internal Management Network

The internal management network must be implemented as a single, dedicated, Layer 2 broadcast domain for the exclusive use of each server cluster. Sharing of this network by more than one server cluster is not a supported configuration.

During the server software installation process, several network services such as DHCP, and PXE, are expected to run over the internal management network. These services are used to bring up the different hosts to an operational state. Therefore, it is mandatory that this network be operational and available in advance, to ensure a successful installation.

On each host, the internal management network can be implemented using a 10 Gb Ethernet port. In either case, requirements for this port are:

- must be capable of PXE-booting
- can be used by the motherboard as a primary boot device

CAN/OAM Network

You should ensure that the following services are available on the CAN/OAM Network:

- DNS Service - Needed to facilitate the name resolution of servers reachable on the CAN/OAM Network.

  The server can operate without a configured DNS service. However, a DNS service should be in place to ensure that links to external references in the current and future versions of the web administration interface work as expected.
- NTP Service - The Network Time Protocol (NTP) can be optionally used by the server controller nodes to synchronize their local clocks with a reliable external time reference. However, it is strongly suggested that this service be available, among other things, to ensure that system-wide log reports present a unified view of the day-to-day operations.

The server compute nodes always use the controller nodes as the time server for the entire cluster.

Provider Network

There are no specific requirements for network services to be available on the provider network. However, you must ensure that all network services required by the guests running in the compute nodes are available. For configuration purposes, the compute nodes themselves are entirely served by the services provided by the controller nodes over the internal management network.

Infrastructure Network

This is an optional network.

As with the internal management network, the infrastructure network must be implemented as a single, dedicated, Layer 2 broadcast domain for the exclusive use of each server cluster.

Sharing of this network by more than one server cluster is not a supported configuration.

The infrastructure network can be implemented as a 10 Gb Ethernet network. In its absence, all infrastructure traffic is carried over the internal management network.

Board Management Network

Board Management CTL (IPMI Control) Network External access to the board management network, the board management modules are assigned IP addresses accessible from the OAM network, and the controller uses the OAM network to connect to them.

Next Step

Review the *Support Matrix*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Denver Deployment Support Matrix

To ensure the performance and stability of the HP Helion OpenStack Carrier Grade, it is very important to meet the requirements and conform to the recommendations listed in this document.

- *Supported Hardware*
- *Required Specifications*
- *Hardware Configurations*
- *Software Requirements*
- *External Storage*
- *Supported Guest Operating Systems*

Supported Hardware

The following servers are supported for the lifecycle manager host, and for the controllers and compute servers.

Lifecycle Manager Host The lifecycle manager host is a single server with at least a 500 GB disk size, 4GB of virtual memory and 2 virtual CPUs.

Controllers and compute servers The following servers are supported for the controllers and compute servers in the *KVM region*. The servers must meet the specifications in *the Required Specifications table below*:

Controller:

- DL360 (Gen 9 or Gen 8)
- DL380 (Gen 9 or Gen 8)

Compute:

- DL360 (Gen 9 or Gen 8)
- DL380 (Gen 9 or Gen 8)
- BL460 (Gen 9 or Gen 8)

Notes:

- If you are using Gen9 systems, you must update the firmware to HPE Service Pack for ProLiant (SPP) Version 2015.06.0.
- If you are using Gen8 systems, you will experience reduced performance.

Required Specifications

The following table lists the specifications for the servers that will host the lifecycle manager, HP Helion OpenStack, and the KVM region.

Server	Used for	Requirements
HPE ProLiant Rack Servers		
DL360 Gen9 DL380 Gen9	• Controller	• 2 x Intel Xeon® E5-2640v3 • 8 x 16GB (1x16GB) Dual Rank x4 DDR4-2133 memory • 4 x 1.2TB 6G SAS 10K rpm SFF (2.5-inch) • 1 x FlexFabric 10Gb 2-port 556FLR-SFP • 1 x Smart Array P440ar/2G FIO Controller
	• Compute	• 2 x Intel Xeon® E5-2680v3 • 16 x 16GB (1x16GB) Dual Rank x4 DDR4-2133 memory • 4 x 1.2TB 6G SAS 10K rpm SFF (2.5-inch)

Server	Used for	Requirements
		• 1 x FlexFabric 10Gb 2-port 556FLR-SFP **AND** HPE Ethernet 10Gb 2-port 560SFP+ Adapter • 1 x Smart Array P440ar/2G FIO Controller/2 x Ethernet 10Gb 2P 560SFP
DL360 Gen8 DL380 Gen8	• Controller	• 2 x Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.6GHz • 128 GB DDR3 1600 MHz • HPE FlexFabric 10Gb 2port 554FLR-SFP+ Adapter **OR** HPE FlexFabric 10Gb 2port 534FLR-SFP+ Adapter
	• Compute	• 2 x Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.8GHz • 256 GB DDR3 1600 MHz • HPE FlexFabric 10Gb 2port 554FLR-SFP+ Adapter **AND** HPE Ethernet 10Gb 2-port 560SFP+ Adapter
HPE ProLiant BladeSystem		
BL460c Gen9	• Compute	• 2 x Intel® Xeon® E5-2680v3 • 16 x 16GB (1x16GB) Dual Rank x4 DDR4-2133 memory • 2 x 1.2TB 6G SAS 10K rpm SFF (2.5-inch) • 1 x Smart Array P244br/1GB FBWC • 1 x HPE FlexFabric 20Gb 2-port 650FLB **AND** 1 x HPE Ethernet 10Gb 2-port 560M Adapter
BL460c Gen8	• Compute	• 2 x Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.8GHz • 256 GB DDR3 1600 MHz • 2 x 1.2TB 6G SAS 10K rpm SFF (2.5-inch) • 1 x HPE FlexFabric 10Gb 2port 554FLB-SFP+ Adapter **AND** 1 x HPE Ethernet 10Gb 2-port 560M Adapter
Switch		
HP FlexFabric 5930 Switch Series		

Required Hardware Configurations

The servers, selected from the *Supported Hardware* lists, must be configured as follows for HP Helion OpenStack Carrier Grade.

One (1) **Lifecycle Manager Host**. You must have a server with a 40GB Disk and 8,192 MB RAM for the lifecycle manager host. This server will also host three (3) virtual machines that serve as controllers for HP Helion OpenStack Carrier Grade. Each of the controller nodes requires 20GB of virtual disk, 16GB of virtual memory, and 4 virtual CPUs.

Two (2) **KVM region controllers**. You must have two (2) baremetal systems to install the KVM region controllers. For systems with multiple NICs, only one NIC may be active or connected.

One (1) or more **KVM Region compute servers**. You must have at least one (1) baremetal system to install the KVM region compute servers.

- **KVM region NICs.** The following NICs have been verified for PXE booting of KVM region servers:
  - Emulex 10G
  - Intel 82599

  Important: Using the correct NICs is essential to proper installation of HP Helion OpenStack Carrier Grade.

Software Requirements

Lifecycle Manager Host. The lifecycle manager host requires the Ubuntu Server 14.04.2 LTS operating system.

Non-KVM Region Controllers. The servers should be baremetal. The HP Helion OpenStack Carrier Grade installation process installs the required software.

KVM Region Controllers. The servers should be baremetal. The HP Helion OpenStack Carrier Grade installation process installs the required software.

KVM Region Compute. The servers should be baremetal. The HP Helion OpenStack Carrier Grade installation process installs the required software.

External Storage

The following back-end drivers are supported to enable management of the OpenStack Block Storage volumes in the non-KVM region.

- HPE 3PAR StoreServ, version 3.1.3 or 3.2.1 MU2 or higher .
- HPE StoreVirtual VSA with LeftHand OS 11.5.

You will configure the installer to integrate one or both of these drivers during the installation process.

Supported Guest Operating Systems

The following guest operating systems (guest OSs) are supported for the HP Helion OpenStack Carrier Grade servers.

Lifecycle Manager Host. There are no supported guest OSs for the Lifecycle Manager Host server.

KVM Region Compute and Controllers. The following Guest OSs are supported for the servers in the KVM region for both cloud topologies:

- WindRiver Linux 6.0
- WindRiver Linux 5.0
- CentOS 6.4
- Fedora 19
- RHEL 6.5
- OpenSUSE 12.3

Next step

Review the *Installation Prerequisites*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 1 - Preparing the Installation Environment for the Denver Deployment

This document describes the prerequisite steps required to install HP Helion OpenStack Carrier Grade in a baremetal environment.

Hardware and software requirements

Before you start, if you have not done so already, make sure your environment meets the hardware and software requirements. See the *HP Helion OpenStack Support Matrix*.

Preparing the lifecycle manager host

Perform the following tasks on the lifecycle manager host:

- *Configure proxy information* on page 37
- *Install Ubuntu packages* on page 37
- *Configure the XRDP remote desktop display* on page 38
- *Install and configure NTP* on page 39

- *Configure SSH* on page 39
- *Preparing the Network for Installation* on page 40
- *Integrating LDAP* on page 40
- *Bring Up Single VSD VM Manually*
- *Prepare the servers* on page 40

Install Ubuntu Server 14.04.2 LTS

The lifecycle manager host must have Ubuntu Server 14.04.2 LTS installed before performing the HP Helion OpenStack Carrier Grade installation.

Configure proxy information

Before you begin your installation on the lifecycle manager host, configure the proxy information for your environment using the following steps:

1. Launch a terminal and log in to your lifecycle manager host as root:

```
sudo su -
```

2. Edit the `/etc/environment` file to add the following lines, using values specific to your environment.

   Note: The `export no-proxy` command is optional:

```
vsc_config_restore.yml ATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin:/sbin:/bin:/usr/games:/usr/local/games"
export http_proxy=http://<web_proxy_IP>/
export https_proxy=http://<web_proxy_IP>/
export no_proxy=localhost,127.0.0.1,<IP_address>,<provider_network>
```

   Where:

```
<web_proxy_IP> is your web proxy IP address.
<IP_address> is the IP address of the lifecycle manager host
```

3. Source the `environment` file:

```
source /etc/environment
```

Install Ubuntu packages

Before starting the installation, you must install the following packages on the lifecycle manager host.

- ntp
- firefox
- gedit
- xrdp
- xfce4
- qemu-kvm
- libvirt-bin
- python-libvirt
- qemu-system-x86
- libssl-dev
- libffi-dev
- git
- python-virtualenv
- python-dev

- virt-manager
- xorg
- gnome-core
- gnome-system-tools
- gnome-app-install
- sshpass
- gnupg
- jq
- vlan
- sudo
- ansible

To install the packages on the lifecycle manager host:

1. On the KLM host, run the following command to install all required packages:

```
sudo su -l -c "apt-get install -y ntp firefox gedit xrdp xfce4 qemu-kvm
 libvirt-bin python-libvirt qemu-system-x86 libssl-dev libffi-dev git
 python-virtualenv python-dev virt-manager xorg gnome-core gnome-system-
tools gnome-app-install sshpass gnupg jq vlan sudo ansible"
```

2. Add the 802.1q module to the kernel on boot. The 802.1q standard supports VLAN tagging on an ethernet network.

```
sudo su -c 'echo "8021q" >> /etc/modules'
```

3. Reboot the server
4. Log out and re-login to the lifecycle manager host to activate the proxy configuration.

Configure the XRDP remote desktop display

Configure XRDP on the lifecycle manager host for the remote desktop connection to access the server remotely as follows.

1. Edit the `sesman.ini` file:
   a. Open the file:

   ```
   vi /etc/xrdp/sesman.ini
   ```

   b. Update the`MaxSessions=1` to `MaxSessions=50`.
   c. Save and close the file.
2. Execute the following command to configure the system to use XRDP:

```
echo "xfce4-session" > ~/.xinitrc
```

3. Execute the following command to restart the XDRP service:

```
sudo /etc/init.d/xrdp restart
```

If the XDRP display does not work as expected, (you see a gray screen):

1. Update the `startwm.sh` file:

```
vi /etc/xrdp/startwm.sh

#!/bin/sh

if [ -r /etc/default/locale ]; then
. /etc/default/locale
```

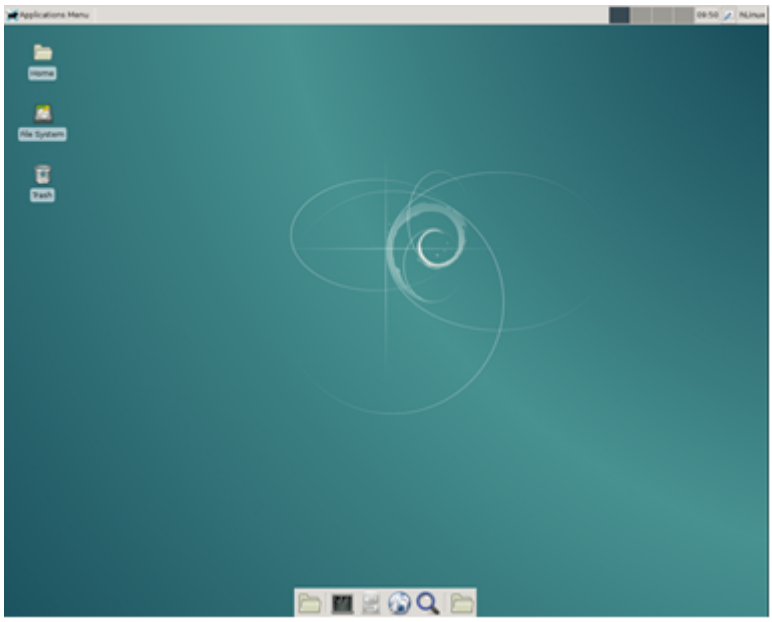
```
export LANG LANGUAGE
fi

#. /etc/X11/Xsession
. /usr/bin/startxfce4
```

Note: Make sure you add a space between `.` and `/`.

2. Restart XDRP:

```
sudo /etc/init.d/xrdp restart
```

When you XRDP to the lifecycle manager host, the screen appears similar to the following image:



Install and configure NTP

You must configure the lifecycle manager host as an NTP client.

You can install NTP on the lifecycle manager host and configure it as an NTP server. Or, you can use a pre-existing NTP server that is reachable from the management network.

For information on configuring the lifecycle manager host as an NTP client, see *Configure all other servers as NTP clients*.

For information on installing NTP on the lifecycle manager host, see *Installing an NTP Server*.

Configure SSH

On the lifecycle manager host, the OpenSSH server must be running and the firewall configuration should allow access to the SSH ports.

1. Enable root login in the `/etc/ssh/sshd_config`:

   a. Set the following values:

```
# Authentication:
LoginGraceTime 120
#PermitRootLogin without-password
PermitRootLogin yes
#StrictModes yes
```

```
StrictModes no
PermitRootLogin yes
```

2. Disable strict host key checking:
   a. In the `~/.ssh/config` file (create the file if it does not exist) add following lines

   ```
   Host *
   StrictHostKeyChecking no
   ```

   b. Save the file,
3. Restart the SSH service:

   ```
   service ssh restart
   ```

4. Configure the public key and passwordless SSH access.

   a. Enter the following command:

   ```
   ssh-keygen -t rsa
   ```

   b. Press Enter to use default path (`/root/.ssh/id_rsa`)

   c. Press Enter when prompted for the `passphrase`.

   d. Press Enter to confirm the empty `passphrase`.

   The output of the public key will display, similar to the following:

   ```
   ssh-copy-id 192.168.122.1
   ```

   If you get a *permission denied* error, make sure you are logged in as root.

Preparing the Network for Installation

Before installing HP Helion OpenStack Carrier Grade, you are responsible for preparing the network for all installations.

See *Preparing the Network for Installation*

Integrating LDAP

OPTIONAL: The HP Helion OpenStack Identity service can use Lightweight Directory Access Protocol (LDAP) to integrate your organization's existing directory service and user account management processes.

See *Enabling LDAP*

Prepare the servers

Perform the following tasks on each server you will use as a compute server or controller in the non-KVM and KVM regions:

- Configure the boot order with Network/PXE boot as the first option:

  For example, to set the boot order for a HPE SL390, from the iLO prompt enter `set system1/bootconfig1/bootsource5 bootorder=1`.
- Configure the BIOS:
  - to the correct date and time
  - to use UTC (Coordinated Universal Time)
  - with only one network interface enabled for PXE/network boot and any additional interfaces should have PXE/network boot disabled
  - to stay powered off in the event of being shutdown rather than automatically restarting

- Update to the latest firmware recommended by the system vendor for all system components, including the BIOS, BMC firmware, disk controller firmware, drive firmware, network adapter firmware, and so forth.

  Note: If you are using ProLiant Gen9 blades or rack servers, you must update the Snap3 firmware.

Next Step

Download the Installation Packages

HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 2 - Download the Denver Installation Packages

This document describes the prerequisite steps to download the installation files required to install HP Helion OpenStack Carrier Grade.

Download the HP Helion OpenStack Carrier Grade installation files

Download the installation files as indicated in the following tables. Also download the associated MD5 file for verification.

File Name	Copy to location on the Lifecycle Manager	Notes
cg-hlm.qcow2	/var/lib/libvirt/images Can copy this to any other directory and update the group_vars/all file with that dir folder path	
cg-hos-misc.tar.gz	/root/cg	
cg-hos-src.tar.gz	**Create cg folder if not present**	
cg-infra-src.tar.gz	/root	
cg-ironic-deploy-images.tar.gz	/root/cg	For Sacramento deployments only.

KVM Region Installation files

Download the following files for installing the KVM region. Also download the associated MD5 file for verification.

File Name	To be copied to the KVM Host
`bootimage_avs_only.iso`	`/root` on `controller-0` in the KVM region.
`HCG2.0GA-guest-SDK.tar.gz`	`/root` on `controller-0` in the KVM region. SDK files to be used as needed.
`WR-15.09-sample-guest.img`	`/root` on `controller-0` in the KVM region. Sample guest operating system files to be used as needed.
`TS_HP_15_Custom_PATCH_0002.patch`	Patch instructions are provided in *Deploying the KVM Region*

Verify the downloaded checksums

You should also use a checksum verification tool, such as sha256sum, which should come installed with Ubuntu.

1. Run the checksum tool against the download package:

```
sha256sum <path-to-file>/hcg2_kvm_esx_ironic_vrs.tar
```

or

```
sha256sum <path-to-file>/hcg2_kvm_esx_ironic_vrs.tar
sha256sum <path-to-file>/hcg2_kvm_esx_ironic_part2of2.vrs.tar
```

2. Compare the output of the checksum tool to the download checksum file.

```
sha256sum.exe hcg2_kvm_esx_ironic_vrs.tar
97f5b83c7aa0410ecc90f870f22bf8a691f8491a69c2ec26e0e71a24
 hcg2_kvm_esx_ironic_vrs.tar
```

Note that the checksum file contains the date that the file was generated, the checksum string, and the name of the file that was used, similar to the following:

```
Fri Jul 31 10:55:37 EDT 2015
97f5b83c7aa0410ecc90f870f22bf8a691f8491a69c2ec26e0e71a24
 hcg2_kvm_esx_ironic_vrs.tar
```

Next Step

Deploying the Lifecycle Manager

HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 3 -Deploying the Lifecycle Manager in a Denver Deployment

The first phase of the HP Helion OpenStack Carrier Grade installation involves creating a bootstrapping the lifecycle manager VM and installation services.

The installation uses Ansible playbooks, which are files that contain scripts that execute required installation processes.

Prepare the system for deployment

Use the following steps to prepare the server on which the lifecycle manager will be deployed (the lifecycle manager host):

1. Log into the lifecycle manager host using the default credentials
2. Edit the `/root/infra-ansible-playbooks/group_vars/all` file for your environment. For information on each variable, refer to the comments in the file with each variable.
   - Set the `ovs_cloud_only` variable to `2`
   - Set the `cloud_type` variable to `'av'`
   - Set the CLM IP network details for to your network setup
   - Set the Cobbler IP addresses according to your network setup

   The `group_vars/all` file should appear similar to the following:

```
---

############################################## Variables for HLM
 ##################################################################
#These variables are relevant in both All Virtual and BareMetal scenarios.

#Set this to '0' for dcn cloud, '1' for ovs cloud, '2' for denver or
 denver_virtual cloud.
ovs_cloud_only:  2
```

```
#Set this to 'bm' if cloud is being deployed over baremetal.
#Set this to 'av' if the cloud is all virtual
cloud_type: 'av'

#These are hlm related variables that must be changed according to your
 Baremetal Env
hlm_login_id:       root
hlm_password:       cghelion

#The following variables are for CLM network IP details for HLM
hlm_clmstaticip:    10.10.2.100
hlm_clmnetmask:     255.255.255.0
hlm_clmgateway:     10.10.2.1

#The variables starting with cobbler_ are inputs that are usually given to
 initcobbler.sh. Set accordingly.
cobbler_pxestartip: 10.10.1.100
cobbler_pxeendip:   10.10.1.200
cobbler_pxestaticip: 10.10.1.7
cobbler_pxenetmask: 255.255.255.0
cobbler_hlinux_password: ohcanada
cobbler_web_password: cobbler

#Set the location of your images that will be used by libvirt
imagelocation: /var/lib/libvirt/images

#Set the location of your infra-ansible-playbooks
ansible_dir: ~/infra-ansible-playbooks

##################################################################################

############################################## Variables for DCN
 ################################################################
#Set the location of dcn bits on KVM
#There must be 4 debs, 2 tar.gz files, 1 vsc qcow2
#You must copy your VSD qcow2 to the imagelocation on the KVM if you want
 to provision it on the same KVM as the HLM
dcn_dir: ~/cg/dcn
##################################################################################

############################################## Variables for VSD
 ################################################################
#Ignore these variables if creating an OVS cloud. This section is relevant
 only for DCN cloud - in both BM and All Virtual cases
#These variables are used for VSD Configuration
#If you have already configured a VSD and ignore the following variables

dns_domain_name: helion.cg
dns_address: 10.10.10.25
vsd_address: 10.10.10.10
vsd_gateway: 10.10.10.1
vsd_netmask: 255.255.255.0
vsd_name: vsd
vsdimagename: VSD-3.0.0_HP_r3.0_36
upstream_ntp_servers:
   - 10.10.10.25
   - 10.1.64.20
##################################################################################
```

3. Edit the `group_vars/all-virtual` file:
   - Update the `kvm_user` and `kvm_password` variables with your KVM Credentials.
   - Change the `Cloud_Topology` variable to `denver_virtual`

4. Edit the `group_vars/all-kvm-net` file to make sure the VLAN tag IDs are correct according to your network configuration.
5. Change to `infra-ansible-playbooks` directory

```
~/ cd infra-ansible-playbooks
```

6. Execute the following command to create required Ansible roles: `DCN-RCP-INFRA`, `DCN-RCP-CLOUD`, `HLM-RCP-CFG`. These roles create the lifecycle manager, the HP Helion OpenStack Carrier Grade controllers and configure the lifecycle manager.

```
ansible-playbook -i hosts setup_rcpcloud.yml
```

7. Check the `/root/infra-ansible-playbooks/hosts` file to enter the IP address of the `vibr0` interface in the `hlm_kvm_host` field, as shown in the following example.

```
[hlm_kvm_host]
192.168.122.1
```

Deploy the Lifecycle Manager Virtual Machine

Use the following steps on the lifecycle manager host to deploy the lifecycle manager on that host using Ansible playbooks.

1. Execute the following command:

```
ansible-playbook -i hosts setup_hlm_onBM.yml
```

```
TASK: [HLM-CFG | Create a directory to hold the nuage packages] ***************
changed: [192.168.122.16]

TASK: [HLM-CFG | Copy the dcn files to the hlm node from the kvm host] ********
changed: [192.168.122.16] => (item=/root/cg/dcn/nuage-openstack-neutron-juno-plugin.tar.gz)
changed: [192.168.122.16] => (item=/root/cg/dcn/nuage-python-openvswitch_3.0.7-125_all.deb)
changed: [192.168.122.16] => (item=/root/cg/dcn/nuage-openvswitch-common_3.0.7-125_amd64.deb)
changed: [192.168.122.16] => (item=/root/cg/dcn/nuage-openvswitch-switch_3.0.7-125_amd64.deb)
changed: [192.168.122.16] => (item=/root/cg/dcn/nuage-openstack-nuagenetlib-juno.tar.gz)
changed: [192.168.122.16] => (item=/root/cg/dcn/vsc_singledisk.qcow2)
changed: [192.168.122.16] => (item=/root/cg/dcn/nuage-metadata-agent_3.0.7-125_all.deb)

TASK: [HLM-CFG | Copy the debs in debian repo in HLM] *************************
changed: [192.168.122.16]

TASK: [HLM-CFG | Run dpkg scan to ensure the debian repo is updated with new DCN packages] ***
changed: [192.168.122.16]

PLAY RECAP ********************************************************************
192.168.122.1              : ok=17   changed=8    unreachable=0    failed=0
192.168.122.16             : ok=40   changed=27   unreachable=0    failed=0
```

2. Locate the IP address for the lifecycle manager in the `/root/infra-ansible-playbooks/group_vars/all` file of the lifecycle manager host under `hlm_clmstaticip` field. You will use this IP address to SSH into the lifecycle manager VM during the HP Helion OpenStack Carrier Grade installation process.

Next Step

Install Required Patches

HP Helion OpenStack® Carrier Grade 2.1 Beta: Using the HCG Dashboard

Introduction

HCG-Dashboard is a cloud management tool which allows users to Define, Deploy, Manage and Monitor cloud.

This tool facilitates users to provide and validate cloud definitions required define a cloud through web interface.

Once the cloud is defined user will be able guided through various stages of deployment

After the cloud is deployed, user will be able to perform various post deployment activities as Service resets, patching and upgrade.

Currently, HCG-Dashboard supports "RCP" cloud only**.**

For beta- the UI is hosted on Django's internal web server. In the coming weeks, the UI will be hosted on Apache2.

How to access the dashboard?

1. UI will be setup as part of hlm_prepareenv.sh script so it will be available as soon as you execute that script
2. The dashboard service runs on port 8080 and can be accessed using http://<hlm ip>:8080/
3. If you are accessing UI from an outside machine (like a jump server), you should be using hlm ip (in above URL) that is accessible from that machine

Features Available Today

The UI supports Reduced Control Plane creation and configuration. The UI supports Cloud Definition for RCP template only.

Use the "Cloud Input" wizard on the UI to:

1. Specify Cloud Name
2. Specify KVM Servers info and Map the KVM servers to the Controllers
3. In the KVM servers get validated for connectivity and credentials correctness.
4. Specify Network information for all 5 types of networks (CLM, API, BLS) (If you do not have Segment IDs, Enter -1)
5. View validation results of network information provided (Validation for API and BLS networks not part of 2.1 Beta but will be added for 2.1 GA)
6. Specify all variables
7. View validation results of DNS Server IP and NTP Server IP (There is a known cosmetic bug for the results of this validation, will be fixed in upcoming builds)
8. Click Finish to save all this data into your clouds json files.
9. By default, RCP template is used to create the cloud definitions.

Use the "Deploy Cloud" wizard on the UI to (More details below):

1. Provision the Nodes (equivalent to hlm provision)
2. Generate the cloud configuration from jsons (equivalent to hlm generate)
3. Network Initialize the cloud nodes (equivalent to hlm netinit)
4. Deploy the cloud nodes (equivalent to hlm deploy)

Use the "Manage Cloud" wizard on the UI to:

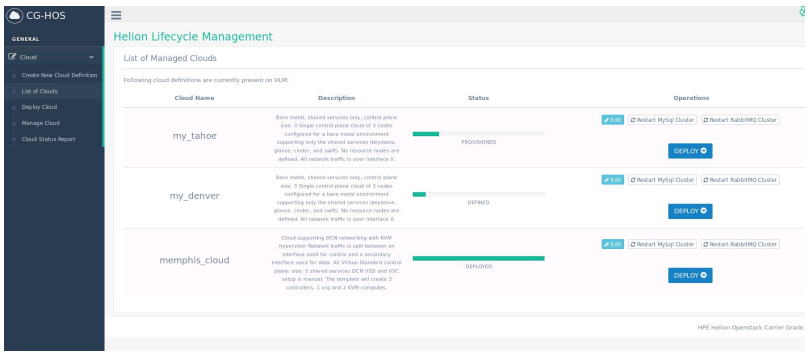
1. Reset service including - MySQL, RabbitMQ, NTP, Apache, Keystone, Glance, Swift, Cinder, Elastic Search, Logstash, Kibana, Beaver, Icinga and Attis

Important to Note

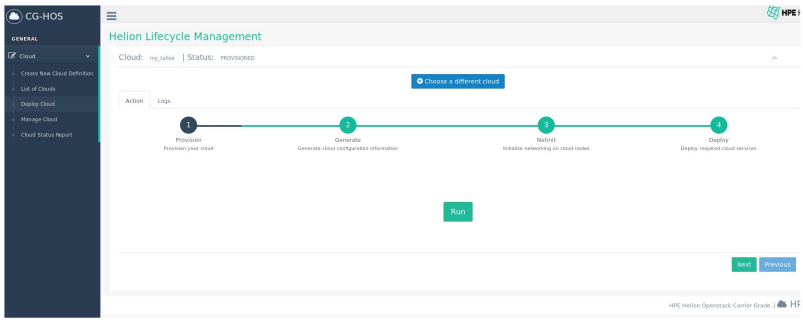
Editing an existing cloud definition is supported except for the Inventory Nodes (KVM Servers)

Deploy Cloud workflow

- After you enter all necessary inputs to your cloud, you will be redirected to a page where you can see description and current status of your cloud along with a few other options:



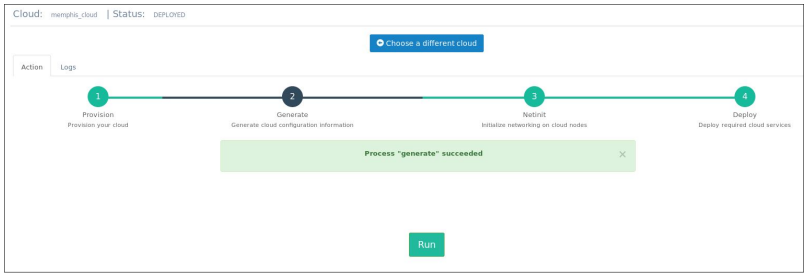
- You can click on "DEPLOY" button (as seen in above page) to start/return to a deploy workflow:



- "Deploy Workflow" consists of four phases - provision, generate, netinit and deploy
- At the top you will see the name of your cloud and current status - "DEFINED" | "PROVISIONED" | "GENERATED" | "NETINITIALIZED" | "DEPLOYED"
- Depending on the status, marker on the wizard will move by default to a process which was completed successfully
- To execute a particular process, you can navigate (or directly click) on corresponding step and click "Run"

  (Note: you will not be able to navigate to step "n" if step "n-1" is not completed)
- Once you hit the "Run" button, you will see your process being executed as shown below:
- The process runs asynchronously in background. So while the process is running, if you close your session or browser, you can still return to the same page again to check status of your process.
- Also, when your process is running, you can look at the current log content by clicking on the "logs" tab and selecting a log file pertaining to that process as seen below:

- Once the process completes, you will be notified whether it passed or failed as seen below:



Next Step

Launching the Horizon Interface

HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 4 - Deploying the Denver Template

After the lifecycle manager is installed, the next task in installing the Denver topology is to deploy the HP Helion OpenStack cloud.

If you are installing the `denver` template, which includes the KVM region and uses AVS networking, follow these instructions. If you are installing a different deployment, disregard these instructions.

Launch the HPE Helion OpenStack cloud

Use the following steps on the lifecycle manager host to log on to the lifecycle manager:

1. Log into the lifecycle manager.

   ```
   ssh <CLM_IP>
   ```

   where: HLM_VM_IP is the CLM IP of the lifecycle manager. Locate the IP address for the lifecycle manager in the `/root/infra-ansible-playbooks/group_vars/all` file under `hlm_clmstaticip` field.

   Use the default credentials:

   ```
   User Name: root
   Password: cghelion
   ```

   Important: After logging in with the default password, make sure you change the password for the `root` user.
2. Execute the following command to switch to the root user:

   ```
   sudo su -
   ```
3. Change to the home directory.

   ```
   cd ~
   ```

Provision the new cloud

1. Execute the following command to provision and configure the HPE Helion OpenStack cloud.

   ```
   hlm define -c <cloud-name> -t rcp
   ```

   Where:: `<cloudname>` is the name of the cloud to create.

   The cloud name can be any combination of up to 40 digits, letters:

   - Cannot contain with the – character;
   - Must be greater than 0 characters;

- No restriction on the number of letters or digits (0 or more).

The command creates the `/var/hlm/clouds/<cloudname>` directory, which contains several JSON template files.

Configuring JSON files

The HP Helion OpenStack deployment requires several JSON files.

Important: Do not store backup of the JSON files inside your cloud directory or any where inside the `/var/hlm/clouds` directory. You can create a backup folder on `/root/` directory or on a remote system.

Edit the node-provision.json file

Modify the `node-provision.json` file in the `/var/hlm/clouds/<cloudname>` directory of the lifecycle manager. This file supplies input values to the hprovision script, later in the installation.

Edit the `node-provision.json` file to change only the following fields:

Field	Description
Pxe-mac-address	MAC address of the interface you want to PXE boot onto. This is not same as iLO MAC address.
pm_ip	Power management IP (iLO ip)
pm_user	Power management user (iLO username)
pm_pass	Power management password (iLO password)
failure_zone, vendor, model, os_partition_size, data_partition_size	Enter the same value as for these fields an in the `nodes.json` file used during cloud deployment

Click here to see a *sample node-provision.json file*.

Configure PXE boot

After you edit the `node-provision.json` file, you must enable one-time PXE boot on the servers to set the correct boot order. Execute the following on the lifecycle manager:

1. Copy the `ilopxebootonce.py` from the `/root/cg-hlm/dev-tools/ilopxebootonce.py` to the `<cloudname>` directory where you have the `node-provision.json` file.
2. Execute the following script:

```
python ilopxebootonce.py node-provision.json
```

After the script is run, the `Current One-Time Boot Option` is set to `Network Device 1` on all the servers listed in `node-provision.json` file.

Edit the environment.json file

Modify the `environment.json` file in the `/var/hlm/clouds/<cloudname>` directory of the lifecycle manager. Configure the VLANs and network addresses as appropriate for your environment. Set the following for the CLM, CAN, and BLS network:

```
"cidr":
          "start-address":
```

The three controller nodes should have CLM, CAN, EXT, BLS on eth0 and TUL on eth1.

Example:

In the following example, the IP addresses have been masked for security:


```
{
    "product": {
        "version": 1
    },

    "node-type": [
        {
            "name": "CCN",
            "interface-map": [
                {
                    "name": "INTF0",
                    "ethernet-port-map": {
                        "interface-ports": [ "eth1" ]
                    },
                    "logical-network-map": [
                        {
                            "name": "CLM",
                            "type": "vlan",
                            "segment-id": "",
                            "network-address": {
                                "cidr": "10.207.x.x/24",
                                "start-address": "10.207.x.x",
                                "gateway": "10.207.x.x"
                            }
                        }
                    ]
    },
    {
                    "name": "INTF1",
                    "ethernet-port-map": {
                        "interface-ports": [ "eth2" ]
                    },
                    "logical-network-map": [
                        {
                            "name": "CAN",
                            "type": "vlan",
                            "segment-id": "",
                            "network-address": {
                                "cidr": "10.207.x.x/24",
                                "start-address": "10.207.x.x",
                                "gateway": "10.207.x.x"
                            }
                        }
       ]
    },
    {
                    "name": "INTF2",
                    "ethernet-port-map": {
                        "interface-ports": [ "eth3" ]
                    },
                    "logical-network-map": [
                        {
                            "name": "BLS",
                            "type": "vlan",
                            "segment-id": "",
                            "network-address": {
                                "cidr": "10.207.x.x/24",
                                "start-address": "10.207.x.x",
                                "gateway": "10.207.x.x"
                            }
                        }
```

```
        ]
                }
            ]
        }
    ]
}
```

NOTE: The configuration processor assigns the first address of the CLM address range to itself for serving python and debian repositories. Make sure that you set the first IP address of the CLM range for the eth2 (CLM) address of the HLM host.

Edit the Inet-control.json file

Modify the `Inet-control.json` file in the `/var/hlm/clouds/<cloudname>` directory of the lifecycle manager.

Edit the ansible.json file

Modify the `ansible.json` file in the `/var/hlm/clouds/<cloudname>/vars` directory of the lifecycle manager. Make sure the the DNS and NTP server details in the `properties` section are correct for your environment.

In the following example, the IP addresses have been masked for security:

```
{
    "product": {
        "version": 1
    },

    "property-groups": [
        {
            "name": "ansible-vars",
            "properties": {
                "dns_domain_name": "helion.cg",
                "dns_address": "10.x.x.x",
                "ext_dns_ip": "10.x.x.x",
                "upstream_ntp_servers": [
                    "10.x.x.x",
                    "16.x.x.x",
                    "2.debian.pool.ntp.org"
                ],
                "ssl_cert_file": "ca.crt",
                "ssl_key_file": "cakey.pem",
                "ssl_passphrase": "cghelion"
            }
        }
    ]
}
```

Edit the wr.json file

Modify the `wr.json` file in the `/var/hlm/clouds/<cloudname>/vars/` directory of the lifecycle manager with values appropriate for your environment. Make sure the CLM, BLS and CAN IP addresses in the `network` section are correct for your environment.

In the following example, the IP addresses have been masked for security:

```
{
    "product": {
        "version": 1
    },
```

```
    "property-groups": [
        {
            "name": "wr-vars",
            "properties": {
                "database_storage": 50,
                "backup_storage": 300,
                "shared_instance_storage": 250,
                "region_name": "regionone",
                "logical_interface": [
                    {
                        "lag_interface": "N",
                        "lag_mode": 4,
                        "interface_mtu": 1500,
                        "interface_ports": [
                            "eth0"
                        ],
                        "network": [
                            {
                                "ip_start_address": "10.x.x.x",
                                "ip_end_address": "10.x.x.x",
                                "name": "CLM"
                            },
                            {
                                "ip_start_address": "172.x.x.x",
                                "ip_end_address": "172.x.x.x",
                                "name": "BLS"
                            },
                            {
                                "ip_start_address": "10.x.x.x",
                                "ip_end_address": "10.x.x.x",
                                "name": "CAN"
                            }
                        ]
                    }
                ],
                "pxeboot_cidr": "10.x.x.x/24",
             "license_file_name": "license.lic",
                "physnet_VLAN_range_mappings":
 ["physnet1:1000:1999","physnet2:2000:2020"],
                "pci_vendor_id": ["8086:10ca","8086:10ed"]
            }
        }
    ]
}
```

Verify the JSON files

After editing the JSON files, validate each JSON file to make sure there are no syntax errors using the tool of your preference. For example, using the Python json.tool:

```
python -m json.tool <filename>.json
```

Provision the cloud nodes and bring the cloud nodes up

1. On the lifecycle manager, use the following script to start the provisioning of the HPE Helion OpenStack cloud:

   ```
   hlm provision -c <cloudname>
   ```

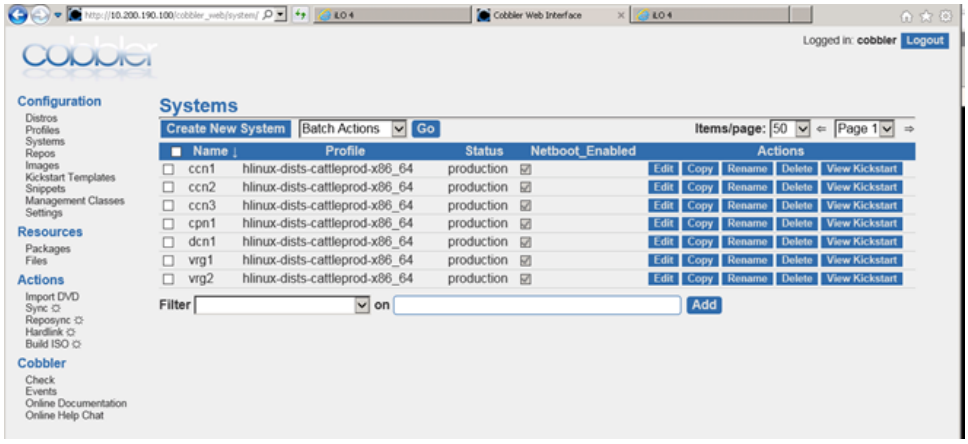
   Where: `<cloudname>` is the name of the cloud you created. The script takes approximately 15 to 30 minutes.

```
2015-07-28 03:08:23,511 : [INFO] : Tracking cobbler for pxe boot completion...

2015-07-28 03:12:07,236 : [INFO] : Status of  ccn1  changed to  stop

2015-07-28 03:12:09,401 : [INFO] : Status of  ccn2  changed to  stop

2015-07-28 03:12:31,929 : [INFO] : Status of  ccn3  changed to  stop

2015-07-28 03:12:31,939 : [INFO] : Writing nodes.json file on path  /var/hlm/clouds/infra/nodes.json
```

This script prepares the servers for the HPE Helion OpenStack Carrier Grade cloud installation including the hLinux operating system. The script also PXE boots the nodes specified in `node-provision.json` file and tracks the PXE boot completion process. The script also creates the `nodes.json` file in the directory.

You can log in to the iLO server management tool for each of the nodes to monitor the boot process. Consult your iLO documentation for information on how to log into iLO.

2. Make sure the nodes are booted up using iLO. For example:



Note: In rare situations, a node might not boot due to an issue with network configuration. If this happens, you need to log into that node and manually boot using the Retry Auto-Configuration option. The provisioning will continue as you reboot that node. See *Node fails to boot during HLM provision*.

Once the baremetal nodes are provisioned, make sure the `nodes.json` file is generated to the `var/hlm/clouds/<cloud name>/` directory. The `nodes.json` file will have entries for three controllers.

3. Verify that each node in the `nodes.json` file is installed and active.

   a. Ping proxy node from lifecycle manager with the IP using IP specified in `nodes.json` file.
   b. SSH to the compute proxy node from the lifecycle manager using IP specified in `nodes.json` file.

Configure the back-end drivers

Configure the back-end drivers to enable management of the OpenStack Block Storage volumes on HPE StoreVirtual VSA and/or HPE StoreServ (3PAR) storage arrays. The HPE Block Storage (Cinder) service allows you to configure multiple storage back-ends. A sample file provides all the variables needed to use VSA and/or 3PAR attached to the KVM region. You need to edit this file for your environment and save as `cinder_conf`.

Use the following steps to configure back-end support:

1. Change to the `/cinder/blocks` directory:

```
cd /var/hlm/clouds/<cloudname>/services/cinder/blocks
```

   Where `<cloudname>` is the name you assigned to the cloud. The directory contains several sample Cinder configuration files that you can edit, depending upon which storage method(s) you are using.

2. Edit the `cinder_conf.multiBackendSample` file.

   Use the `enabled_backends` variable to list each of the back-ends you are using.

Region/Hypervisor	Volume Backend	Backend Name
KVM	3PAR	hp3par
KVM	VSA	hplefthand

You can use either 3PAR and VSA in the KVM region or select both if you have respective storage arrays

Note: The HP 3PAR Web Services API server must be enabled and running on the HP 3PAR storage system. For more information, see the OpenStack documentation at: *Enable the HP 3PAR Fibre Channel and iSCSI drivers*.

A typical configuration file that enables both VSA and 3PAR back-ends appears similar to the following example:

```
[DEFAULT]
enabled_backends=hp3par, hplefthand
...

[hp3par]
volume_backend_name=<mybackendname1>
hp3par_api_url=https://<management_ip>:8080/api/v1
hp3par_username=<username>
hp3par_password=<password>
hp3par_cpg=<cpg>
san_ip=<san_ip>
san_login=<username>
san_password=<password>
hp3par_iscsi_ips=<iscsi_target_ips seperated by ,>
volume_driver=cinder.volume.drivers.san.hp.hp_3par_iscsi.HP3PARISCSIDriver
hp3par_debug=False
hp3par_iscsi_chap_enabled=false
hp3par_snapshot_retention=48
hp3par_snapshot_expiration=72

[hplefthand]
volume_backend_name=<mybackendname2>
hplefthand_username = <username>
hplefthand_password = <password>
hplefthand_clustername = <Cluster Name>
hplefthand_api_url = https://<Iscsi Virtual IP address>/lhos
volume_driver =
 cinder.volume.drivers.san.hp.hp_lefthand_iscsi.HPLeftHandISCSIDriver
hplefthand_debug = false
```

3. Save the file to `cinder_conf`.

Deploy the HPE Helion OpenStack cloud

1. Run the HPE Helion OpenStack Carrier Grade configuration processor:

```
hlm generate -c <cloudname>
```

This command runs the configuration processor, a script (`hcfgproc`) that is incorporated into the installation environment. This command generates the necessary configuration for the cloud.

When the command completes without errors, you will a message:

```
2015-07-28 03:32:36,189 : [INFO] :

2015-07-28 03:32:36,189 : [INFO] : ##############################################################################

2015-07-28 03:32:36,189 : [INFO] : # The configuration processor completed successfully.

2015-07-28 03:32:36,189 : [INFO] : ##############################################################################

2015-07-28 03:32:36,307 : [INFO] :
The cloud "infra" was generated successfully.
```

2. Review the CloudDiagram, `hosts.hf`, and `/etc/network/interfaces.d/eth.cfg` files to make sure the network settings are correct.
3. Initialize network interfaces on all the cloud nodes using the following command:

   ```
   hlm netinit -c <cloudname>
   ```

   Where: `<cloudname>` is the name of the cloud you created.

   After this command completes, all cloud nodes and CLM network interfaces are configured.

Deploy HPE Helion OpenStack

1. Use the following command to deploy the HPE Helion OpenStack cloud:

   ```
   hlm deploy -c <cloudname>
   ```

   This command takes a significant period of time. When this command completes without errors or warnings, the non-KVM cloud installation is complete. Use the following sections to configure the Horizon interface and configures virtual networking.

   ```
   }
   ##################################################

   The deployment was successful.


   Running Step: Validate...
   Running Step: Model Creation...
   Running Step: Controller Creation...
   Running Step: Checkpoint...

   Checkpoint created: 20150728_040654_201836__deployment
   ```

2. Enter `exit` to leave the root shell.

Configure LDAP to enable CLI and use Keystone v3

By default, the HPE Helion OpenStack Carrier Grade services are configured to use Keystone v2 authorization. The services need to be modified to use Keystone v3. Users will not be able to execute OpenStack CLI commands until the specific changes are made on all three controller nodes in the non-KVM region.

For information, see *Configuring LDAP CLI Support*

Next Step

Launching the Horizon Interface

HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 5 - Launching the Horizon Interface

After the HP Helion OpenStack cloud is installed, you can launch the Horizon interface to verify that the installation was successful.

Import the Horizon browser certificate

You need to import the Horizon security certificate (`ca.crt`) into your browser. The `ca.crt` is available in the lifecycle manager in the `~/<cloudname>` folder. You can use any file transfer program to move the certificate file from the lifecycle manager to the local system.

Use the instructions provided by the browser manufacturer to import the `ca.crt` file. For a list of browsers supported by OpenStack, see *https://wiki.openstack.org/wiki/Horizon/BrowserSupport*.

Also, clear the cache of the browser.

Login to Horizon

At this point, you can log into the Horizon interface, a web-interface you can use to manage and maintain HP Helion OpenStack Carrier Grade. Use the *CAN IP address* to launch Horizon. You can locate the CAN IP address in the `/root/stackrc` file on any of the controller nodes in the non-KVM region. The CAN IP address contains port `5000`.

For example:

```
export OS_PASSWORD=qekuTPcc26Ig
export OS_USERNAME=admin
export OS_TENANT_NAME=admin
export OS_AUTH_URL=https://10.20.4.120:5000/v2.0
export OS_CACERT=/etc/stunnel/ssl/hlm/certs/ca.crt
export OS_REGION_NAME=tahoe
unset OS_PROJECT_DOMAIN_NAME
unset OS_PROJECT_NAME
unset OS_USER_DOMAIN_ID
unset OS_IDENTITY_API_VERSION
unset OS_AUTH_VERSION
```

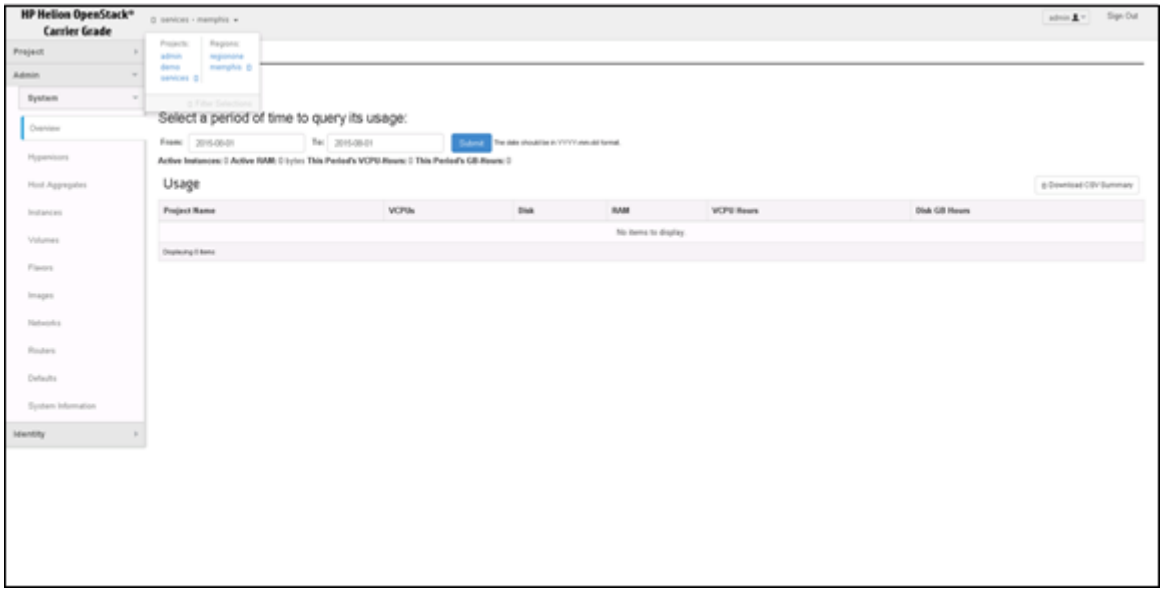
In this case, the CAN IP address is located in the `OS_AUTH_URL=https://10.x.x.x:5000/v2.0` line. You would log in using `https://10.x.x.x`.

Enter the IP in the browser to access the log-in page:

```
https://<CAN_IP>
```

By default, the user name is `admin`. You can find the installation password for `admin` in the `/root/stackrc` file from any of the controller nodes.

The Horizon interface appears similar to the following:



Next Step

Deploying the KVM Region.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 6 - Deploying the KVM Region in a Denver Deployment

After the lifecycle manager is up and running and HP Helion OpenStack is installed, use the following steps to deploy the KVM region.

The process for installing the KVM region involves the following tasks:

- *Step 1: Bring Up Controller-0 in the KVM Region*
- *Step 2: Deploy the KVM Region Custom Patch*
- *Step 3: Configure the KVM region cloud*
- *Step 4: Configure and unlock the compute controllers*
- *Step 5: Deploy the Horizon Patch*

Step 1: Bring Up Controller-0 in the KVM Region

1. Make sure the server you will use for controller-0 is powered on and the other servers to be used in KVM region are shutdown.
2. Launch the iLO interface for the server.
3. Execute the following command to use the `bootimage_avs_only.iso` to boot the controller node.

```
mount bootimage_avs_only.iso
```

4. Follow the install wizard. Select the Graphics mode for the controller only. Do not select `Controller +Compute`.

   After the installation is complete, you will need to reboot the server. After the reboot:

1. Log in as user name `wrsroot` and password `wrsroot`. Make sure you change the password.
2. Temporarily assign an IP address to the `PXE NIC - eth0`. Use the IP you have reserved for the KVM PXE.

```
ip addr add <CIDR> dev eth0
ifconfig eth0 up
```

3. Set the default gateway to the PXE network gateway

```
route add default gw <CIDR_gateway_IP>
```

4. Copy the following KVM revion license files from the lifecycle manager to the `/home/wrsroot/` directory of the `controller-0`.

   - `license.lic` Located in the `/root/cg-hlm/windriver-files` directory
   - `region_config` Located in the `/var/hlm/clouds/<cloud-name>/desired_state/<cloud-name>/001/base/stage/windriver-config` directory
   - `cakey.pem` Located in the `/var/hlm/clouds/<cloud-name>/desired_state/<cloud-name>/001/base/stage/windriver-config` directory

   These files are loaded to the lifecycle manager during the installation process.

Step 2: Deploy the KVM Region Custom Patch

This patch addresses a number of issues in the KVM region.

1. On KVM region `controller-0`, create a directory for the patch:

```
mkdir -p /tmp/patches
```

2. Copy the following patch file to the `/tmp/patches` directory:

   - `TS_HP_15_Custom_PATCH_0001_2.patch`

     You should have downloaded this patch file in the Prerequisites.

3. Execute the following commands:

```
sudo sw-patch upload-dir /tmp/patches
sudo sw-patch query
sudo sw-patch query-hosts
sudo sw-patch apply TS_HP_15_Custom_PATCH_0001_2.patch
source /etc/nova/openrc
```

4. Patch the standby controller:

```
system host-patch-reboot <standby-controller>
```

Assuming controller-0 is active controller:

```
system host-patch-reboot controller-1
```

5. After the patched controller node comes up, switch the active controller:

```
system host-swact <active-controller>
```

Assuming controller-0 is active controller:

```
system host-swact controller-0
```

6. Exit the SSH session and login to the newly active controller.
7. Execute the following commands:

```
source /etc/nova/openrc
```

8. Patch the standby controller:

```
system host-patch-reboot <standby-controller>
```

9. Reboot the compute nodes:

```
system host-patch-reboot compute-0
system host-patch-reboot compute-1
```

10. Make controller-0 active:

```
system host-swact controller-1
```

Step 3: Configure the KVM region cloud

1. In the iLO web interface, launch a console session to the `controller-0` node.
2. Execute the following command to install the KVM region cloud:

Important: Always execute this command from a console window, not an SSH session

```
sudo config_region region_config
```

```
localhost:~$ sudo config_region
Parsing region configuration file...  DONE
Validating region configuration file...  DONE
Configuring management interface...  DONE
Retrieving keystone token... DONE
Retrieving services, endpoints and users from keystone...  DONE
Validating keystone configuration...  DONE
Creating config apply file...  DONE

Applying configuration (this will take several minutes):
```

Ignore the message which displays during `config_region` process.

```
Step 9 of 29 [####  ]dm-6 WRITE SAME failed. Manually zeroing.
```

```
Applying configuration (this will take several minutes):
Step  9 of 29 [############  ]dm-6: WRITE SAME failed. Manually zeroing.
INIT: Id "pmon" respawning too fast: disabled for 5 minutes ]
Step 29 of 29 [##############################################]
localhost:~$ _
```

3. After `controller-0` is deployed, add and configure the remaining nodes as `controller-1` and `compute-'n'`.

```
system host-add --hostname controller-1 --personality controller --
mgmt_mac <mgmt_mac> --bm_mac <bm_mac> --bm_ip <ilo_ip> --bm_type ilo4 --
bm_username <ilo_user> --bm_password <ilo_password>
system host-add --hostname <unique-compute-name> --personality compute --
mgmt_mac <mgmt_mac> --bm_mac <ilo_mac> --bm_ip <ilo_ip> --bm_type ilo4 --
bm_username <ilo_user>  --bm_password <ilo_password>
```

Note: When adding a controller, the name is assigned in order. Unique controller names are ignored.

```
+-------------------------------------+
| Value                               |
+-------------------------------------+
| none                                |
| locked                              |
| offline                             |
| 10.1.3.46                           |
| fc:15:b4:93:3b:b8                   |
| ilo4                                |
| cghelion                            |
| {u'bm_region': u'External'}         |
| 2015-08-18T20:23:07.823701+00:00    |
| None                                |
| b53demo-compute0                    |
| None                                |
| None                                |
| None                                |
| 3                                   |
| None                                |
| None                                |
| {}                                  |
| 10.20.3.70                          |
| d0:bf:9c:c0:9b:f8                   |
| disabled                            |
| compute                             |
| False                               |
| None                                |
| None                                |
| None                                |
| 0                                   |
| 32c032e1-fe5e-4f00-a478-d20fb77e971e |
+-------------------------------------+
```

4. In the iLO web interface, set the controller and compute nodes to one-time PXE booting from the network.
5. Restart the nodes.
6. *Access the Horizon dashboard* using the CAN network IP (HTTPS).
7. Select **regionkvm** in the *region selector*.
8. Click **Admin** then **Inventory** to monitor the status of nodes being PXE booted. After a succesful PXE boot, the **Operational State** should be **Disabled** and the **Availability State** should be **Online**.

   Note: The Horizon Dashboard will be running on the first IP address of the CLM network range (refer to the `ip_start_address` value provided for the CLM network in the `definition.json` during the non-KVM Region deployment).

The log-in credentials for Horizon are as follows:

```
username: admin
password:  <random>
```

The Horizon password is randomly generated during the installation. You can locate the password in the `stackrc` file on any of the non-KVM region controllers.

Step 4: Configure and unlock the compute controllers

After the controller-1 and the compute nodes come up successfully after PXE boot, execute the following commands from controller-0 to unlock each compute node in the inventory.

- *For a Non-Bonded Environment*
- *For a Bonded Environment*

For a Non-Bonded Environment

1. After the controller-1 and the compute nodes come up successfully after PXE boot, execute the following commands from controller-0 to unlock the compute nodes.

   a. Create the Infra interface:

   ```
   system host-if-add -V <bls/infra VLAN ID> -nt <network_type> <host-name
    or ID> <interface_name> <interface_type> <port or interfaces>
   ```

   b. Add an IP address to the Infra interface:

   ```
   system host-addr-add <host-name or ID> <interface_name> <ipv4/
   ipv6_address> <prefix-length>
   ```

   c. Configure the VRS interface:

   ```
   system host-if-modify <host-name or ID> -n <interface_name> -nt
    <network_type> --ipv4-mode=static eth-x
   ```

   Where `eth-x` is the interface on which untagged TUL is presented.

   d. Add an IP address to the VRS interface:

   ```
   system host-addr-add <host-name or ID> vrs <ipv4/ipv6_address>
    <prefix_length>
   ```

   e. Update the host:

   ```
    system host-update <host-name or ID> vsc_controllers=<ipv4/
   ipv6_address>,<ipv4/ipv6_address>
   ```

   Enter the IP address of the VSC controllers

   f. Unlock the host:

   ```
   system host-unlock <host-name or ID>
   ```

   Example commands:

   ```
   system host-if-add -V 722 -nt infra compute-3 infra vlan pxeboot0
   system host-addr-add compute-3 infra 10.70.22.81 24
   system host-if-modify compute-3 -n vrs -nt data-vrs --ipv4-mode=static
    eth4
   system host-addr-add compute-3 vrs 10.70.5.83 24
   system host-update compute-3 vsc_controllers=10.70.5.31,10.70.5.32
   ```

```
system host-unlock compute-3
```

For bonded NIC environments

If you are using a bonded NIC environment, after configuring and unlocking the compute nodes, perform these steps:

1. Use the following commands to delete the MGMT interface:
   a. Obtain the compute name or ID number:

   ```
   system host-list
   ```

   b. Obtain the UUID of the MGMT interface to remove:

   ```
   system host-if-list
   ```

   c. Remove the PXE boot flag off the interface:

   ```
   system host-if-modify -nt "none" compute-0 pxeboot0
   ```

   d. Delete the interface:

   ```
   system host-if-delete compute-0 95e7b495-1454-49d1-8123-301215503e86
   ```

2. Use the following commands to create a bonded interface and setup node to be unlocked:

```
system host-if-add -a 802.3ad -x layer2 -nt pxeboot compute-0 bond0 ae
 "none" eth0 eth1
system host-if-add -V 303 -nt mgmt compute-0 mgmt vlan bond0
system host-if-add -V 74 -nt infra compute-0 infra vlan bond0
system host-addr-add compute-0 infra 172.16.74.244 24
system host-if-add -a balanced -x layer2 -nt "none" compute-0 bondvrs ae
 "none" eth2 eth3
```

3. Use one of the following steps to configure a static IP address for the bonded NIC interface or assign an IP address from an IP address pool:
   - To assign a static IP:

   ```
   system host-if-modify compute-0 -nt data-vrs --ipv4-mode=static bondvrs
   system host-addr-add compute-0 bondvrs 10.30.6.244 24
   ```

   - To assign an IP address from a pool:

   ```
   system addrpool-add vrspool 10.30.6.0 24 --order random --ranges
    10.30.6.240-10.30.6.249
   system host-if-modify compute-0 bondvrs -nt data-vrs --ipv4-mode=pool --
   ipv4-pool=vrspool
   system host-if-modify compute-1 bondvrs -nt data-vrs --ipv4-mode=pool --
   ipv4-pool=vrspool
   ```

4. Execute the following command to assign IP addresses to compute-0:

```
system host-update compute-0 vsc_controllers=10.30.6.31,10.30.6.32
```

Step 5: Deploy the Horizon Patch

Due to an API error, you cannot create a PCI-Passthrough or SR-IOV interface using the Horizon UI. To correct this issue, deploy the following patch.

You should have downloaded the following patch files during the prerequisites:

- WR-HZN-1011

The README with the patch download contains information on files changed by these patches.

Execute the following commands:

1. Copy the WR-HZN-1011 directory to the `/var/hlm/clouds/<cloudname>/patches` directory on the lifecycle manager.
2. Execute following command to apply patch

   ```
   hlm patch -c <cloud-name> -n WR-HZN-1011 -t <tier>
   ```

   Where: <tier> is the tier on which the various controllers are running.

   For example:

   ```
   hlm patch -c sac36 -n WR-HZN-1011 -t BASE-CCP-T2
   ```

   The tier information can be found in the `/var/hlm/clouds/<cloudname>/desired_state/<cloudname>/001/base/stage/ansible/hosts` file.

Next Steps

Post-Installation Tasks.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Post-Installation Tasks in a Denver Deployment

After HP Helion OpenStack Carrier Grade is fully installed and deployed, perform the tasks in this section.

Perform a full backup

After the deployment is complete, do a full backup of the deployment. This will make it easier to recover should you encounter a problem. For more information, see *Backup and Restore Configuration Files*.

Verify the VSC VMs

The installation process creates virtual machines for VSC. VSC VMs are installed and are operational.

For more information, see *Verifying the VSC VMs*.

Verify the VRS-G Node

The installation creates a VRS-G node as part of the cloud deployment. Use the following command to verify that the VRS-G is active.

For more information, see *Verifying the VRS-G Node*.

Verify LDAP

You should verify that LDAP is functioning correctly.

For more information, see *Verifying the LDAP Deployment*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 8A- Verifying the LDAP Deployment

After installing HP Helion OpenStack Carrier Grade, you can use the following commands to verify that LDAP is functioning correctly.

Verify the VRS-G Node

The installation creates a VRS-G node as part of the cloud deployment. Use the following command to verify that the VRS-G is active:

```
show vswitch-controller vswitches
```

The output for the command should appear similar to the following image:

```
-------------------------------------------------------------------------------
*A:vscha1# show vswitch-controller vswitches

===============================================================================
VSwitch Table
===============================================================================
vswitch-instance                Personality Uptime        Num VM/hostIf/BridgeIf
-------------------------------------------------------------------------------
va-10.20.6.2/1                  VRS         2d 20:25:30   0/0/0
va-10.20.6.3/1                  VRS         2d 20:25:09   0/0/0
va-10.20.6.12/1                 VRS         3d 20:25:00   0/0/0
va-10.20.6.13/1                 VRS         3d 20:25:00   0/0/0
va-10.20.6.106/1                VRS_G       3d 01:16:03   0/0/0
va-10.20.6.107/1                VRS_G       3d 01:16:06   0/0/0
-------------------------------------------------------------------------------
No. of virtual switches: 6
===============================================================================
```

Verify that the domain name and DNS server are listed in the `/etc/resolv.conf` file on all the cloud nodes,.

```
cat etc/resolv.conf
```

```
root@B51-CCP-T2-M1-NETCLM:~# cat /etc/resolv.conf
domain  dcn-one.helion.cg
nameserver  10.1.2.44
root@B51-CCP-T2-M1-NETCLM:~#
```

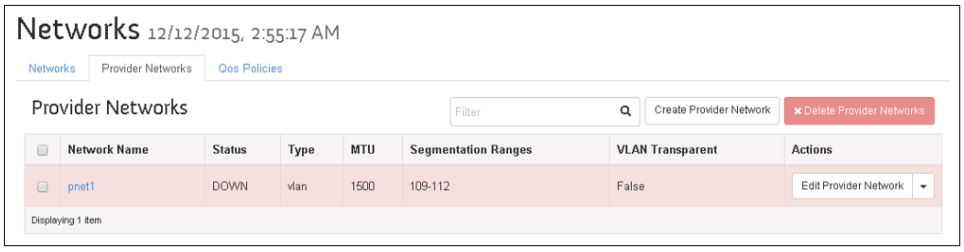
HP Helion OpenStack® Carrier Grade 2.1 Beta: Step 8B- Configuring the Provider Networks

After the HP Helion OpenStack Carrier Grade cloud is fully deployed, perform the following tasks in the Horizon UI.

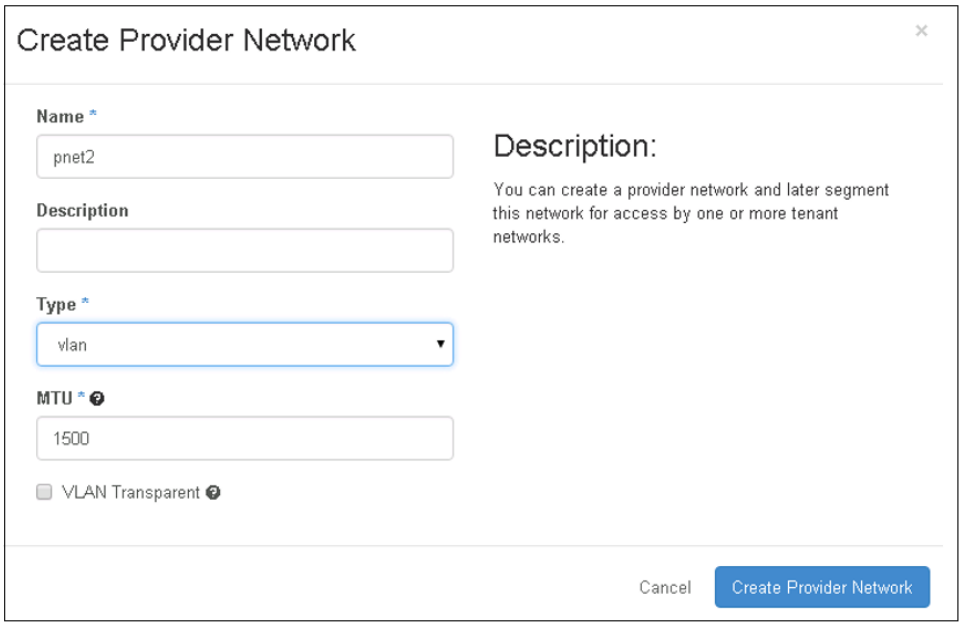
Create Provider Networks

Use the following steps to create a provider network. Or, see *Creating and Deleting Provider Networks* and *Creating a Segmentation Range*.

1. Launch the *Helion dashboard*
2. Click **Admin**, then **System**, then **Networks**.
3. Select the **Provider Networks** tab.

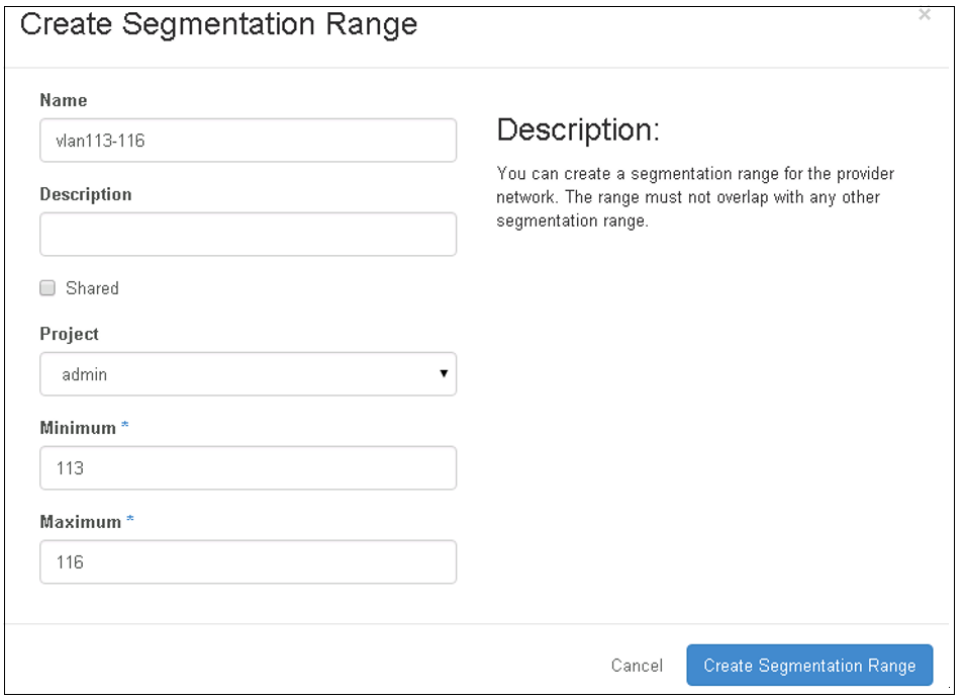


4. Click **Create Provider Network** button to create the provider network.



5. Add the VLAN ID range to a provider network.

6. Click **Create Range** to open the Create Segmentation Range page.

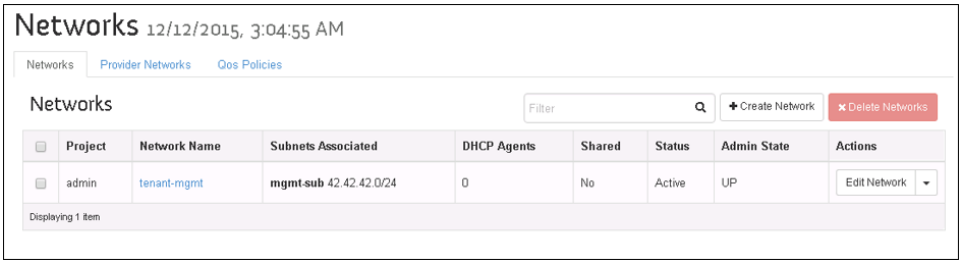


Complete the form as required.

- **Name** - Enter the name of the segmentation range.
- **Description** - Enter a free-text field for reference.

- **Shared** - If selected, shares the range for use by all tenants.
- **Project** - Select the tenant associated with the segmentation range.
- **Minimum** Enter the lowest value of a range of IDs.
- **Maximum** Enter the highest value of a range of IDs.

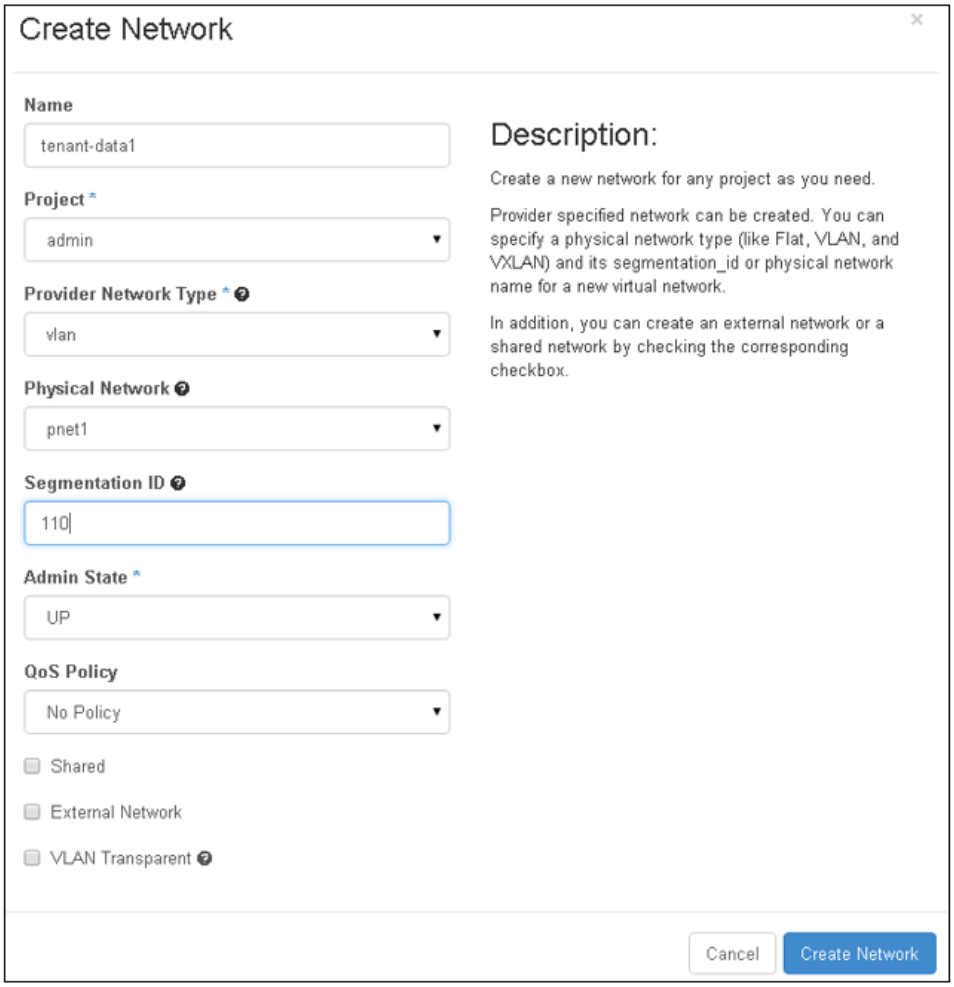
7. Click **Create Segmentation Range** to commit the changes.
8. Once the Provider network is successful, hit the network tab and create the necessary networks.



Create Networks

Use the following steps to create the required network. Or, see *Creating and Deleting Networks*.

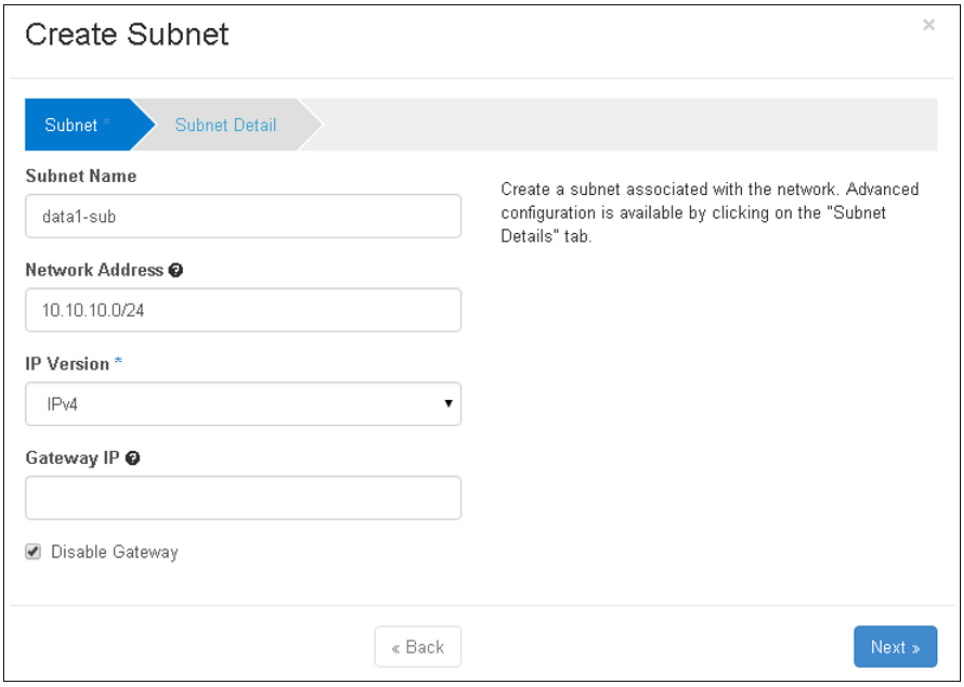
1. Click **Create Network** button to start creating the network.



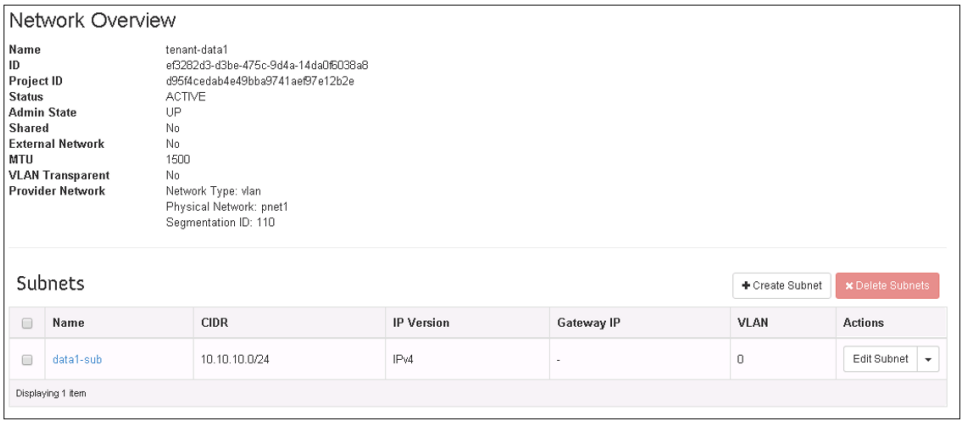
Note : Segmentation ID is the VLAN id that is intended to use for the network. For example, in the above diagram, we used 110 VLAN ID for the data network.

2. Click **Create Subnet**.

3. After the network is complete, click **Create Subnet**.



4. Complete the **Subnet** and **Subnet Detail** tabs.
5. Click **Create**.



HP Helion OpenStack® Carrier Grade 2.1 Beta: Known Issues and Workarounds

Before running the infra playbooks and bringing up HLM

Issue 0: The infra playbooks will also create Virtual Machines for Controllers. The UI now does it - so it must be disabled in infra playbooks

Workaround: Ensure in setup_vcloud.yml, all roles except SETUP-INFRA-ON-AV and HLM-CFG are either removed or commented.

Navigation on UI

Issue 1: Left side links "Manage Cloud" and Cloud Status Report dont work - they are under constructions

Workaround: Ignore these pages

Before Running any Deploy Workflow, apply the following workarounds:

Issue 2: wr.json generated by UI is malformed.

Cause: Disable the nuage_vrs field last minute before the build - caused this issue

Workaround: Manually correct the wr.json. Generate a temporary cloud definition using rcp topology. Copy its wr.json into your current cloud folder under vars subfolder and hand edit with correct values

Issue 3: UI will fail your CLM network validation

Cause: Validation checks if the startip is in-use, and fails if it is. But in CLM case - the startip is always in use cause its used by HLM.

Workaround: Ignore the UI failure and proceed to the next page of the wizard

Issue 4: Correct node-provision.json is not copied from temporary location to your cloud folder by UI

Cause: The some paths have changed after deploying the hlm-ui on /var/*www*... path which the code was not build to handle.

Workaround: After clicking Finish on Cloud Input Wizard, manually copy node-provision.json from /root/hlm-ui/hcginstaller-src/DB_JSON/node-provision.json to the /var/hlm/clouds/<yourcloud>/

During Deploy Workflow from UI:

Issue 5: Provisioning took very long on one of our test beds. The controllers were already provisioned and booted.

Workaround: If the process is not ending, ensure your ssh into each controller using its PXE IP. PXE IP can be found in nodes.json file under cloud folder. If the process is still running kill it. Do ps aux | grep python and see the line that has provision in it and kill that process and proceed with generate step

Next Step

Launching the Horizon Interface

HP Helion OpenStack® Carrier Grade 2.1 Beta: Configuring SR-IOV or PCI-Passthrough

You can connect a VM directly to a physical interface using PCI passthrough or SR-IOV.

SR-IOV

A PCI-SIG Single Root I/O Virtualization and Sharing (SR-IOV) Ethernet interface is a physical PCI Ethernet NIC that implements hardware-based virtualization mechanisms to expose multiple virtual network interfaces that can be used by one or more virtual machines simultaneously.

With SR-IOV based NICs, the traditional virtual bridge is no longer required. Each SR-IOV port is associated with a virtual function (VF).

When compared with a PCI Passthtrough Ethernet interface, a SR-IOV Ethernet interface:

- Provides benefits similar to those of a PCI Passthtrough Ethernet interface, including lower latency packet processing.
- Scales up more easily in a virtualized environment by providing multiple VFs that can be attached to multiple virtual machine interfaces.
- Shares the same limitations, including the lack of support for LAG, QoS, ACL, and live migration.
- Has the same requirements regarding the VLAN configuration of the access switches.

The process for configuring SR-IOV includes creating a VLAN provider network and subnet, then attaching VMs to that network. See *Configuring SR-IOV*.

PCI Passthrough Ethernet Interfaces

A passthrough Ethernet interface is a physical PCI Ethernet NIC on a compute node to which a virtual machine is granted direct access. This minimizes packet processing delays but at the same time demands special operational considerations.

For all purposes, a PCI passthrough interface behaves as if it were physically attached to the virtual machine. Therefore any potential throughput limitations coming from the virtualized environment, such as the ones introduced by internal copying of data buffers, are eliminated. However, by bypassing the virtualized environment, the use of PCI passthrough Ethernet devices introduces several restrictions that must be taken into consideration.

They include:

- no support for LAG, QoS, ACL, or host interface monitoring
- no support for live migration
- no access to the compute node's AVS switch

A passthrough interface bypasses the compute node's AVS switch completely, and is attached instead directly to the provider network's access switch. Therefore, proper routing of traffic to connect the passthrough interface to a particular tenant network depends entirely on the VLAN tagging options configured on both the passthrough interface and the access port on the switch.

The access switch routes incoming traffic based on a VLAN ID, which ultimately determines the tenant network to which the traffic belongs. The VLAN ID is either explicit, as found in incoming tagged packets, or implicit, as defined by the access port's default VLAN ID when the incoming packets are untagged. In both cases the access switch must be configured to process the proper VLAN ID, which therefore has to be known in advance. See *Configuring PCI-Passthrough*.

Related links

For more information, see *SR-IOV Passthrough for Networking* in the OpenStack wiki.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Configuring SR-IOV

An *SR-IOV Ethernet interface* is a physical PCI Ethernet NIC that implements hardware-based virtualization mechanisms to expose multiple virtual network interfaces that can be used by one or more virtual machines simultaneously.

With SR-IOV based NICs, the traditional virtual bridge is no longer required. Each SR-IOV port is associated with a virtual function (VF).

The process for configuring SR-IOV includes creating a VLAN provider network and subnet, then attaching VMs to that network.

Configure WR Compute Nodes

1. Log into the KVM region `controller-0` node with root privileges.
2. Identify the compute node with Niantic NIC and configure the node.

```
system host-port-list <compute-name>
```

The Niantic NIC is displayed in the device column as `82599ES 10-Gigabit SFI/SFP+` .

For example:

```
system host-port-list tb4c1
+--------------------------------------+------+----------
+--------------+--------+-----------+-------------
+-----------------------------------------------+
| uuid                                 | name | type     | pci address  |
 device | processor | accelerated | device type
         |
+--------------------------------------+------+----------
+--------------+--------+-----------+-------------
+-----------------------------------------------+
| c64c1a38-8583-4912-bb48              | eth0 | ethernet | 0000:04:00.0 |
 0      | 0         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| 93595f54-1125-4c4d-b1e9              | eth1 | ethernet | 0000:04:00.1 |
 0      | 0         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| b51cfd2f-6986-44a2-bfba              | eth2 | ethernet | 0000:05:00.0 |
 0      | 0         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| 077ae91a-62df-4f82-a7bc              | eth3 | ethernet | 0000:05:00.1 |
 0      | 0         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| cdfdc700-bf4b-4850-83c5              | eth4 | ethernet | 0000:08:00.0 |
 0      | 0         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| fb3f8504-2dfd-4aec-8963              | eth5 | ethernet | 0000:08:00.1 |
 0      | 0         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| 8d49e7c4-b88f-4ada-969b              | eth6 | ethernet | 0000:81:00.0 |
 0      | 1         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| 318b6db3-2fa9-4a30-9ecd              | eth7 | ethernet | 0000:81:00.1 |
 0      | 1         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| 4e8f8a8f-18ad-4e40-bde8              | eth8 | ethernet | 0000:84:00.0 |
 0      | 1         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
| 8cc8cfb5-8794-451d-bf36              | eth9 | ethernet | 0000:84:00.1 |
 0      | 1         | True        | 82599ES 10-Gigabit SFI/SFP+ Network
 Connection |
+--------------------------------------+------+----------
+--------------+--------+-----------+-------------
+-----------------------------------------------+
```

3. Use the following commands to configure the NIC interface for SR-IOV.

```
system host-lock <compute-name>
system host-if-modify -nt pci-sriov -N <number-VFs> -p <provider-network>
 <compute-name> <interface>
system host-unlock <compute-name>
```

Where:

- `<compute-name>` is the compute node with the Niantic NIC
- `<number-VFs>` is the number of VFs to use
- `<provider-network>` is the physical network VLAN range presented to this port
- `<interface-name>` is the name Niantic NIC

In this example, Ethernet interface `eth8` is assigned the network type SR-IOV, enabled to use 16 VFs, and configured as connected to provider network `physnet1`.

```
system host-lock mem17-compute0
system host-if-modify -nt pci-sriov -N 16 -p physnet1 mem17-compute0 eth8
system host-unlock mem17-compute0
```

Create a Provider Network

Virtual machine instances (VMs) with SR-IOV interfaces require a VLAN provider network that is managed by the HPE Networking Service (Neutron). Provider networks are the payload-carrying networks used implicitly by end users when they move traffic over their tenant networks.

To create provider network:

1. Log into the KVM region `controller-0` node with root privileges.
2. Execute the following command to create the network:

```
neutron net-create <network-name> --provider:network_type
 vlan --provider:segmentation_id <segmentation_id>  --
provider:<physical_network_name>
```

Where:

- `<network-name>` is the name of the network
- `<segmentation_id>` is the VLAN ID
- `<physical_network_name>` is name of the physical network over which the virtual network is implemented.

The following example creates a neutron provider network with VLAN ID 810 and uses `physnet1`:

```
neutron net-create sriov-net-810 --provider:network_type vlan --
provider:segmentation_id 810  --provider:physical_network physnet1
```

3. Execute the following command to create a subnet:

```
neutron subnet-create --name <subnet-name> <network-name> <CIDR> --
disable-dhcp --no-gateway  --allocation-pool start=<IP_ADDR>,end=<IP_ADDR>
```

Where:

- `<subnet-name>` is the name of the network or subnet
- `<CIDR>` is the CIDR of subnet to create
- `<IP_ADDR>` is the start and end allocation pool IP addresses for this subnet (This option can be repeated).

The following example creates a subnet for the network just created:

```
neutron subnet-create --name subnet-810 hrushi-sriov-net-810
 31.31.31.0/24 --disable-dhcp --no-gateway  --allocation-pool
 start=31.31.31.100,end=31.31.31.200
```

Launch a Virtual Machine

You can now crate virtual machine instances using SR-IOV. There are two options to launch a VM using SRIOV:

- **Option A** Create a neutron port with vNIC type direct and launch a VM using that port. See the example below:

```
neutron port-create <network-name> --vnic-type direct
nova boot <vm-name> --image <image-name> --flavor <flavor-name> --nic
 port-id=<port-uuid>
```

Where:

- `network-name` is the name of the network to create the port
- `vm-name` is the name of the virtual machine name to create
- `image-name` is the name of the image to use when creating the VM (see `nova image-list`).
- `flavor-name` is the name of the flavor to use when creating the VM (see `nova flavor-list`).
- `port-uuid` is the UUID of the port to attach to the NIC.

```
neutron port-create 125e6f3c-e1aa-49c8-a20a-0ede67d9b6fe --vnic-type
 direct
nova boot sriov-fixed --image wrl --flavor 2 --nic port-id=abd5b42a-
e8f5-4297-91ba-707c01195cc7
```

- **Option B** Launch a VM with vif-model as *pci-sriov*. See the example below:

```
nova boot <vm-name> --image <image-name> --flavor <flavor-name> --nic
 port-id=<port-uuid>
```

Example:

```
nova boot sriov-vif-model --image wr-new --flavor m1.small --nic net-
id=125e6f3c-e1aa-49c8-a20a-0ede67d9b6fe,vif-model=pci-sriov
```

NOTE: The SR-IOV vNIC is not assigned an IP address automatically. The IP will be provided through the ToR switch and orchestrated by NFV-D. If you do not use the Orchestrator must manually assign IP.

Also see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

Related links

For more information, see *SR-IOV Passthrough for Networking* in the OpenStack wiki.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Configuring PCI-Passthrough

A *passthrough Ethernet interface* is a physical PCI Ethernet NIC on a compute node to which a virtual machine is granted direct access. This minimizes packet processing delays but at the same time demands special operational considerations.

Assumption:

- You have HP Helion OpenStack Carrier Grade is installed and running
- You have identified the NIC ports to be used for PCI Passthrough devices from each compute node

There are two methods to support PCI-PT vNICs:

- Classic community using nova flavor: This option is similar to attaching any pci device i.e. not only restricted to NIC device. The type of pci device, no of pci devices are driven through nova flavors. See *Classic community using nova flavor*.
- vif-model: This option is implemented using Wind River way of launching VMs using nova's extension named 'vif-model'. See *Using nova vif-model extension*.

Classic community using nova flavor

This option is similar to attaching any pci device i.e. not only restricted to NIC device. The type of pci device, no of pci devices are driven through nova flavors. Controller and compute use the alias mechanism to chose compute and pci devices respectively. The drawback of this approach is it doesn't indicate which tenant network the pci device is on and what is the IP-MAC relationship recorded in neutron. In short, this implementation is neutron unaware.

```
nova boot vm1-pci-pt1 --flavor pci-pt --image wr-new
```

Non-KVM Region

No changes needed on the controller nodes in the non-KVM region. However, if you need information on the provider network and the VLAN ranges configured for that network, view the `/etc/neutron/plugins/ml2/ml2_conf.ini` file. For example in this scenario, there are two provider networks: `physnet1` and `physnet2`. The examples in this document use `physnet1`.

```
[ml2_type_vlan]
network_vlan_ranges = physnet1:810:813,physnet2:814:815
```

Configure the KVM Region Controller Nodes

The *HPE Compute Service (Nova)* requires scheduling logic, based on the PCI device vendor ID and its alias, to pickup the right compute node . The alias typically refers to provider net.

1. Update the `pci_alias` field in the `/etc/nova/nova.conf` file on both KVM region controllers to indicate the PCI device to use, similar to the following example:

   ```
   [DEFAULT]
   pci_alias={"vendor_id":"8086", "product_id":"10fb", "name":"physnet1"}
   ```

   This command defines pci_alias `physnet1` to present a request for PCI devices with vendor_id as `0x8086` and product_id as `10fb`.

   The example used `physnet1` as in the earlier steps. `physnet1` represents a provider net where a set of VLANs are presented.

   Note: The product ID can be retrieved from the compute node by running the following command:
2. Get the PCI bus ID of one of the interfaces dedicated for PCI-passthrough interface. In this example, `eth8` is the PCI device:

   ```
   [root@mem17-compute1 ~(keystone_admin)]# ls -lrt /sys/class/net/eth8/device
   lrwxrwxrwx 1 root root 0 Oct 16 18:37 /sys/class/net/eth8/device -
   > ../../../0000:87:00.0
   ```
3. Using the PCI bus ID, you can get the product id, for example:

   ```
   [root@mem17-compute1 ~(keystone_admin)]# cat /sys/bus/pci/
   devices/0000:87:00.0/device
   0x10f8
   ```

Configure the KVM Region Compute Nodes

Update the `pci_passthrough_whitelist` of PCI devices available to VMs. This list gets created when you assign one or more interfaces as a pci-passthrough device. During this assignment, make sure that the name of the provider network (-p flag) is identical to the name provided in the `nova.conf` of the controller nodes.

```
system host-lock mem17-compute1
system host-if-modify -nt pci-passthrough -p physnet1 mem17-compute1 eth8
system host-unlock mem17-compute1
```

In this example, Ethernet interface `eth8` is assigned the network type `pci-passthrough`, and configured as connected to provider network `physnet1`.

Output:

```
[root@controller-0 nova(keystone_admin)]# system host-if-list mem17-compute1
+--------------------------------------+----------+-----------------
+----------+---------+-----------+---------------+----------------------
+------------+-------------------+
| uuid                                 | name     | network type    | type
  | vlan id | ports     | uses i/f      | used by i/f          | attributes |
 provider networks |
+--------------------------------------+----------+-----------------
+----------+---------+-----------+---------------+----------------------
+------------+-------------------+
```

```
| 022165ba-57fc-4061-a07f-54f3b9e9e89c | vrs      | data-vrs        | ethernet
 | None    | [u'eth6'] | []            | []                   | MTU=1500   |
 None              |
| 25167958-6ec4-477d-962e-b4fda445baa7 | infra    | infra           | vlan
  | 822     | []        | [u'pxeboot0'] | []                   | MTU=1500   |
 None              |
| 2cb17917-1683-403c-8b32-3896b4c4e91f | pxeboot0 | pxeboot         | ethernet
 | None    | [u'eth0'] | []            | [u'mgmt0', u'infra'] | MTU=1500   |
 None              |
| c4cb43cd-bddd-4999-bab5-2f0db8e6ac2f | eth8     | pci-passthrough | ethernet
 | None    | [u'eth8'] | []            | []                   | MTU=1500   |
 physnet1          |
| c67dcd7a-f117-4a01-907e-f60fc98e1b10 | mgmt0    | mgmt            | vlan
  | 802     | []        | [u'pxeboot0'] | []                   | MTU=1500   |
 None              |
| dbce134c-633f-4b0f-b4c9-73501ccda55c | eth9     | pci-sriov       | ethernet
 | None    | [u'eth9'] | []            | []                   | MTU=1500   |
 physnet2          |
| fdb4b7cf-6b8b-421a-bdc2-a07209a31548 | eth7     | pci-sriov       | ethernet
 | None    | [u'eth7'] | []            | []                   | MTU=1500   |
 physnet1          |
+--------------------------------------+----------+-----------------
+----------+---------+-----------+---------------+----------------------
+------------+-------------------+
```

After the interface is unlocked, the newly added PCI device ID is listed in the `/etc/nova/nova.conf` file. For example:

```
{"physical_network": "physnet1", "address": "0000:87:00.0"}
```

Execute the following command to validate that the correct PCI bus ID is listed for the interface. In this example, `eth8` is the PCI device:

```
[root@mem17-compute1 ~(keystone_admin)]# ls -lrt /sys/class/net/eth8/device
lrwxrwxrwx 1 root root 0 Oct 16 18:37 /sys/class/net/eth8/device -
> ../../../0000:87:00.0
```

Creating a Flavor

When crating new VM, you select a flavor to define that instance. A flavor is a list of attributes applied to a virtual machine when a new instance is created.

You can create flavors that request PCI devices when you create instances. When creating flavors for PCI passthrough, provide metadata similar to the following:

```
[root@controller-0 nova(keystone_admin)]# nova flavor-show pci-pt
+----------------------------
+------------------------------------------------------------------------------------------
+
| Property                   | Value
                                                                  |
+----------------------------
+------------------------------------------------------------------------------------------
+
| OS-FLV-DISABLED:disabled   | False
                                                                  |
| OS-FLV-EXT-DATA:ephemeral  | 0
                                                                  |
| disk                       | 2
                                                                  |
| extra_specs                | {"hw:wrs:pci_numa_affinity": "prefer",
 "pci_passthrough:alias": "physnet1:1", "hw:mem_page_size": "any"} |
| id                         | 813de4a1-0830-4809-8eb3-c017e59eb631
                                                                  |
| name                       | pci-pt
                                                                  |
```

```
| os-flavor-access:is_public | True
                                                                  |
| ram                        | 2048
                                                                  |
| rxtx_factor                | 1.0
                                                                  |
| swap                       |
                                                                  |
| vcpus                      | 1
                                                                  |
+----------------------------
+------------------------------------------------------------------------------------------
+
```

In the above example, the `"pci_passthrough:alias": "physnet1:1"` value indicates, schedule on the compute node which has PCI device with alias physnet1 and has at least 1 pci device. If you wish to launch a VM with 4 pci devices, the value would be 4.

Launching a VM

To implement PCI-passthrough you need to launch a VM using a flavor configured for passthrough.

In the following example, a VM is launched with 1 interface being virtio coming from management network. The PCI interface will show up automatically inside the VM. You need to manually assign IP to the raw device or create a VLAN interface and assign IP to ensure VMs can communicate through PCI device.

```
nova boot vm1-virtio-pci-pt1 --flavor pci-pt --image wr-new --nic net-
id=f38149ff-b745-4453-b737-4a8e86a846dc
[root@controller-0 ~(keystone_admin)]# nova show 3096f2e0-
a700-4567-8cc1-1014fbf6c157
+--------------------------------------
+------------------------------------------------------------------------------------------
+
| Property                             | Value

                                                |
+--------------------------------------
+------------------------------------------------------------------------------------------
+
| OS-DCF:diskConfig                    | AUTO

                                                |
| OS-EXT-AZ:availability_zone          | c1

                                                |
| OS-EXT-SRV-ATTR:host                 | mem17-compute1

                                                |
| OS-EXT-SRV-ATTR:hypervisor_hostname  | mem17-compute1

                                                |
| OS-EXT-SRV-ATTR:instance_name        | instance-0000005e

                                                |
| OS-EXT-STS:power_state               | 1

                                                |
| OS-EXT-STS:task_state                | -

                                                |
| OS-EXT-STS:vm_state                  | active

                                                |
```

```
| OS-SRV-USG:launched_at                | 2015-10-21T19:17:43.000000
                                                                    |
| OS-SRV-USG:terminated_at              | -
                                                                    |
| accessIPv4                            |
                                                                    |
| accessIPv6                            |
                                                                    |
| config_drive                          |
                                                                    |
| created                               | 2015-10-21T19:17:30Z
                                                                    |
| flavor                                | pci-pt (813de4a1-0830-4809-8eb3-
c017e59eb631)
                                                                      |
| hostId                                |
 6546371a0480bb8b8b055e8273ccb8fb2f3906b0ba89c8fa5204d84c
       |
| hrushi-appnet network                 | 30.30.30.23
                                                                    |
| id                                    | 3096f2e0-
a700-4567-8cc1-1014fbf6c157
                                                                                                        |
| image                                 | wr-new (3b944c85-fc8b-45ca-
a5af-7b6d746f36b2)
                                                                          |
| key_name                              | -
                                                                    |
| metadata                              | {}
                                                                    |
| name                                  | pci-pt-1
                                                                    |
| os-extended-volumes:volumes_attached | []
                                                                    |
| progress                              | 0
                                                                    |
| security_groups                       | default
                                                                    |
| status                                | ACTIVE
                                                                    |
| tenant_id                             | 55c75656e1dc4fcc8657394385e9a4dc
                                                                    |
| updated                               | 2015-10-21T19:17:43Z
                                                                    |
| user_id                               | f51a0888292a4e9eb0131ecef3407f3c
                                                                    |
```

```
| wrs-if:nics                          | {"nic1": {"vif_model": null,
 "mac_address": "fa:16:3e:4f:d6:c2", "port_id": "4c8fe01a-e1d8-4a91-
b780-0925ff1111aa", "network": "hrushi-appnet", "mtu": null}} |
| wrs-res:topology                     | node:0,  2048MB, pgsize:2M, vcpus:0

                                                 |
| wrs-res:vcpus                        | [1, 1, 1]

                                                 |
| wrs-sg:server_group                  |

                                                 |
+-------------------------------------
+------------------------------------------------------------------------------------------
+
```

Using the OpenStack Nova vif-model Extension

This option is implemented by launching VMs using the Nova vif-model extension'. When a VM is launched on a specific tenant network using 'vif-model' as 'pci-passthrough', a `neutron port-create` command is requested, which registers the mac address and IP reservation of the PCI-Passthrough interface and its .

```
nova boot vm1-pci-pt1  --image wr-new --flavor m1.small --nic net-
id=64291690-4086-4cb0-a764-9fb56971e863,vif-model=pci-passthrough
```

Create a neutron flat or VLAN network

Example, here provider net name being used is physnet1. The same value must be used when you configure compute host w/ pci device.

```
neutron net-create hrushi-sriov-net-810 --provider:network_type vlan --
provider:segmentation_id 810  --provider:physical_network physnet1
neutron subnet-create --name sriov-subnet-810 hrushi-sriov-net-810
 31.31.31.0/24 --disable-dhcp --no-gateway  --allocation-pool
 start=31.31.31.100,end=31.31.31.200
```

Define pci devices on the compute node

Ensure the -p flag is set to the name of the physnet used to create the flat network. Refer above step to define pci device and its provider net name.

```
system host-lock mem17-compute1
system host-if-modify -nt pci-passthrough -p physnet1 mem17-compute1 eth8
system host-unlock mem17-compute1
```

Launch VM using nova vif-model extension

Here the net-id is the vlan or flat network netid.

```
nova boot vm1-pci-pt1  --image wr-new --flavor m1.small --nic net-
id=64291690-4086-4cb0-a764-9fb56971e863,vif-model=pci-passthrough
```

Related links

For more information, see *PCI Passthrough* in the OpenStack wiki.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Best Practices

When working with HP Helion OpenStack Carrier Grade, review the following best practices.

Installation Best Practices

When deploying HP Helion OpenStack Carrier Grade, review the following best practices.

For more information, see *Installation Best Practices*.

HP Helion OpenStack® Carrier Grade 2.0: Installation Best Practices

When deploying HP Helion OpenStack Carrier Grade, review the following best practices.

Perform a Backup After Installation

After deployment is complete and cloud is configured with work loads, do a full backup of the cloud. This will make it easier to recover should you encounter a problem.

For more information, see *Backup and Restore Configuration Files*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Installing the Non-KVM Region

After the lifecycle manager is installed, the next task is to deploy the HP Helion OpenStack cloud into the non-KVM region.

Use one of the following links, depending upon which deployment model you are using:

- Denver. The Denver deployment includes a KVM region and uses AVS networking. See *Deploying the Denver template*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Installing the Non-KVM Region

After the lifecycle manager is installed, the next task is to deploy the HP Helion OpenStack cloud into the non-KVM region.

Use one of the following links, depending upon which deployment model you are using:

- Denver. The Denver deployment includes a KVM region and uses AVS networking. See *Deploying the denver template*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Configuring LDAP for Keystone v3

By default, the HP Helion OpenStack Carrier Grade services are configured to use Keystone v2 authorization. The services need to be modified to use Keystone v3. You will not be able to execute OpenStack CLI commands until the following changes are made on all three controller nodes in the non-KVM region.

Modify the `stackrc` files

The `stackrc` file is a configuration file that contains all of the settings that control the supported services and the repositories used to download the source for those services.

1. On the lifecycle manager host, use the following commands to modify the `/root/stackrc` file with values appropriate to your environment, using the following example.

```
export OS_PASSWORD=admin
export OS_USERNAME=admin
export OS_TENANT_NAME=admin
export OS_AUTH_URL=https://10.200.52.100:5000/v2.0
export OS_CACERT=/etc/stunnel/ssl/hlm/certs/ca.crt
export OS_REGION_NAME=memphis
unset OS_PROJECT_DOMAIN_NAME
unset OS_USER_DOMAIN_ID
unset OS_IDENTITY_API_VERSION
unset OS_AUTH_VERSION
unset OS_PROJECT_NAME
```

2. Execute the following commands to source the – `/root/stackrcv3` file:

```
source stackrcv3
```

3. Execute the following OpenStack CLI command to create a new project:

```
openstack project create ldapdemo --domain americas
```

```
+-------------+----------------------------------+
| Field       | Value                            |
+-------------+----------------------------------+
| description |                                  |
| domain_id   | c1f0e239545f428fb53128650ae23771 |
| enabled     | True                             |
| id          | a8df892e5100435fb08ef9660f4158b9 |
| name        | ldapdemo                         |
+-------------+----------------------------------+
```

4. Make note of the `domain-id`.
5. Execute the following command to list all user names:

```
openstack user list --domain Americas
```

```
+----------------------------------------------------------------+------------------
| ID                                                             | Name
+----------------------------------------------------------------+------------------
| f2322730f835a34ef5ee2af7e1a6af1cde7f6dc2da3a4387af62b5d228afed3f | admin
| f525e05d6e47cbd51117158f229340ed925a43dae06c7301a50fb2346abf8d4a | cinder
| 04bbaddd381fae6e8a20d2999d26676d721bd2633e84cb27edbaa274fc012dee | nova
| 60315befce457854a036da1e5d46475de70fa0488f96949530781d8999d2cacf | glance
| 74afb5b91975d1174d08dcff229063eadc773b90492556348d0aaaa7a9ca73bf | demo
| d3b7e7ab795a19ed8fce25b1d91b202289828c26b2994090a26ce283023b6e97 | ceilometer
| 92457ec2c7165d41b4a7ee86350cceaa8ca1e6d20ea2a5a410680f185d800be7 | heat
| 6946e9c299d09ddb0f9a929c1c1b16c87930099f764ae6092e3d3d0da03937fe | swift
| 2ea3bf0678164b09bdd9644e6d6a97863501529a5a3a7ecdabb07128d101b0a6 | neutron
| e3dc162c43230e66dad314d5f9664f0452883ecabfb8feee860438dbf179e97b | cg-ldap
| c4f791623849d082708deee86fef253f84b848b12aaed067c7b70292f8b30986 | cg-ldap-admin
| 533e3d290490ccf8fa4e61127af6a64c643d7e3e88dd9adac0b41796c49f3748 | patching
| 60f99b5af93b70e1ac7846dba86a786a60e298007e3965025682d911cb379d8c | power_mgmt
| a31f83080572f100dfde046c666fb0f99d2b2b53fcf350fca842cb8085bb0990 | sysinv
| 95651c66f4965ad5da360e6854062de7c3ed5aeaaf5076e9f10890484e4b971f | heat_domain_admin
| f5e439af51702c16d2a76a3ecdcdfc4b8f75d51f2fd926346875d1ee469dd258 | ldapuser1
| 1cbf1ddd1f9fbc14b11441df97165ea15052866efa7710a14f6488c3c31410af | ldapuser2
+----------------------------------------------------------------+------------------
```

6. Make note of the ID number for the `cg-ldap-admin` user.
7. Execute the following command to add the `cg-ldap-admin` user (from the previous step) as an admin to the project you created as an admin.

```
openstack role add --user <user id> --project ldapdemo admin
```

8. Create a text file with the LDAP username/password, project/tenant name, domain name and ID, Identity service API version, and other values as shown:

```
export OS_USERNAME=<ldapusername>
export OS_PASSWORD=<ldapuserpassword>
export OS_PROJECT_NAME=ldapdemo
export OS_TENANT_NAME=ldapdemo
export OS_PROJECT_DOMAIN_NAME=americas
export OS_USER_DOMAIN_ID=<DOMAIN_GUID>
export OS_IDENTITY_API_VERSION=3
export OS_AUTH_VERSION=3
export OS_AUTH_URL=<CAN_AUTH_URL>
```

```
#export OS_AUTH_URL=<CLM_AUTH_URL>
export OS_CACERT=/etc/stunnel/ssl/hlm/certs/ca.crt
export OS_REGION_NAME=memphis
```

The file should appears similar to the following:

```
export OS_USERNAME=cg-ldap
export OS_PASSWORD=cg-ldap
export OS_PROJECT_NAME=ldapdemo
export OS_TENANT_NAME=ldapdemo
export OS_PROJECT_DOMAIN_NAME=americas
export OS_USER_DOMAIN_ID=48b0aac906394e99855af16bfdbd9d32
export OS_IDENTITY_API_VERSION=3
export OS_AUTH_VERSION=3
export OS_AUTH_URL=https://10.20.4.100:5000/v3
#export OS_AUTH_URL=http://10.20.3.103:35357/v3
export OS_CACERT=/etc/stunnel/ssl/hlm/certs/ca.crt
export OS_REGION_NAME=regionone
```

9. Save the files as `stackrcv3`, replacing the existing file.

Install the HPE Identity Operations (Keystone) package on all the controllers

1. On the lifecycle manager host, change to the to the `~/<cloudname>` directory.

```
cd ~/<cloudname>
```

2. Execute the following command, using your cloudname and failure-zone:

```
hupdate -c <cloudname> -f <failureZone> hoscg-update.tgz
```

Where:

- <cloudname> is the name of your cloud;
- <failurezone> is controller mapping can be obtained from <cloud-directory>/nodes.json file on the lifecycle manager host.

Execute this command on all three non-KVM controllers, using a different failure zone for each. The command output ends with the following upon completion:

```
PLAY RECAP
 *********************************************************************
B53DEMO-CCP-CPN-N0001-NETCLM : ok=10   changed=0    unreachable=0
 failed=0
B53DEMO-CCP-T1-M1-NETCLM     : ok=4    changed=0    unreachable=0
 failed=0
B53DEMO-CCP-T1-M2-NETCLM     : ok=4    changed=0    unreachable=0
 failed=0
B53DEMO-CCP-T2-M1-NETCLM     : ok=25   changed=0    unreachable=0
 failed=0
B53DEMO-CCP-T2-M2-NETCLM     : ok=52   changed=47   unreachable=0
 failed=0
B53DEMO-CCP-T2-M3-NETCLM     : ok=25   changed=0    unreachable=0
 failed=0
B53DEMO-CCP-VRG-N0001-NETCLM : ok=4    changed=0    unreachable=0
 failed=0
B53DEMO-CCP-VRG-N0002-NETCLM : ok=4    changed=0    unreachable=0
 failed=0
localhost                    : ok=6    changed=2    unreachable=0
 failed=0
```

Configure Controllers

On each of the three non-KVM region conrollers, you meed to perform the following tasks:

1. Replace the `/etc/keystone/keystone-paste.ini` file on all three controllers. From the lifecycle manager host, execute the following command for each controller:

   ```
   scp ~/~/patch_cghelion1.1/keystone-paste.ini cghelion@<controller-ip>
   ```

   Where: `<controller-ip>` is the IP address for each controller.
2. Edit the `/etc/nova/nova.conf` file to comment out the following line:

   ```
   #auth_version = 2.0
   ```
3. Edit the `/etc/ceilometer/ceilometer.conf` file to comment out the following line:

   ```
   #auth_version = 2.0
   ```
4. Modify Cinder and Glance INI files by making the following change:

   Replace `paste.filter_factory = keystoneclient.middleware.auth_token:filter_factory`

   With: `paste.filter_factory = keystonemiddleware.auth_token:filter_factory`

   In the following files:

   - /etc/cinder/api-paste.ini
   - /etc/glance/glance-api-paste.ini
   - /etc/glance/glance-registry-paste.ini
   - /etc/glance/glance-registry.conf
5. Execute the following commands to restart affected OpenStack services:

   ```
   service glance-registry restart
   service glance-api restart
   service cinder-api restart
   service nova-api restart
   ```
6. Execute a `glance image-list` command.

   ```
   glance image-list
   ```

   The output of the command appears similar to the following:

   ```
   /opt/stack/venvs/python-glanceclient/local/lib/python2.7/site-packages/
   requests/packages/urllib3/connection.py:251: SecurityWarning: Certificate
    has no `subjectAltName`, falling back to check for a `commonName` for
    now. This feature is being removed by major browsers and deprecated by
    RFC 2818. (See https://github.com/shazow/urllib3/issues/497 for details.)
   SecurityWarning
   /opt/stack/venvs/python-glanceclient/local/lib/python2.7/site-packages/
   requests/packages/urllib3/connection.py:251: SecurityWarning: Certificate
    has no `subjectAltName`, falling back to check for a `commonName` for
    now. This feature is being removed by major browsers and deprecated by
    RFC 2818. (See https://github.com/shazow/urllib3/issues/497 for details.)
   SecurityWarning
   +--------------------------------------+-------------+-------------
   +------------------+------------+--------+
   | ID                                   | Name        | Disk Format |
    Container Format | Size       | Status |
   +--------------------------------------+-------------+-------------
   +------------------+------------+--------+
   ```

```
| 46ffcdbb-e393-4730-8e4e-8592394bbc15 | cirros      | vmdk        | bare
            | 18743296   | active |
| e25e8f97-c130-4a82-8988-05483cd7701d | cirros-qcow | qcow2       | bare
            | 13200896   | active |
| 49ee2a3a-eb0e-4e14-a7aa-24e459f4497e | cirros-test | qcow2       | bare
            | 13147648   | active |
| 57fc3e34-910f-49e6-9277-a46ed8156b42 | rhel65vmdk  | vmdk        | bare
            | 1001783296 | active |
+--------------------------------------+-------------+-------------
+------------------+------------+--------+
```

Return installing the non-KVM region for:

- *Denver template*

HPE Helion OpenStack® Carrier Grade 2.1 Beta: Configuring NIC Bonding and PCI BUS Enumeration

HP Helion OpenStack® Carrier Grade 2.1 Beta: Administration

Refer to the table of contents on the left side of the screen for a link to the HP Helion OpenStack Administrator Guide and links to several other administrative tasks you can perform.

HP Helion OpenStack® Carrier Grade 2.1 Beta: KVM Region Administrator Guide

The *KVM Region Administrator Guide* is addressed to HP Helion OpenStack Carrier Grade administrators responsible for the following areas in the KVM region:

- Creating and maintaining resources used by end users (tenants), such as virtual machines, storage pools, network objects, and access credentials.
- Operating and maintaining components of the HP Helion OpenStack Carrier Grade product, such as clusters, nodes, system software, licensing files, and backup and restore facilities

See: *HP Helion OpenStack Carrier Grade Administrator Guide in PDF*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Centralized Logging Overview

Because a typical HP Helion OpenStack Carrier Grade cloud consists of multiple servers, locating a specific log from a specific server can be difficult.

The HP Helion OpenStack Carrier Grade Centralized Logging feature collects logs on a central system, rather than leaving the logs scattered across the network. The administrator can use a single Kibana interface to view log information in charts, graphs, tables, histograms, and other forms.

Centralized logging helps the administrator triage and troubleshoot the distributed HP Helion OpenStack Carrier Grade cloud deployment from a single location. The admin is not required to access the several remote servers (SSH) to view the individual log files.

Centralized logging logs the following *HP Helion services*:

- Identity (Keystone)
- Image Operations (Glance)
- Block Storage (Cinder)
- Orchestration (Heat)
- Ceilometer
- Compute Operations (Nova)

In addition Centralized Logging also processes logs for the following HP Helion OpenStack features:

- HAProxy

- syslog
- keepalived

This document describes the Centralized Logging feature and contains the following sections:

- *Installation*
- *Centralized Logging components*
- *Centralized Logging log types*
- *Kibana configuration*
- *Changing the default Kibana password* on page 83
- *Logging into Kibana*

Installation

The Centralized Logging feature is automatically installed on all controllers as part of the HP Helion OpenStack Carrier Grade installation.

No specific configuration is required to use Centralized Logging. However, you can tune or configure the individual components as needed for your environment. Tuning and configuring these components is outside the scope of this document.

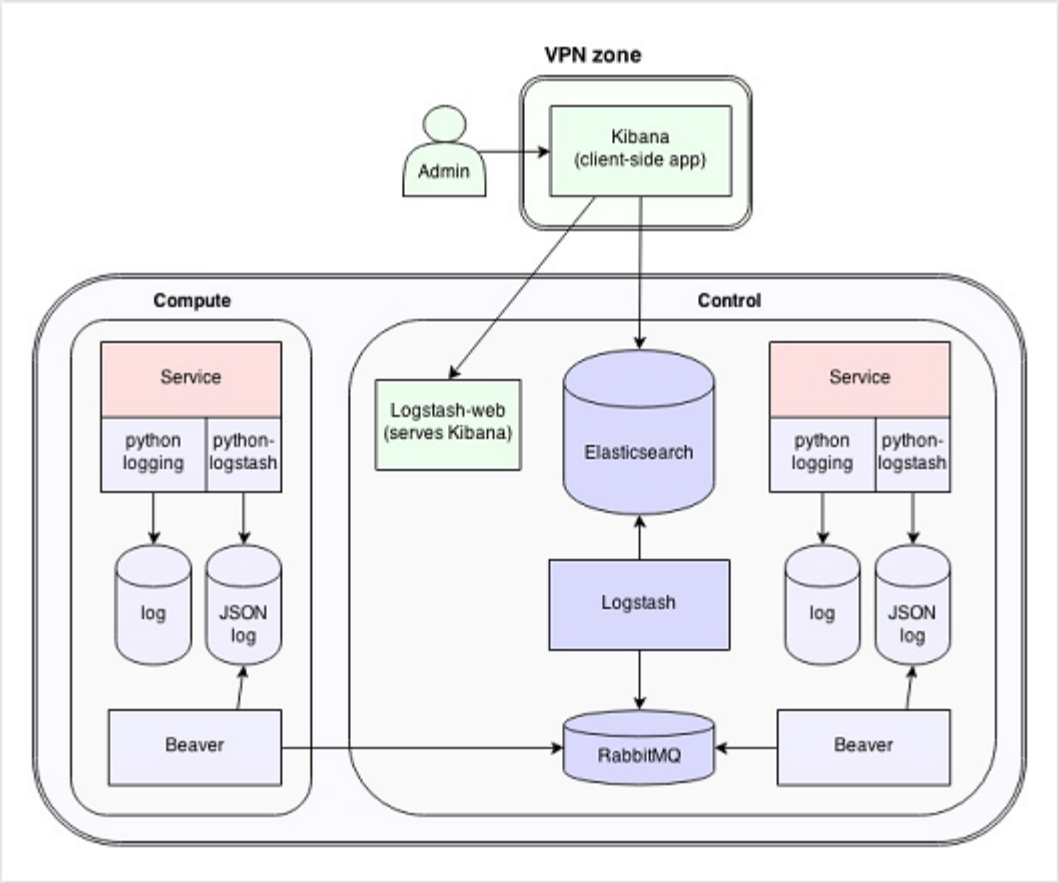
Centralized Logging components

Centralized logging consists of several components, including Logstash, Elasticsearch, RabbitMQ, and Kibana.

- **Beaver** is a python daemon that takes information in log files and sends the content to RabbitMQ.
- **RabbitMQ** is a message broker for collection of logging data across nodes.
- **logstash** is a log processing system for receiving, processing and outputting logs. logstash retrieves logs from RabbitMQ, processes and enriches the data, then stores the data in Elasticsearch.
- **Elasticsearch** is data store offering fast indexing and querying.
- **Kibana** is a client-side JavaScript application to visualize the data in Elasticsearch through a web browser. Kibana enables you to create charts and graphs using the log data.

These components are configured to work out-of-the-box and the admin should be able to view log data using the default configurations.

At a high level, the Helion services forward logs to Beaver. Then, Beaver forwards JSON messages to RabbitMQ on the controller0 node. Logstash connects to RabbitMQ to read queued messages and process the messages according to the Logstash configuration file. Logstash then forwards the processed log files in Elasticsearch. Users can use the Kibana interface to view and analyze the information, as shown in the following figure:



Note: Logging requires 4GB of disk space to make sure that all logging messages are retained.

Centralized Logging log types

The following table lists the types of logs collected by Centralized Logging and provides information on how the logs are maintained.

Data name	Confidentiality	Integrity	Availability	Backup?	Description
Log records	Restricted	High	Medium	No	Log records have a limited life, and are not archived. The log file on the local filesystem provides a fallback source of logging data (up to 20GB or 45 days) if the logging system fails.
Log metadata	Restricted	High	Medium	No	Elasticsearch indexes logged data to

Data name	Confidentiality	Integrity	Availability	Backup?	Description
					allow flexible searching.
Credentials	Confidential	High	Medium	No	Credentials for access to Elasticsearch and RabbitMQ are stored in configuration files owned by root with mode 0600.

Log rotation will happen daily or when the current logfile reaches 2GB, whichever happens sooner. The number of rotations held will be balanced to attempt to cap logs from all services at 200GB.

Kibana configuration

You can use the Kibana dashboards to view log data. Kibana is a tool developed to create charts, graphs, tables, and histograms based on logs send to Elasticsearch by logstash.

While creating Kibana dashboards is beyond the scope of this document, it is important to know that you can use the default Kibana dashboards or create custom dashboards. The dashboards are JSON files that you can modify or create new dashboards based on existing dashboards.

Note: Kibana is client-side software. To operate properly, the browser must be able to access port 81 on the HLM host.

Changing the default Kibana password

Follow these steps to change the default password of the Kibana web interface.

1. Log into one of the controller nodes in the non-KVM region.
2. Delete the Kibana password file.

```
rm /etc/logstash/kibana.htpasswd
```

3. Execute the followinf command:

```
htpasswd -b -c /etc/logstash/kibana.htpasswd kibana <new-password>
```

   Where <new-password> is the new Kibana password
4. Execute the following command to restart the apache2 service

```
service apache2 restart
```

5. Repeat these steps on all controllers in the non-KVM region.

Logging into Kibana

Launch a web browser on the seed cloud host to the following IP address, using the CLM virtual IP address for the controller you want to monitor:

```
http://<CLM_IP>:81
```

Example:

```
http://192.0.2.2:81
```

Log in with the user name/password. The user name is `kibana` and the password is the password you created in the previous section.

For more information

For information the centralized logging components, use the following links:

- *Logstash*
- *Elasticsearch*
- *RabbitMQ*
- *Kibana Dashboard*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Backup and Restore

HP Helion OpenStack Carrier Grade includes a backup and restore application called Attis which you can use to backup and restore essential system files and databases of the running cloud. Attis is automatically installed on each of the controller nodes in the non-KVM region. Attis uses a command line interface. For more information, see *Attis Backup and Restore CLI*.

Important: Before you start your first backup, you must use the Attis CLI to specify where HP Helion OpenStack Carrier Grade will store backup files. For more information, see *Configuring the Backup and Restore Location*

Attis Administrator Responsibilities for Protecting Credentials

Attis performs encrypted backup and restore of system data. The key for encryption and decryption is stored in the Attis configuration file on each controller node in `/root/crypt_key`. If this key is lost, your backups can not be restored. Consider storing the backup encryption key separately from your cloud infrastructure, in addition to the copy stored on each controller node.

Be aware that keys and passwords for other OpenStack services are stored in configuration files on cloud infrastructure nodes, protected by filesystem controls. Protect servers from unauthorized access and protect against exposure of credentials in configuration files. Attis backups contain copies of these credentials as well, protected using backup encryption, but exposure of the Attis backup key could result in unauthorized exposure of credentials stored in backups.

What gets backed up

The following components can be backed up and restored:

- Lifecycle manager data [opt and root files]
- Percona® XtraDB® cluster on controllers in non-kvm region
- Percona® XtraDB® cluster on VSD
- System files on VSC
- System files in kvm region
- MySQL database and Neutron, Nova, Ironic files under /etc on the baremetal controller (Sacramento deployments only)

Authenticate

Each Attis session, you must authenticate before executing any commands

1. Log one of the non-KVM region controllers as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Authenticate using export variables:

```
source stackrc
```

or

```
export OS_TENANT_NAME=<The name of your project/tenant>
export OS_USERNAME=<Your Helion OpenStack username>
export OS_PASSWORD=<Your Helion OpenStack password>
export OS_AUTH_URL=<The address of the Identity API served through
 keystone>
```

Optionally you can pass the authentication values when you execute a CLI command, for example:

```
--os-tenant-name "admin" --os-username "admin" --os-password "1234" --os-
auth-url "http://127.0.0.1:5000/v2.0"
```

Obtain the Attis config ID

Most of the Attis backup and restore commands require a config ID. You can obtain the ID using the `attis config` command.

1. Log one of the non-KVM region controllers as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Authenticate using export variables:

```
source stackrc
```

or

```
export OS_TENANT_NAME=<The name of your project/tenant>
export OS_USERNAME=<Your Helion OpenStack username>
export OS_PASSWORD=<Your Helion OpenStack password>
export OS_AUTH_URL=<The address of the Identity API served through
 keystone>
```

Optionally you can pass the authentication values when you execute a CLI command, for example:

```
--os-tenant-name "admin" --os-username "admin" --os-password "1234" --os-
auth-url "http://127.0.0.1:5000/v2.0"
```

4. Execute the following command:

```
attis config
```

The output appears similar to the following:

```
+----------------------------+-------------------------------------
+---------+---------------------------+---------+
| id                         | name                                | type
    | appliance                 | timeout |
+----------------------------+-------------------------------------
+---------+---------------------------+---------+
| 4c490c33-2f09-ca1aebf5a20d | Cloud_Controller_Appliance_DB_Backup |
 backup  | cloudcontrollerappliances | 3600    |
| f6b9215a-a5f2-07843de71e9a | HLM_Appliance_Data_Backup            |
 backup  | hlmappliances             | 3600    |
```

```
| 30490651-f820-d40f7f65c290 | HLM_Appliance_Data_Restore           |
 restore | hlmappliances             | 3600    |
| c9c69606-8fe3-b3e0419ad231 | HLM_Appliance_opt_files_Backup       |
 backup  | hlmappliances             | 3600    |
| 17edcc39-5f5c-39cc48c92895 | HLM_Appliance_opt_files_Restore      |
 restore | hlmappliances             | 3600    |
| 720264d5-fd17-f0a5e9b88ab3 | HLM_Appliance_root_files_Backup      |
 backup  | hlmappliances             | 3600    |
| c0e33946-6641-6ad688d2cf37 | HLM_Appliance_root_files_Restore     |
 restore | hlmappliances             | 3600    |
| b71d6f61-7347-e3929ac1e4a4 | VSC_Appliance_config_files_Backup    |
 backup  | vscappliances             | 3600    |
| b71e32b0-7347-e3929ac1e4a4 | VSC_Appliance_config_files_Restore   |
 restore | vscappliances             | 3600    |
| 098316b0-66c3-e3929ac1e4a4 | VSD_Appliance_DB_Backup              |
 backup  | vsdappliances             | 3600    |
| f4ec104f-6936-e3929ac1e4a4 | VSD_Appliance_DB_Restore             |
 restore | vsdappliances             | 3600    |
| 13b370f8-79f1-d72dee4aa55b | WR_Appliance_system_files_Backup     |
 backup  | wrappliances              | 3600    |
| 1cdcf21c-79f1-c76cce2f76d6 | WR_Appliance_system_files_Restore    |
 restore | wrappliances              | 3600    |
+----------------------------+-------------------------------------
+---------+---------------------------+---------+
```

Use the ID associated with the appropriate configuration file:

- `Cloud_Controller_Appliance_DB` -- Use this configuration file when backing up the MySQL database on a controller.
- `HLM_Appliance_Data` -- Use this configuration when backing up or restoring the lifecycle manager
- `HLM_Appliance_opt_files` -- Use this configuration when backing up or restoring the files in the `opt` directory on the lifecycle manager.
- `HLM_Appliance_root_files` -- Use this configuration when backing up or restoring the files in the `root` directory on the lifecycle manager.
- `VSC_Appliance_config_files` -- Use this configuration when backing up or restoring the VSC system files.
- `VSD_Appliance_DB` -- Use this configuration when backing up or restoring the VSD database.
- `WR_Appliance_system_files` -- Use this configuration when backing up or restoring the KVM-region system files.

See:

Backing Up the Cloud

Restoring the Cloud

Attis CLI for Backing Up and Restoring

HP Helion OpenStack® Carrier Grade 2.1 Beta: Configuring the Backup and Restore Environment

Before performing a back up or restore using Attis, perform the following one-time tasks:

- *Configuring the Backup and Restore Location* on page 87
- *Configure the restore templates* on page 88
- *#topic10581c2bc/trust*
- *Set the KVM Password* on page 89
- *#topic10581c2bc/baremetal*
- *#topic10581c2bc/keys*

Configuring the Backup and Restore Location

Before you start your first backup, you must use the Attis CLI to specify where HP Helion OpenStack Carrier Grade will store backup files. For information about the attis CLI, see the *Attis Backup and Restore CLI*.

You can store backup files using:

- SCP: A location on a remote server where the backup file is secure copied.
- NFS: A location on a network file system.
- FILE: A location on the cloud controller.

HPE recommends that you use an SCP or NFS server so that backup files are automatically moved to an off-appliance location in case of a catastrophic failure of the cloud controllers. You can use the FILE option if you want to manually mount shared storage on all three nodes of the cloud controller.

IMPORTANT: If you do not set a storage location, the backup will not succeed. In the backup job list, you will see that SSH connection to the storage path failed, and the state is Failed.

Perform the following steps on any cloud controller node.

1. Log into HLM node
2. SSH to any controller nodes from HLM using controller credentials (default username: cghelion)
3. Switch to the root user by running sudo –i.
4. Set the type of backup storage location.
   - To set the backup storage location to an SCP server, run:

     ```
     attis storage --use SCP
     ```

   - To set the backup storage location to an NFS server, run:

     ```
     attis storage --use NFS
     ```

5. List the storage details.

   ```
   root@ma1:~# attis storage
   +--------------------------------------+------+----------+
   | id                                   |type  |selected  |
   +--------------------------------------+------+----------+
   |529cd8fb-c6a2-401d-9caf-61caeede7f81  |FILE  |False     |
   |d6210603-01b1-4d76-9068-e3ffa44a449e  |NFS   |False     |
   |7abb6f30-3f10-4918-9f8d-a58b157d59b9  |SCP   |True      |
   +--------------------------------------+------+----------+
   ```

6. View the storage parameters that you will need to update by selecting the storage ID of the selected type. Example:

   ```
   root@ma1:~# attis storage --id 7abb6f30-3f10-4918-9f8d-a58b157d59b9
   +--------------------------------------+------+----------+
   | id                                   |type  |selected  |
   +--------------------------------------+------+----------+
   |7abb6f30-3f10-4918-9f8d-a58b157d59b9  |SCP   |True      |
   +--------------------------------------+------+----------+
   +---------------------------------+-------------------------------------
   +---------+
   |id           |storage_id        | parameter_name               | value
           |
   +---------------+---------------+---------------------
   +-------------------------+
   | 18bb9b5e-<...>| 7abb6f30-<...> | user                 |
           |
   | 78aaa60e-<...>| 7abb6f30-<...> | storage_path         |
           |
   ```

```
| c0a5c549-<...>| 7abb6f30-<...> | server               |
        |
| e34ac1b2-<...>| 7abb6f30-<...> | private_key_filepath | /home/
attis/.ssh/id_rsa |
+---------------+----------------+----------------------
+-------------------------+
```

7. Set the attis configuration of the storage type you entered in step 4 by entering:

```
attis storage --id <storage_id from the table> --update '{"parameter":"new
 value", "parameter":"new value"}'
```

where parameter in an SCP configuration is:

- user: User to SSH into the remote SCP server.
- storage_path: Path on the remote SCP server where you want to store backup files.
- server: IP address or DNS resolvable hostname of the remote server.
- private_key_filepath: Private key used to SSH to the remote SCP server. By default /home/attis/.ssh/id_rsa on the controller is prepopulated.

SCP Example

To specify the details of an SCP server to use for backup file storage:

```
attis storage --update '{"storage_path":"/
mybackupDirOnRemoteMachine","private_key_filepath":"/home/attis/.ssh/
id_rsa","server":"hostofscplocation","user":"remotescpuser"}' --id <copy
 the storage_id from attis storage>
```

IMPORTANT: If you select SCP, you must copy the public key text located at /home/attis/.ssh/id_rsa.pub from controller nodes and paste it into the authorized_keys file of the SCP server.

```
sudo su attis
ssh-copy-id <remotescpuser>@<hostofscplocation>
```

If you want to generate a new key for setting up trust between attis and the SCP server, copy the private key to each controller node. Then use the attis command storage --update to update the private_key_filepath.

NFS Example

To specify the details of an NFS server to use for backup file storage:

```
attis storage --update '{"server":"NFS server ip",
 "client_mount_path": "name of storage mount on cloud controller",
 "storage_path":"mybackupDironRemoteMachine"}' --id <copy the storage_id
 from attis storage>
```

8. Restart Attis server on all three controllers if the storage option is changed to NFS or FILE option:

```
service attis-server restart
```

Configure the restore templates

Before performing a restore:

1. Log into the cloud controller as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Update required parameters of the configuration template you are using before you trigger restore. Enter values into each of the blank fields in the file:

- **for NFS storage** edit `/etc/attis/config_template/cloudcontrollerappliancedbrestore_NFS.json` file
- **for SCP storage** edit the `/etc/attis/config_template/cloudcontrollerappliancedbrestore_scp.json` file.

You can use the `attis backuplog` command to locate the `backup_base_dirpath` and `restore_to_incrementnumber` values in the `base_folder` and `last_incremental_ref` column from output of command.

The following is an example of `/etc/attis/config_template/cloudcontrollerappliancedbrestore_scp.json`:

```
{
    "config": {
        "flow_name": "cloudcontrollerappliancedb",
        "name": "Percona_Xtradb_Restore_cloudcontrollerappliancedb",
        "parameters": {
            "target": "cloudcontrollerappliances",
            "Percona_XtraDB_Restore_temp_dirpath": "/home/attis-access",
            "Percona_XtraDB_Restore_target_user":"attis-access",
            "restore_dbpath": "/var/lib/mysql",
            "backup_base_dirpath":"2015-11-23-13:11:32",
            "restore_to_incrementnumber":"51288833"
        }
    },
    "storage": {
        "type": "SCP",
        "parameters": {
            "storage_path": "/home/attis-access",
            "user": "attis-access",
            "private_key_filepath":"/home/attis/.ssh/id_rsa",
            "server":"HLM-NETCLM"
        }
    }
}
```

4. Update the `Storage` parameters (SCP or NFS).

Set the KVM Password

If the KVM region controller username and/or password is set other than defaults, use the Attis CLI to update those values in the KVM region controller configurataion file.

To change the username/password:

1. Log into the active KVM region controller.
2. Execute the following commands:

```
attis config --id <config_id of WR_Appliance_system_files_Backup> --
update-parameter '{"wr_controller_backup_user":"YOUR_USER"}'
attis config --id <config_id of WR_Appliance_system_files_Restore> --
update-parameter '{"wr_controller_backup_password":"YOUR_PASSWORD"}
```

HP Helion OpenStack® Carrier Grade 2.1 Beta: Backing Up the Cloud

HP Helion OpenStack Carrier Grade includes a backup and restore application called Attis which you can use to backup and restore essential system files and databases of the running cloud. Attis is automatically installed on each of the controller nodes in the non-KVM region. Attis uses a command line interface. For more information, see *Attis Backup and Restore CLI*.

Important: Before you start your first backup, make sure Attis is properly configured. For more information, see *Configuring the Backup and Restore Environment*

Attis Administrator Responsibilities for Protecting Credentials

Attis performs encrypted backup and restore of system data. The key for encryption and decryption is stored in the Attis configuration file on each controller node in `/root/crypt_key`. If this key is lost, your backups can not be restored. Consider storing the backup encryption key separately from your cloud infrastructure, in addition to the copy stored on each controller node.

Be aware that keys and passwords for other OpenStack services are stored in configuration files on cloud infrastructure nodes, protected by filesystem controls. Protect servers from unauthorized access and protect against exposure of credentials in configuration files. Attis backups contain copies of these credentials as well, protected using backup encryption, but exposure of the Attis backup key could result in unauthorized exposure of credentials stored in backups.

When to perform backups

We recommend performing regular backups, preferably hourly, and especially after changing the configuration and before and after updating HP Helion OpenStack Carrier Grade software. Additionally, you should create a backup from HLM VM as follows:

- when the HP Helion OpenStack Carrier Grade installation is complete
- when any change is made to the HP Helion OpenStack Carrier Grade components

How to perform backups

- *Backing up the lifecycle manager* on page 91
- *Backup Cloud Controller Database* on page 92
- *#topic10581c2ab/vsd-database*
- *#topic10581c2ab/vsc*
- *Backup KVM region system files* on page 93
- *#topic10581c2ab/baremetal*

Obtain the Attis config ID

Most of the Attis backup and restore commands require a config ID. You can obtain the ID using the `attis config` command.

1. Log one of the non-KVM region controllers as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Authenticate using export variables:

```
source stackrc
```

or

```
export OS_TENANT_NAME=<The name of your project/tenant>
export OS_USERNAME=<Your Helion OpenStack username>
export OS_PASSWORD=<Your Helion OpenStack password>
export OS_AUTH_URL=<The address of the Identity API served through
 keystone>
```

Optionally you can pass the authentication values when you execute a CLI command, for example:

```
--os-tenant-name "admin" --os-username "admin" --os-password "1234" --os-
auth-url "http://127.0.0.1:5000/v2.0"
```

4. Execute the following command:

```
attis config
```

The output appears similar to the following:

```
+----------------------------+-------------------------------------
+---------+---------------------------+---------+
| id                         | name                                | type
    | appliance                 | timeout |
+----------------------------+-------------------------------------
+---------+---------------------------+---------+
| 4c490c33-2f09-ca1aebf5a20d | Cloud_Controller_Appliance_DB_Backup |
 backup  | cloudcontrollerappliances | 3600    |
| f6b9215a-a5f2-07843de71e9a | HLM_Appliance_Data_Backup            |
 backup  | hlmappliances             | 3600    |
| 30490651-f820-d40f7f65c290 | HLM_Appliance_Data_Restore           |
 restore | hlmappliances             | 3600    |
| c9c69606-8fe3-b3e0419ad231 | HLM_Appliance_opt_files_Backup       |
 backup  | hlmappliances             | 3600    |
| 17edcc39-5f5c-39cc48c92895 | HLM_Appliance_opt_files_Restore      |
 restore | hlmappliances             | 3600    |
| 720264d5-fd17-f0a5e9b88ab3 | HLM_Appliance_root_files_Backup      |
 backup  | hlmappliances             | 3600    |
| c0e33946-6641-6ad688d2cf37 | HLM_Appliance_root_files_Restore     |
 restore | hlmappliances             | 3600    |
| b71d6f61-7347-e3929ac1e4a4 | VSC_Appliance_config_files_Backup    |
 backup  | vscappliances             | 3600    |
| b71e32b0-7347-e3929ac1e4a4 | VSC_Appliance_config_files_Restore   |
 restore | vscappliances             | 3600    |
| 098316b0-66c3-e3929ac1e4a4 | VSD_Appliance_DB_Backup              |
 backup  | vsdappliances             | 3600    |
| f4ec104f-6936-e3929ac1e4a4 | VSD_Appliance_DB_Restore             |
 restore | vsdappliances             | 3600    |
| 13b370f8-79f1-d72dee4aa55b | WR_Appliance_system_files_Backup     |
 backup  | wrappliances              | 3600    |
| 1cdcf21c-79f1-c76cce2f76d6 | WR_Appliance_system_files_Restore    |
 restore | wrappliances              | 3600    |
+----------------------------+-------------------------------------
+---------+---------------------------+---------+
```

Use the ID associated with the appropriate configuration file:

- `Cloud_Controller_Appliance_DB` -- Use this configuration file when backing up the MySQL database on a controller.
- `HLM_Appliance_Data` -- Use this configuration when backing up or restoring the lifecycle manager
- `HLM_Appliance_opt_files` -- Use this configuration when backing up or restoring the files in the `opt` directory on the lifecycle manager.
- `HLM_Appliance_root_files` -- Use this configuration when backing up or restoring the files in the `root` directory on the lifecycle manager.
- `VSC_Appliance_config_files` -- Use this configuration when backing up or restoring the VSC system files.
- `VSD_Appliance_DB` -- Use this configuration when backing up or restoring the VSD database.
- `WR_Appliance_system_files` -- Use this configuration when backing up or restoring the KVM-region system files.

Backing up the lifecycle manager

You can use Attis to back up any of the following the lifecycle manager data:

- All files under the `/opt/` folder on the lifecycle manager host. This backs up all the installed code configuration and also `h*` installation scripts.
- All files under the `/root/` folder on the lifecycle manager host. This backs up all the source code, packages, linux netboot, infra-ansible-playbooks, SSH keys, and cloud folders.
- All files under `/root` and `/opt`.

Attis implements a tree-structure for certain backup/restore configurations. For example, to back up the `/opt` and `/root` folders on the lifecycle manager host:

1. Log in to lifecycle manager host as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Authenticate using export variables:

```
source stackrc
```

or

```
export OS_TENANT_NAME=<The name of your project/tenant>
export OS_USERNAME=<Your Helion OpenStack username>
export OS_PASSWORD=<Your Helion OpenStack password>
export OS_AUTH_URL=<The address of the Identity API served through
 keystone>
```

Optionally you can pass the authentication values when you execute a CLI command, for example:

```
--os-tenant-name "admin" --os-username "admin" --os-password "1234" --os-
auth-url "http://127.0.0.1:5000/v2.0"
```

4. Execute the following command to start the backup:

```
attis backup --config-id <Config_ID_of_HLM_Appliance_Data_Backup>
```

To only back up only the `/opt` files, execute the following command:

```
attis backup --config-id <Config_ID_of_HLM_Appliance_opt_files_Backup>
```

Backup Cloud Controller Database

You can use Attis to back up the three node MySQL cluster (Percona XtraDB Cluster) that runs in cloud controller nodes.

For disaster recovery, you should take full backups of the MySQL cluster frequently, such as on a daily basis. Backing up the node on any single controller will back up the full cluster.

1. Log in to one of the non-KVM region controllers as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Authenticate using export variables:

```
source stackrc
```

or

```
export OS_TENANT_NAME=<The name of your project/tenant>
export OS_USERNAME=<Your Helion OpenStack username>
```

```
export OS_PASSWORD=<Your Helion OpenStack password>
export OS_AUTH_URL=<The address of the Identity API served through
 keystone>
```

Optionally you can pass the authentication values when you execute a CLI command, for example:

```
--os-tenant-name "admin" --os-username "admin" --os-password "1234" --os-
auth-url "http://127.0.0.1:5000/v2.0"
```

4. Execute the following command to start the backup:

```
attis backup --config-id
 <Config_ID_of_Cloud_Controller_Appliance_DB_Backup>
```

If an entire cluster goes down, due to an issue (such as data corruption or MySQL defect), and the cluster does not come back up, you can use the backup to restore the cluster to a previous well-known state (backup) and start the cluster from that point.

Backup KVM region system files

You can use Attis to back up the KVM region system files.

To backup the KVM region system files:

1. Log into the active KVM region controller as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Authenticate using export variables:

```
source stackrc
```

or

```
export OS_TENANT_NAME=<The name of your project/tenant>
export OS_USERNAME=<Your Helion OpenStack username>
export OS_PASSWORD=<Your Helion OpenStack password>
export OS_AUTH_URL=<The address of the Identity API served through
 keystone>
```

Optionally you can pass the authentication values when you execute a CLI command, for example:

```
--os-tenant-name "admin" --os-username "admin" --os-password "1234" --os-
auth-url "http://127.0.0.1:5000/v2.0"
```

4. Execute the following command to perform the back up.

```
attis backup --config-id <Config_ID_of_ WR_Appliance_system_files_Backup>
```

HP Helion OpenStack® Carrier Grade 2.1 Beta: Restoring the Cloud

HP Helion OpenStack Carrier Grade includes a backup and restore application called Attis which you can use to backup and restore essential system files and databases on the running cloud. Attis is automatically installed on each of the controller nodes in the non-KVM region. Attis uses a command line interface. For more information, see *Attis Backup and Restore CLI*.

Important: Before you start your first backup, make sure Attis is properly configured. For more information, see *Configuring the Backup and Restore Environment*

Attis Administrator Responsibilities for Protecting Credentials

Attis performs encrypted backup and restore of system data. The key for encryption and decryption is stored in the Attis configuration file on each controller node in `/root/crypt_key`. If this key is lost, your backups can not be restored. Consider storing the backup encryption key separately from your cloud infrastructure, in addition to the copy stored on each controller node.

Be aware that keys and passwords for other OpenStack services are stored in configuration files on cloud infrastructure nodes, protected by filesystem controls. Protect servers from unauthorized access and protect against exposure of credentials in configuration files. Attis backups contain copies of these credentials as well, protected using backup encryption, but exposure of the Attis backup key could result in unauthorized exposure of credentials stored in backups.

When to restore

You should restore the HLM VM or other appliances if there are any issues with the HP Helion OpenStack Carrier Grade components, for example:

- there is database corruption
- when two controllers have failed. HA Services are not guaranteed to be resilient after a second failure.

Obtain the Attis config ID

Most of the Attis backup and restore commands require a config ID. You can obtain the ID using the `attis config` command.

1. Log one of the non-KVM region controllers as the `cghelion` user.
2. Change to the root user:

   ```
   sudo -i
   ```

3. Authenticate using export variables:

   ```
   source stackrc
   ```

   or

   ```
   export OS_TENANT_NAME=<The name of your project/tenant>
   export OS_USERNAME=<Your Helion OpenStack username>
   export OS_PASSWORD=<Your Helion OpenStack password>
   export OS_AUTH_URL=<The address of the Identity API served through
    keystone>
   ```

   Optionally you can pass the authentication values when you execute a CLI command, for example:

   ```
   --os-tenant-name "admin" --os-username "admin" --os-password "1234" --os-
   auth-url "http://127.0.0.1:5000/v2.0"
   ```

4. Execute the following command:

   ```
   attis config
   ```

   The output appears similar to the following:

   ```
   +----------------------------+--------------------------------------
   +---------+---------------------------+---------+
   | id                         | name                                 | type
       | appliance                 | timeout |
   +----------------------------+--------------------------------------
   +---------+---------------------------+---------+
   ```

```
| 4c490c33-2f09-ca1aebf5a20d | Cloud_Controller_Appliance_DB_Backup |
 backup  | cloudcontrollerappliances | 3600    |
| f6b9215a-a5f2-07843de71e9a | HLM_Appliance_Data_Backup            |
 backup  | hlmappliances             | 3600    |
| 30490651-f820-d40f7f65c290 | HLM_Appliance_Data_Restore           |
 restore | hlmappliances             | 3600    |
| c9c69606-8fe3-b3e0419ad231 | HLM_Appliance_opt_files_Backup       |
 backup  | hlmappliances             | 3600    |
| 17edcc39-5f5c-39cc48c92895 | HLM_Appliance_opt_files_Restore      |
 restore | hlmappliances             | 3600    |
| 720264d5-fd17-f0a5e9b88ab3 | HLM_Appliance_root_files_Backup      |
 backup  | hlmappliances             | 3600    |
| c0e33946-6641-6ad688d2cf37 | HLM_Appliance_root_files_Restore     |
 restore | hlmappliances             | 3600    |
| b71d6f61-7347-e3929ac1e4a4 | VSC_Appliance_config_files_Backup    |
 backup  | vscappliances             | 3600    |
| b71e32b0-7347-e3929ac1e4a4 | VSC_Appliance_config_files_Restore   |
 restore | vscappliances             | 3600    |
| 098316b0-66c3-e3929ac1e4a4 | VSD_Appliance_DB_Backup              |
 backup  | vsdappliances             | 3600    |
| f4ec104f-6936-e3929ac1e4a4 | VSD_Appliance_DB_Restore             |
 restore | vsdappliances             | 3600    |
| 13b370f8-79f1-d72dee4aa55b | WR_Appliance_system_files_Backup     |
 backup  | wrappliances              | 3600    |
| 1cdcf21c-79f1-c76cce2f76d6 | WR_Appliance_system_files_Restore    |
 restore | wrappliances              | 3600    |
+----------------------------+--------------------------------------
+---------+---------------------------+---------+
```

Use the ID associated with the appropriate configuration file:

- `Cloud_Controller_Appliance_DB` -- Use this configuration file when backing up the MySQL database on a controller.
- `HLM_Appliance_Data` -- Use this configuration when backing up or restoring the lifecycle manager
- `HLM_Appliance_opt_files` -- Use this configuration when backing up or restoring the files in the `opt` directory on the lifecycle manager.
- `HLM_Appliance_root_files` -- Use this configuration when backing up or restoring the files in the `root` directory on the lifecycle manager.
- `VSC_Appliance_config_files` -- Use this configuration when backing up or restoring the VSC system files.
- `VSD_Appliance_DB` -- Use this configuration when backing up or restoring the VSD database.
- `WR_Appliance_system_files` -- Use this configuration when backing up or restoring the KVM-region system files.

Restoring the lifecycle manager

You can use Attis to restore an HP Helion OpenStack Carrier Grade lifecycle manager.

To restore the lifecycle manager from a previous backup.:

1. Log in to lifecycle manager host as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Execute the following command to start the restore:

```
attis restore --config-id <Config_ID_of_ HLM_Appliance_Data_Restore> --
backup-id BACKUP_ID
```

Where:

- `CONFIG_ID` authenticates using the ID configuration file.
- `BACKUP_ID` is the ID of the backup from which you want to perform the restore. Use the `attis backuplog` command to get the back up ID for the job.

Restoring the Cloud Controller Database

You can use Attis to restore the three node MySQL cluster (Percona XtraDB Cluster) that runs in cloud controller nodes.

To restore the cloud controller database from a previous backup.:

1. Log into the cloud controller as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Perform one of the following:

   for NFS storage

```
attis restore --config-path /etc/attis/config_template/
cloudcontrollerappliancedbrestore_NFS.json
```

   for SCP storage

```
attis restore --config-path /etc/attis/config_template/
cloudcontrollerappliancedbrestore_scp.json
```

4. After restore job is complete, ssh to the compute proxy nodes from HLM, and restart nova-compute service:

```
service nova-compute restart
```

Restoring the KVM region system files

You can use Attis to restore the KVM region system files from a previous backup..

1. Log into the active KVM region controller as the `cghelion` user.
2. Change to the root user:

```
sudo -i
```

3. Execute the following command to perform the back up.

```
attis restore --config-id <Config_ID_of_WR_Appliance_system_files_Restore>
 --backup-id BACKUP_ID
```

Restoring the Baremetal Controller database and files

You can use Attis to restore the baremetal controllers in a Sacaramento deployment from a previous backup.

1. Log into the active baremetal controller as the `cghelion` user.
2. Change to the Attis user:

```
sudo su attis
```

3. Execute the following command:

```
attis restore --config-id <Config_ID_of_BM_Controller_Data_Restore> --
backup-id BACKUP_ID
```

After remove comment, change <dash> to <dash><dash>

HP Helion OpenStack® Carrier Grade 2.1 Beta: Backup and Restore CLI

HP Helion OpenStack Carrier Grade includes a backup and restore application called Attis which you can use to backup and restore essential system files and components of the non-KVM cloud. Attis is automatically installed on each of the controller nodes in the non-KVM region. Attis uses a command line interface.

The following document describes the full Attis CLI for backing up and restoring. You can also use the built-in Attis help system by entering `attis help` before any command when working with the CLI. For example:

```
attis help storage
```

Attis Administrator Responsibilities for Protecting Credentials

Attis performs encrypted backup and restore of system data. The key for encryption and decryption is stored in the Attis configuration file on each controller node in `/root/crypt_key`. If this key is lost, your backups can not be restored. Consider storing the backup encryption key separately from your cloud infrastructure, in addition to the copy stored on each controller node.

Be aware that keys and passwords for other OpenStack services are stored in configuration files on cloud infrastructure nodes, protected by filesystem controls. Protect servers from unauthorized access and protect against exposure of credentials in configuration files. Attis backups contain copies of these credentials as well, protected using backup encryption, but exposure of the Attis backup key could result in unauthorized exposure of credentials stored in backups.

Synopsis

```
attis [command] --version -v --log-file [LOG_FILE] -q -h --debug
```

Optional arguments

- `--version` Shows the Attis version number and exits.
- `-v, --verbose` Increases verbosity of output. Can be repeated.
- `--log-file LOG_FILE` Specifies a file to log output. Enter a path and file name for the log file.
- `-q, --quiet` Suppresses output except warnings and errors.
- `-h, --help` Shows help message and exits.
- `--debug` Shows tracebacks on errors.

Commands

- `backup`. Triggers the backup service.
- `backuplog`. Shows backup logs.
- `complete`. Prints bash completion command
- `config`. Shows stored configuration for Attis service.
- `help`. Shows detailed help for another command.
- `job`. Shows previous Attis backup/restore jobs.
- `queue`. Shows dispatcher queues.
- `restore`. Triggers the Attis restore service.
- `storage`. Shows storage configuration for the Attis service.
- `task`. Shows previous Attis backup/restore tasks.

Important commands

Back up

The following command triggers the backup service. Use `attis help backup` for more information.

```
attis backup [-h] [--config-id CONFIG_ID] [--config-path CONFIG_PATH]

        [--os-tenant-name TENANT_NAME] [--os-username USERNAME]

        [--os-password PASSWORD] [--os-auth-url AUTH_URL]
                        [--backup-type BACKUP_TYPE]
```

Arguments:

- `--config-id CONFIG_ID` Backup using configuration with id. Refer to attis config.
- `--config-path CONFIG_PATH` Backup using configuration from path. Default config location: `/etc/attis/config_template`.
- `--os-tenant-name TENANT_NAME` Specifies the project (tenant) name of the user used to execute the back up.
- `--os-username USERNAME` Specifies the user name to execute the back up
- `--os-password PASSWORD` Specifies the password of the user used to execute the back up
- `--os-auth-url AUTH_URL` Specifies the Keystone authentication URL.
- `--backup-type BACKUP_TYPE` Backup type is full or incremental. Default is full backup.

Restore

The following command triggers a restore. Use `attis help restore` for more information.

```
attis restore [-h] [--config-id CONFIG_ID] [--config-path CONFIG_PATH]

        [--backup-id BACKUP_ID] [--os-tenant-name TENANT_NAME]

        [--os-username USERNAME] [--os-password PASSWORD]
      [--os-auth-url AUTH_URL]
```

Arguments

- `--config-id CONFIG_ID`. Restores using configuration with id. Refer to attis config
- `--config-path CONFIG_PATH`. Restores using configuration from path. Example config location: `/opt/stack/attis-api/etc/attis/config_template/cloudcontrollerappliancedbrestore_scp.json`
- `--backup-id BACKUP_ID`. Specifies the ID of the backup to use with the restore.
- `--os-tenant-name TENANT_NAME`. Specifies the project (tenant) name of the user used to execute the restore.
- `--os-username USERNAME`. Specifies the user name to execute the restore
- `--os-password PASSWORD`. Specifies the password of the user used to execute the restore
- `--os-auth-url AUTH_URL`. Specifies the Keystone authentication URL.

Storage

The following command shows stored storage configuration for the Attis service. Use `attis help storage` for more information.

Synopsis

```
attis storage --update '{"parameter":"new value", "parameter":"new value"}'
 --id <storage_id from the table>
```

Arguments

- `--id ID` Shows storage with specified id, including its parameters and values
- `--type TYPE` Shows storage with specified type

- `--update UPDATE` Updates storage parameters with new values. Arguments should be dictionary format, for example: `'{"storage_path": "/tmp/mybackup"}'`
- `--use USE` Uses the specified storage type. The default is `SCP`.
- `--os-tenant-name TENANT_NAME`. Specifies the project (tenant) name of the user used to execute the storage command.
- `--os-username USERNAME`. Specifies the user name to execute the storage command.
- `--os-password PASSWORD`. Specifies the password of the user used to execute the storage command.
- `--os-auth-url AUTH_URL`. Specifies the Keystone authentication URL.

Examples commands

The following table lists some typical Attis CLI commands.

Command	Action
attis job	shows a list of jobs
attis job --id JOB_ID	shows detail job of id JOB_ID, including sub-tasks
attis job --name JOB_NAME	shows a list of jobs with name JOB_NAME
attis job --last N	shows a list of jobs only in the last N days
attis job --latest	shows the latest job
attis config	shows a list of configs
attis config --id CONFIG_ID	shows detail configs of id CONFIG_ID, including config parameters
attis config --type TYPE	shows a list of configs with type TYPE (backup/restore)
attis config --id CONFIG_ID --update '{"timeout": 1200}'	updates config from the specified config with new values. arguments should be dictionary format
attis config --id CONFIG_ID --update-parameter '{"Percona_XtraDB_Backup_dbuser": "myuser", "Percona_XtraDB_Backup_dbpassword": "mypassword"}'	updates config parameters from the specified config with new values. arguments should be dictionary format
attis backuplog	shows a list of backup logs
attis backuplog --id BACKUP_LOG_ID	shows a list of backup logs with id BACKUP_LOG_ID
attis backuplog --name BACKUP_LOG_NAME	shows a list of backup logs with name BACKUP_LOG_NAME
attis backuplog --last N	shows a list of backup logs in the last N days
attis backuplog --latest	shows the latest backup log
attis backup --config-id CONFIG_ID	executes backup job with parameters fetched from config id CONFIG_ID
attis backup --config-id CONFIG_ID --backup_type BACKUP_TYPE	executes an incremental or full (default) BACKUP_TYPE, with parameters fetched from confid CONFIG_ID
attis restore --config-id CONFIG_ID --backup-id BACKUP_ID	executes restore job using config id CONF_ID and BACKUP_ID, which is backup_id from "attis backuplog"
attis storage	shows a list of available storage

attis storage --id STORAGE_ID	shows the detail of the storage configuration with the specified STORAGE_ID, including parameters
attis storage --type STORAGE_TYPE	shows the storage configuration with the specified STORAGE_TYPE
attis storage --id STORAGE_ID --update '{"storage_path":""}'	updates parameters from the specified storage with new values (arguments should be dictionary format)
attis storage --use STORAGE_TYPE	tells Attis to use the specified STORAGE_TYPE for storing backups

HP Helion OpenStack® Carrier Grade 2.1 Beta: Restart MySQL and RabbitMQ

A default deployment of HP Helion OpenStack Carrier Grade includes a MySQL database instance and RabbitMQ instance on each controller, configured as a MySQL cluster.

In HP Helion OpenStack Carrier Grade in a Reduced Control Plane deployment, the controllers are virtual machines on a single server. In the event that server goes down, you will need to manually restart the MySQL servers after the server is restarted. You might also need to restart RabbitMQ.

Restarting MySQL

If the server hosting the controller VMs goes down, the MySQL server on each controller will need to be manually restarted. HP Helion OpenStack Carrier Grade includes an Ansible playbook that will:

- shut down all MySQL servers
- perform a `mysql stop` command to clear potential errors
- query the status of the MySQL cluster to determine the last MySQL server to fail
- bootstrap that MySQL server
- restart the other MySQL servers

1. Log into the lifecycle manager.

   ```
   ssh <HLM_VM_IP>
   ```

   where: HLM_VM_IP is the CLM IP of the lifecycle manager. Locate the IP address for the lifecycle manager in the `/root/infra-ansible-playbooks/group_vars/all` file under `hlm_clmstaticip` field.
2. Verify that the `ansible/roles/FND-MDB/tasks/restart_cluster.yml` and `ansible/restart-MySQL-CCP-T1.yml` files exist.

   If the `ansible/roles/FND-MDB/tasks/restart_cluster.yml` file does not exist, edit the `ansible/roles/FND-MDB/tasks/deploy.yml` to comment out all the `include` statements and add in restart_cluster.
3. Log into the controller

   ```
   ssh cghelion@<IP of Controller>
   ```
4. Execute the following command to determine the status of the MySQL cluster:

   ```
   "sudo mysql keystone -e \"show status where Variable_name in
    ('wsrep_cluster_size','wsrep_cluster_status','wsrep_incoming_addresses');"\"
   ```

   This command will return an error if MySQL cluster is down.
5. If the cluster is down, execute the following command to restart the cluster:

   ```
   ansible-playbook -i hosts restart-MySQL-CCP-T1.yml
   ```

   If the file does not exist, edit the `ansible/roles/FND-MDB/tasks/deploy.yml` to comment out all `include` statements and add in `restart_cluster`.

6. Execute the following command to determine the status of the MySQL cluster:

```
ssh cghelion@<IP of Controller> "sudo mysql
 keystone -e \"show status where Variable_name in
 ('wsrep_cluster_size','wsrep_cluster_status','wsrep_incoming_addresses');"\"
```

This command should return a cluster status where all VMs are listed.

Restarting RabbitMQ

If the server hosting the controller VMs goes down, the RabbitMQ message broker service might need to be manually restarted.

1. Log into the lifecycle manager.

```
ssh <HLM_VM_IP>
```

where: HLM_VM_IP is the CLM IP of the lifecycle manager. Locate the IP address for the lifecycle manager in the `/root/infra-ansible-playbooks/group_vars/all` file under `hlm_clmstaticip` field.

2. Verify that the `ansible/roles/FND-RMQ/tasks/restart_cluster.yml` and `ansible/restart-RMQ-CCP-T1.yml` files exist.

If the `ansible/roles/FND-RMQ/tasks/restart_cluster.yml` file does not exist, edit the `ansible/roles/FND-RMQ/tasks/deploy.yml` to comment out all the `include` statements and add in restart_cluster.

3. Log into the controller

```
ssh cghelion@<IP of Controller>
```

4. Execute the following command to determine the status of the RabbitMQ cluster:

```
"sudo rabbitmqctl cluster_status"
```

This command will return an error if RabbitMQ cluster is down.

5. If the cluster is down, execute the following command to restart the cluster:

```
ansible-playbook -i hosts restart-RMQ-CCP-T1.yml
```

6. Execute the following command to determine the status of the RabbitMQ cluster:

```
"sudo rabbitmqctl cluster_status"
```

This command should return a cluster status where all VMs are listed.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Patching and Update Processes

This document provides a general description of the HP Helion OpenStack Carrier Grade patching and update processes.

Update Existing HLM:

If you have an existing HLM and you want to upgrade it to a newer CGHOS build, you can do so without tearing it apart.

This will help you to maintain all your existing cloud definitions and generated configuration remain intact while the Debian Repository and HLM code has been updated to the latest version.

Taking Back-Up and Preparing for Upgrade

1.
```
Take a backup of desired_state under your current cloud folder ==> If you
 have any custom machine_architecture.json => ensure you have a backup for
 this file ==> /opt/share/hlm/1/site/machine_architecture.json
```

   a. cd /var/hlm/clouds/<cloudname>
   b. cp -r desired_state desired_state-working-beta
2. Take a backup of log files mv /var/log/hlm/<cloudname> /var/log/hlm/<cloudname>-backup
3. Do not rename the cloud
4. Ensure accelerate process is not running under "root" user on any of the cloud nodes. If you do find such process - kill it
5. Reconcile any differences between Json files of the new build and the one that you have under cloud folder. Since you will be using the same jsons of the under your current cloud folder, you must ensure that if there were any new additions/subtractions into the new build's jsons

Confirm health of existing cloud

1. MySQL
   a. service MySQL status (should be active)
   b. mysql
   c. show status like 'wsrep%';
   d. corfirm above command returned a wsrep_cluster_size that is appropriate for the build
2. RabbitMQ
   a. service rabbitmq-server status (should be active)
   b. rabbitmqctl status
   c. rabbitmqctl cluster_status
      a. should list all nodes in cluster under 'running_nodes'
   d. rabbitctl list_users
      a. should list all users
3. Apache
   a. service apache2 status (should be active)
4. keystone
   a. source stackrc
   b. keystone user-list (should return list of users)
5. Take a general inventory of all your existing networks, instances, subnets etc to compare your setup post upgrade.

Gotchas!

1. If you get hung while running deploy, Kill the ansible process by pressing "ctrl c" and then try hlm deploy with rerun option
2. On bonded nic setups, sometimes there are network lags and you might get timeouts or failures or ssh disconnect issue. Running hlm deploy with rerun usually solves the issue.
3. Ensure the machine_architecture.json that you backed up is copied again under /opt/share/hlm/1/site/

Upgrade Existing HLM with New Build

1. Remove old bits from ~/cg/ on lifecycle manager host
2. Copy the new build bits cg-hos-misc.tar.gz cg-hos-src.tar.gz under ~/cg/ on lifecycle manager host
3. Do not update your ~/infra-ansible-playbooks unless you know for sure the new bits have some code changes to infra-ansible-playbooks. Usually the change list is generated with each build.
4. Go to your ~/infra-ansible-playbooks folder. If you updated the infra playbooks too with new code, then update your group_vars/all file accordingly.
5. Run ansible-playbook -i hosts update_hlm_onBM.yml

6. `The above step has updated your HLM debian repo with latest deb and also has updated your HLM and Ansible code.`

Upgrade Cloud Configuration with Existing Cloud Definitions (No JSON Changes in the cloud definition for adding tiers or nodes. But adding variables is fine.)

Once you have updated your HLM to be on the latest version of the CGHOS Build, you still have your existing cloud configurations (sitting under desired_state folder)

that has not been updated to the newercode.

You will have to perform some steps in order to get your existing cloud definitions updated to the latest.

If you are not interested in your existing cloud definition and updating the existing cloud itself from the current HLM, you can of course ignore these steps and create a new cloud altogether.

Update Cloud Configuration with Existing Cloud Definition (No JSON file Changes)

1. `Since you have a deployed cloud, you already have the cloud definition and configuration sitting under /var/hlm/clouds/<yourcloud>`
2. `In this case, we are NOT modifying any Cloud Definition JSON files. We are only updating the cloud configuration related to ansible roles and varibles.`
3. `Take a backup of your old configurations for "just in case" scenarios.`
4. `Run copy command =>  cp /var/hlm/clouds/<yourcloud>/desired_state /var/hlm/clouds/<yourcloud>/desired_state_build<oldbuild>`
5. `Run => cd ~`
6. `Run => hlm generate -c <yourcloud>`
7. `Run => hlm deploy -c <yourcloud>`
8. `The above will update your whole cloud to the new bits`

Update Cloud Configuration with NEW Cloud Definitions (JSON Changes for adding tiers) [NOT FOR GA]

Since you have a deployed cloud, you already have the cloud definition and configuration sitting under /var/hlm/clouds/<yourcloud>

Following things cannot be updated in JSON files:

- No changes pertaining to networking, new networks cannot be added or old networks cannot be removed
- No changes pertaining to removal of existing tiers
- No changes pertaining to removal of existing roles on tiers

In this case, we can modify the Cloud Definition JSON files but are limited to modify only following things:

- Add new roles to existing Tier (See an expandable sections below for steps)
- Add new Ansible variables
- Add a new Tier

HP Helion OpenStack® Carrier Grade 2.1 Beta: API and SDK Reference

This document describes *the APIs* and *the Software Development Kit (SDK)* available for HP Helion OpenStack Carrier Grade.

APIs

HP Helion OpenStack Carrier Grade is built on OpenStack technologies.

The OpenStack REST API Documentation is open-source; both the published formats (PDF and HTML pages) as well as the docbook/wadl source documents.

The open-source OpenStack REST API Documentation is currently NOT versioned. There is only a master/current version of the OpenStack REST API Documentation containing updates from 'all' versions of OpenStack.

Non-KVM Region API

For the API reference for the non-KVM region, see the *OpenStack API Complete Reference*.

For the specific OpenStack services supported by HP Helion OpenStack Carrier Grade, see *Services Overview*.

KVM Region API

For the API refernece for the KVM region, see *HP Helion OpenStack Carrier Grade 2.1 Beta: REST API Guide*. This document contains HP Helion OpenStack Carrier Grade extensions to the OpenStack Compute API for use with the servers in the KVM region.

HP Helion OpenStack Carrier Grade supports the following external REST APIs through its OAM floating IP address:

- OpenStack REST APIs
  - Object Storage API
  - Block Storage API (with HP Helion OpenStack Carrier Grade extensions)
  - Compute API (with HP Helion OpenStack Carrier Grade extensions)
  - Identity API
  - Image Service API
  - Networking API (with HP Helion OpenStack Carrier Grade extensions)
  - Orchestration API
  - Telemetry API (with HP Helion OpenStack Carrier Grade extensions)
- HP Helion OpenStack Carrier Grade REST APIs
  - SysInv API
  - Patching API

Note:

HP Helion OpenStack Carrier Grade extensions use the OpenStack Extension Mechanism to ensure compatibility with existing clients.

HTTP or HTTPS protocol can be supported for these external REST APIs.

Software Development Kit (SDK)

An SDK can be used by guest applications to interact programmatically with HP Helion OpenStack Carrier Grade.

HP Helion OpenStack Carrier Grade Software Development Kit (SDK)

The HP Helion OpenStack Carrier Grade Software Development Kit (SDK) provides drivers, daemons, API libraries, and configuration files that you can include in a guest image to leverage the extended capabilities of HP Helion OpenStack Carrier Grade. Available components include:

- Accelerated Kernel Network Drivers—Drivers for improved performance of kernel-based networking VNFs
- Accelerated DPDK Network Drivers—Drivers for high-performance DPDK-based networking VNFs
- VM Resource Scaling—A service for scaling the capacity of a guest server on demand
- Guest Heartbeat—A service for health monitoring of guest applications
- Server Group Messaging—A service for low-bandwidth peer messaging between servers in the same group
- SNMP MIB—Resources for system alarms management
- Sample Heat Orchestration Templates—Resources for deploying and managing stacks of applications or application services
- OpenStack REST API Documentation—Documentation for HP Helion OpenStack Carrier Grade REST APIs and HP Helion OpenStack Carrier Grade extensions to OpenStack REST APIs
- Custom Branding—Resources for customizing the Horizon GUI

See the *Software Development Kit documentation*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Lifecycle Manager CLI

The Helion lifecycle management tool contains a command line interface (CLI) that runs as a service on the HLM host. To list available commands supported by that service, type `hlm` on the terminal window on HLM host.

You can get more help about a command using the `--help` parameter:

```
hlm <command name> --help
```

Note: All logs will be generated as `/var/log/hlm/<cloud name>/<command name>`.log

This topic lists the available commands, describes the options, and how to use the commands to carry out particular functionality:

Note: Please refer to the description in code block corresponding to each command.

hlm define

Defines a cloud.

Use this command to deploy a cloud defined by the specified template. This command lists all the available deployment templates. The command creates a `<cloudname>` folder in the `/var/hlm/clouds directory`.

Synopsis

```
hlm define <cloud name> -t <topology name>
hlm define -l
```

Arguments

`<cloud name>` -- Name the cloud `--topology, -t` -- Specify the template to use.

Optional Arguments

`--list-topologies, -l` -- List cloud topologies.

Example:

```
hlm define mycloud -t memphis
```

hlm-deploy

Deploys all cloud services on respective cloud nodes.

This command is for a first-time commit of the cloud configuration. Attempting to deploy an already deployed cloud will return an error.

Synopsis

```
hlm deploy -c <cloud name> [-v <verbose>] [-r <rerun>] [-t <tags|roles|
tiers>]
```

Arguments

`--cloud, -c` -- Specify the name of the cloud to act upon.

`--verbose, -v` -- Produce verbose output.

`--rerun, -r` -- Rerun from a failed task.

`--tags, -t` -- Run only specified tags separated by a space and included in double quotes.

Examples

Deploy the cloud first time

```
hlm deploy -c mycloud
```

Rerun from previously failed role

```
hlm deploy -c mycloud -r
```

Deploy specific services

```
hlm deploy -c mycloud -t "FND-MDB KEY-API"
```

hlm-display

Displays information about the cloud. If no arguments but the cloud name are specified, the topology of the current state is displayed.

Synopsis

```
hlm display -c <cloud name> [] [--topology | --explain | --service-map | --
network-map | --node-map]
```

Arguments

`--cloud, -c` Specify the name of the cloud to display.

`--topology` -- Display the cloud topology. This is the default.

`--explain` -- Display a text description of the cloud.

`--service-map` -- Display the service map file for the cloud.

`--network-map` -- Display the network map file for the cloud.

`--node-map` -- Display the list of nodes that have been allocated in the cloud.

Examples

Display details about how networks will be provisioned in the cloud:

```
hlm display -c mycloud --network-ma
```

hlm-dump

Gathers all log files generated as part of the lifecycle process and compresses them in a single TAR file in the current location or on a location that is specified, using the same name as the cloud: `<cloudname.tar>`.

Synopsis

```
hlm dump -c <cloud name> [-p <dump location>]
```

Arguments

`--cloud, -c` -- Specify the name of the cloud to act upon.

`--path, -p` -- Specify the path to create tar file.

Examples

Create a log dump file in the current directory:

```
hlm dump -c mycloud
```

Create a log dump file in a different directory :

```
hlm dump -c mycloud -p /home/cghelion
```

hlm-generate

Execute the configuration processor that generates cloud configuration files needed for cloud deployment. The HP Helion OpenStack Carrier Grade configuration processor is a script, called `hcfgproc`, that is incorporated into the installation environment. This command generates the necessary configuration for the cloud.

Synopsis

```
hlm generate -c <cloud name> [-C <cloud | service | component>] [-p <control
 plane>] [-v]
```

Arguments

`--cloud, -c` -- Specify the name of the cloud to act upon.

`--change-credential, -C` -- Change the credentials for the entire cloud, all components for a service, or a single component.

`--control-plane, -p` -- Limit the scope of credential change to components of a single control plane.

`--verbose, -v` -- Produce verbose output.

Example

```
hlm generate -c mycloud
```

hlm-list

Lists the clouds that are currently defined.

Synopsis

```
hlm list
```

Examples

```
hlm list
```

hlm-netinit

Configures network interfaces on cloud nodes.

Network interface files along with NIC bonding or PCI enumeration related files (generated by the configuration processor) are copied to cloud nodes. After the interfaces are configured, the command restarts the network service on cloud nodes to reflect the changes.

Synopsis

```
hlm netinit -c <cloud name> [-v]
```

Arguments

`--cloud, -c` -- Specify the name of the cloud to act upon.

`--verbose, -v` -- Produce verbose output.

Example

```
hlm netinit -c mycloud
```

hlm plugin

Deploys a plugin on top of an existing cloud deployment.

Examples

Deploy the Infoblox plugin

```
hlm plugin -c <cloudname> -n infoblox
```

Rollback a plugin that was already deployed

```
hlm plugin -c <cloudname> -n infoblox --rollback
```

hlm provision

Provision nodes to be used in a cloud.

Before executing the command, edit the `node-provision.json` file in the `<cloudname>` directory of the HLM VM for an existing cloud. This command provisions/installs the operation system on the servers specified in the `node-provision.json` file. See the *installation documentation* for your deployment.

Synopsis

```
hlm provision -c <cloud name> [-n <"node1 node2">] [-d <"node1 node2">] [-p]
```

Arguments

`--cloud, -c` -- Specify the name of the cloud to provision.

`--nodes, -n` -- Indicate that specified nodes will be provisioned to the specified cloud.

`--deprovision, -d` -- Indicate that specified nodes will be released from the specified cloud.

`--proxy, -p` -- Indicate that only proxy nodes will be provisioned to the specified cloud.

Optional Arguments

`--list-topologies, -l` -- List cloud topologies.

Examples:

Provsion all nodes:

```
hlm provision -c mycloud
```

Provision specific/new nodes specified in node-provision.json:

```
hlm provision -c mycloud -n "ccn4 ccn5"
```

Deprovision specific nodes:

```
hlm provision -c mycloud -d "ccn4 ccn5"
```

Provision only proxy nodes:

```
 hlm provision -c mycloud -p
```

hlm-start

Start a particular service or start all services. The command starts services on a particular tier or on all tiers.

Synopsis

```
hlm start -c <cloud name> [-v <verbose>] [-t <tags|roles|tiers>]
```

Arguments

`--cloud, -c` -- Specify the name of the cloud to act upon.

`--verbose, -v` -- Produce verbose output.

`--tags, -t` --Run only specified tags separated by a space and included in double quotes.

Examples

Start the Horizon service on all control planes:

```
hlm start -c mycloud -t "HZN-WEB"
```

Start all services on all control planes:

```
hlm start -c mycloud
```

hlm-stop

Stop a particular service or stop all services. The command stops services on a particular tier or on all tiers.

Synopsis

```
hlm stop -c <cloud name> [-v <verbose>] [-t <tags|roles|tiers>]
```

Arguments

`--cloud, -c` -- Specify the name of the cloud to act upon.

`--verbose, -v` -- Produce verbose output.

`--tags, -t` --Run only specified tags separated by a space and included in double quotes.

Examples

Stop the Horizon service on all control planes:

```
hlm start -c mycloud -t "HZN-WEB"
```

Stop all services on all control planes:

```
hlm start -c mycloud
```

HP Helion OpenStack Carrier Grade 2.1 Beta: Operations Guide

HP Helion OpenStack Carrier Grade is a high-performance, high-availability, cloud operating system that enables telecommunications operators to use Commercial-off-the-shelf (COTS) hardware to manage Virtualized Network Functions (VNF) within a carrier grade Network Function Virtualization (NFV) architecture.

HP Helion OpenStack Carrier Grade brings together the flexibility and scalability of the IT cloud, and the high-availability and performance demanded by the Telecommunications industry, into a unique carrier grade, industry-leading solution to deliver a price-performance ratio well above alternative solutions. HP Helion OpenStack Carrier Grade is aligned with the ETSI-NFV architecture.

Virtual machine operations

Use the Compute panel on the Project dashboard to:

- Create a new instance
- Terminate an instance
- Reboot an instance
- Rebuild an instance
- Suspend and resume an instance
- Pause and resume an instance
- Create an instance snapshot

Network Management

The Network panel contains commands to view a visual representation of your network and to enable you to work with your network.

- View your network
- Create or delete a network
- Enable or disable a network
- Create externally available networks
- Create shared networks
- Add or remove a subnet to/from a Network
- Create, Modify, or Delete a port on a Network
- Configure virual ports and virtual routers

Inventory Management

HP Helion OpenStack Carrier Grade provides complete inventory management of hosts in the OpenStack cloud, allowing the system administrator to install, configure, and maintain the individual servers. The inventory service gives the system administrator the following capabilities:

- Host management
  - discovery of new hosts in the cluster
  - installation of the appropriate load, controller, compute, or storage images
  - configuration of the management, OAM, infrastructure, and provider network interfaces on each host
  - creation and use of data interface and CPU profiles to simplify host configuration
  - configuration of the number of CPUs allocated to the Accelerated Virtual Switch (AVS) on each compute node
  - configuration of huge memory page allocations for VM use
- Administrative operations
  - lock/unlock
  - switch active controller host or service
  - reboot and reset host
  - power-on and power-off
  - software re-installation
- Status reporting
  - admin state
  - operational state
  - availability state
  - uptime
  - real-time command execution reports, such as booting and testing
- Host resources
  - volumes
  - flavors
  - images
  - processor, sockets, cores

  - memory
  - disk
  - network interfaces
  - additional hardware devices, such as cryptographic and compression devices

Improved Web Administration Interface

HP Helion OpenStack Carrier Grade web administration interface is an enhanced version of the Horizon web interface provided by OpenStack. The enhancements include:

- Automatic page refresh for immediate notification of status changes. This eliminates the need for manual reloading of web pages to access up-to-date information about the cloud
- Admin Overview page with charts and tables providing a high-level overview of cloud resources
  - avg/max/min compute vCPU usage
  - avg/max/min compute memory usage
  - avg/max/min compute disk usage
  - avg/max/min AVS CPU utilization
  - avg/max/min provider network port utilization
  - current host status (available, unavailable, locked, unlocked)
- Performance management resource usage web page
  - optimized performance management sample DB queries for improved usability
  - capability to filter on fields in the performance management sample's metadata
  - human-readable legends and chart labels using object names instead of long UUID text strings
  - performance management meters can be selected using their brief descriptions
  - meters for CPU, memory, and disk utilization

Alarms Generation and Reporting

- alarms on performance management thresholds and cloud-level services and equipment
- SNMPv2c support

HP Helion OpenStack Carrier Grade 2.1 Beta: Operations Guide

HP Helion OpenStack Carrier Grade is a high-performance, high-availability, cloud operating system that enables telecommunications operators to use Commercial-off-the-shelf (COTS) hardware to manage Virtualized Network Functions (VNF) within a carrier grade Network Function Virtualization (NFV) architecture.

HP Helion OpenStack Carrier Grade brings together the flexibility and scalability of the IT cloud, and the high-availability and performance demanded by the Telecommunications industry, into a unique carrier grade, industry-leading solution to deliver a price-performance ratio well above alternative solutions. HP Helion OpenStack Carrier Grade is aligned with the ETSI-NFV architecture.

Virtual machine operations

Use the Compute panel on the Project dashboard to:

- Create a new instance
- Terminate an instance
- Reboot an instance
- Rebuild an instance
- Suspend and resume an instance
- Pause and resume an instance
- Create an instance snapshot

Network Management

The Network panel contains commands to view a visual representation of your network and to enable you to work with your network.

- View your network
- Create or delete a network
- Enable or disable a network
- Create externally available networks
- Create shared networks
- Add or remove a subnet to/from a Network
- Create, Modify, or Delete a port on a Network
- Configure virual ports and virtual routers

Inventory Management

HP Helion OpenStack Carrier Grade provides complete inventory management of hosts in the OpenStack cloud, allowing the system administrator to install, configure, and maintain the individual servers. The inventory service gives the system administrator the following capabilities:

- Host management
  - discovery of new hosts in the cluster
  - installation of the appropriate load, controller, compute, or storage images
  - configuration of the management, OAM, infrastructure, and provider network interfaces on each host
  - creation and use of data interface and CPU profiles to simplify host configuration
  - configuration of the number of CPUs allocated to the Accelerated Virtual Switch (AVS) on each compute node
  - configuration of huge memory page allocations for VM use
- Administrative operations
  - lock/unlock
  - switch active controller host or service
  - reboot and reset host
  - power-on and power-off
  - software re-installation
- Status reporting
  - admin state
  - operational state
  - availability state
  - uptime
  - real-time command execution reports, such as booting and testing
- Host resources
  - volumes
  - flavors
  - images
  - processor, sockets, cores
  - memory
  - disk
  - network interfaces
  - additional hardware devices, such as cryptographic and compression devices

Improved Web Administration Interface

HP Helion OpenStack Carrier Grade web administration interface is an enhanced version of the Horizon web interface provided by OpenStack. The enhancements include:

- Automatic page refresh for immediate notification of status changes. This eliminates the need for manual reloading of web pages to access up-to-date information about the cloud
- Admin Overview page with charts and tables providing a high-level overview of cloud resources

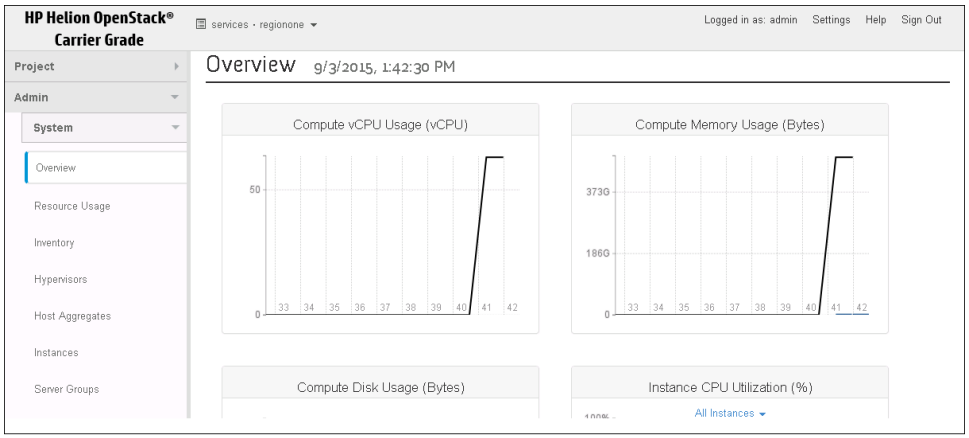
  - avg/max/min compute vCPU usage
  - avg/max/min compute memory usage
  - avg/max/min compute disk usage
  - avg/max/min AVS CPU utilization
  - avg/max/min provider network port utilization
  - current host status (available, unavailable, locked, unlocked)
- Performance management resource usage web page
  - optimized performance management sample DB queries for improved usability
  - capability to filter on fields in the performance management sample's metadata
  - human-readable legends and chart labels using object names instead of long UUID text strings
  - performance management meters can be selected using their brief descriptions
  - meters for CPU, memory, and disk utilization

Alarms Generation and Reporting

- alarms on performance management thresholds and cloud-level services and equipment
- SNMPv2c support

Dashboard Controls

The HP Helion OpenStack Carrier Grade web administration interface provides a dashboard for managing all aspects of the system.



The dashboard consists of a left-hand pane containing menus, and a right-hand pane containing information for the currently selected menu item. It also shows the current user, the current tenant (project), the system ID, and the system time, and includes options for setting user preferences, viewing help, and signing out.

The menu pane contains tabs for different menus. The selection depends on the current user.

- The **Project** (tenant) tab is available for users assigned to one or more tenants as a **member**.
- The **Admin** tab is available for users assigned as **admin** for the HP Helion OpenStack Carrier Grade.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Logging into the Helion Dashboard

The IP address for the Horizon interface is stored in the CAN VIP value in the `/root/stackrc` file on any controller node. The CAN IP contains port `5000`. The CAN VIP can also be got from HLM VM in the `~/<cloud name>/clouds/<cloudname>/001/stage/net/hosts.hf` file. Search for `VIP`.

Note: You need to import the `ca.crt` certificate from the `/root/<cloudname>` on the HLM VM. You can use any file transfer program to move the certificate file from the HLM VM to the local system.

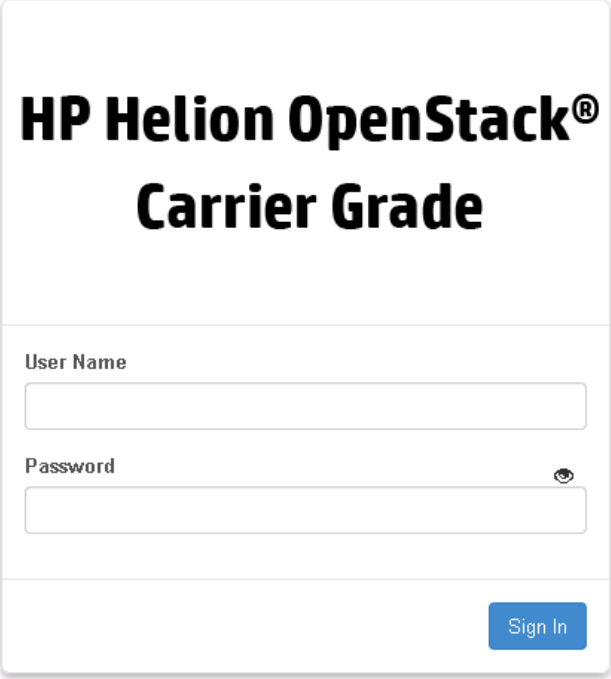
1. Ask the cloud operator for the host name or public IP address where the dashboard is located, your user name, and your password.
2. Open a web browser that has both JavaScript and cookies enabled.

3. In the address bar, enter the host name or IP address for the dashboard:

```
https://<CAN vip>/
```

4. On the **Log In** page, enter your user name and password and then click **Sign In**.

   By default, the user name is `admin`. You can find the installation password for `admin` in the `/root/stackrc` file from any of the controller node. If this is the first time you log in with that user name, make sure you *change the password*.



5. If you are a non-admin user, you will only be able to select a project from the list at the top of the screen.

   Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: How to use the Helion Dashboard

The HP Helion OpenStack Commercial dashboards are browser-based user interfaces that allow you to interact with the HP Helion OpenStack Carrier Grade.

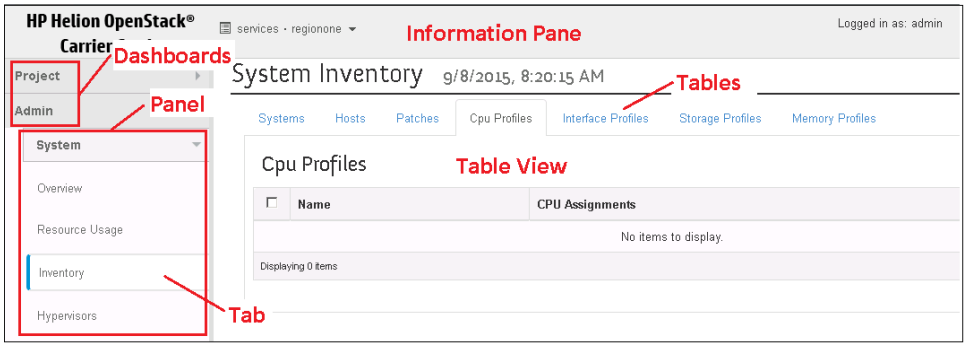
The interface, based on OpenStack Horizon, is grouped into tabs, including *Project*, *Admin* and *Identity*. The tabs expand and contract to show available commands grouped into **panels**.

Across the top are menus to switch between projects and menus where you can access user settings.

How you interact with your network environment depends upon your user type, either an administrative user or a non-administrative user (user). In general, a non-admin user can make changes to projects to which that user is associated. Admin users can make changes throughout the domain.

To access the dashboard, *enter the dashboard URL in a supported browser and log in*.

The layout of a typical Helion page contains dashboards, panels, tabs, and tables, as shown in the following diagram:



At the bottom of this page, you can see some of the services you can manage right from the dashboard.

Project tab

Use the **Project** tab to implement and build out your cloud. This dashboard contains tools to create virtual server instances, create and configure your network, configure access tools (such as key pairs and security groups) and cloud resource templates (stacks).

Menu item	Description
System Panel	
Instances	Controls for managing instances associated with the tenant, including controls for creating snapshots.
Server Groups	Controls for managing server groups associated with the tenant. KVM region only.
Volumes	Controls for managing virtual disk volumes associated with the tenant's instances.
Images & Snapshots	Controls for managing images, and information about available snapshots created from instances.
Access & Security	Controls for network protocol and port security, SSH-based access to virtual machines, API access to services, and floating IP address allocations.
Network Panel	
Topology	Configuration charts depicting system networks, instances, and network connections between instances.
Networks	Controls for managing networks for the current tenant, and viewing QoS (Quality of Service) policies or weightings for tenants of which the user is a member.
Routers	Controls for managing virtual routers. Tenant members can create and delete virtual routers, view router details and delete interfaces, and clear gateways.
Object Store	
Containers	Controls for mamaging storage containers. A container is a storage compartment for your data and provides a way for you to organize your data.
Orchestration Panel	
Stacks	Details for existing services (stacks), and controls for creating new services (launching stacks). Service details

Menu item	Description
	include topologies, resource allocations, and event histories.

Admin tab

Use the **Admin** tab to view, allocate, and manage all resources within the cloud.

The Admin tab allows you to manage instances, define flavors, create and configure images, manage networks, view system resources, manage projects, and manage users.

Menu item	Description
System Panel	
Overview	Performance charts for system health monitoring, including hosts status, provider-network port utilization, and compute node processing, memory, and disk usage.
Resource Usage	Tools for performing Ceilometer database queries using real-time or collected data, to support detailed performance analysis. *KVM servers only*
Inventory	Controls for managing systems, hosts, and standardized CPU, port, or storage profiles that can be applied to hosts. *KVM servers only*
Host Aggregates	Charts for monitoring hypervisor resource usage on compute nodes. *Non-KVM servers only*
Hypervisors	Charts for monitoring hypervisor resource usage on compute nodes.
Instances	Controls for managing virtual-machine instances.
Server Groups	Controls for managing server groups across all tenants. Server groups are collections of instances sharing common attributes. *KVM servers only*
Volumes	Controls for managing virtual disk volumes available for use with instances. The virtual volumes are implemented using storage volumes defined for the storage nodes in the system.
Flavors	Controls for managing standardized processor, disk, and memory complements (flavors) that can be applied to virtual machines.
Images	Controls for managing disk images used to initialize and configure virtual machines.
Networks	Controls for managing tenant networks, provider networks, and QoS (Quality of Service) policies or tenant weightings.
Routers	Controls for managing virtual routers. Administrators can list the virtual routers created for tenants, view router and interface details, and delete routers.
Defaults	Controls for viewing and setting the default quota values for new tenants.

Menu item	Description
Fault Management	System alarms. *KVM servers only*
System Configuration	System configuration updates. *KVM servers only*
System Info	Status information for services and network agent processes, availability zones, and host aggregates.

Identity tab

Use the **Identity** tab to create and delete users, change user passwords, assign users to projects, and other tasks.

Menu item	Description
Projects	Controls for managing tenants.
Users	Controls for managing user accounts.

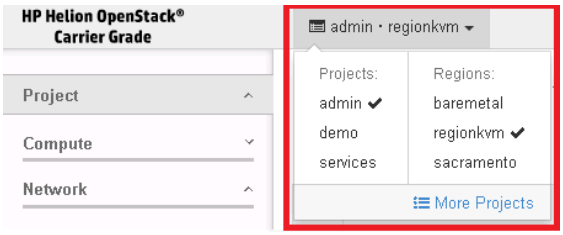
HP Helion OpenStack® Carrier Grade 2.1 Beta: Selecting a Region and Project

When working in HP Helion OpenStack Carrier Grade, you can work in one of the folloiwng regions:

- the non-KVM region, based on the *deployment template used during the installation*
- the KVM region, also called `regionkvm`

  Note: In addition, for Sacramento deployments only, the baremetal region

In the Horizon interface, you can use a selector to move between the two regions.



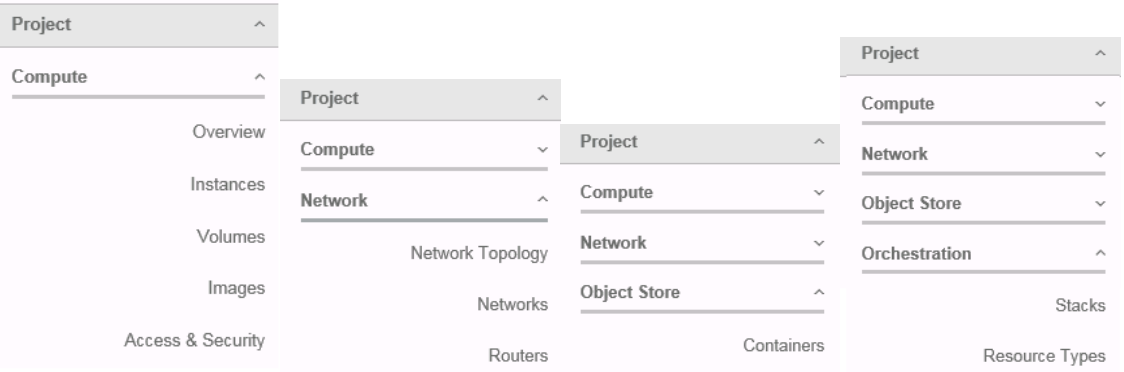
For more information on the regions, see the *Technical Overview*.

Within each region, there are one or more project (tenants). You can use the selector to move between projects.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Using the Project Dashboard

The **Project** menu contains selections for managing the currently selected tenant (project).

The **Current Project** is identified at the top of the **Information Pane**. Users with membership in more than one project can *select a different project using a drop-down list*.



The dashboard contains the following panels and tabs.

Compute

Tab	Description	Reference
Overview	Limit Summary and Uage Summary	*Viewing System Status*
Instances	Controls for managing instances associated with the tenant, including controls for creating snapshots.	*Managing Instances*
Server Groups		KVM Region only
Volumes	Controls for managing virtual disk volumes associated with the tenant's instances.	*Managing Volumes*
Images	Controls for managing images, and information about available snapshots created from instances.	*Managing Images*
Access & Security	Controls for network protocol and port security, SSH-based access to virtual machines, API access to services, and floating IP address allocations.	

Network

Tab	Description	Reference
Network Topology	Configuration charts depicting system networks, instances, and network connections between instances.	
Networks	Controls for managing networks for the current tenant, and viewing QoS (Quality of Service) policies or weightings for tenants of which the user is a member.	
Routers	Controls for managing virtual routers. Tenant members can create and delete virtual routers, view router details and delete interfaces, and clear gateways.	

Object Store

Tab	Description	Reference
Containers		

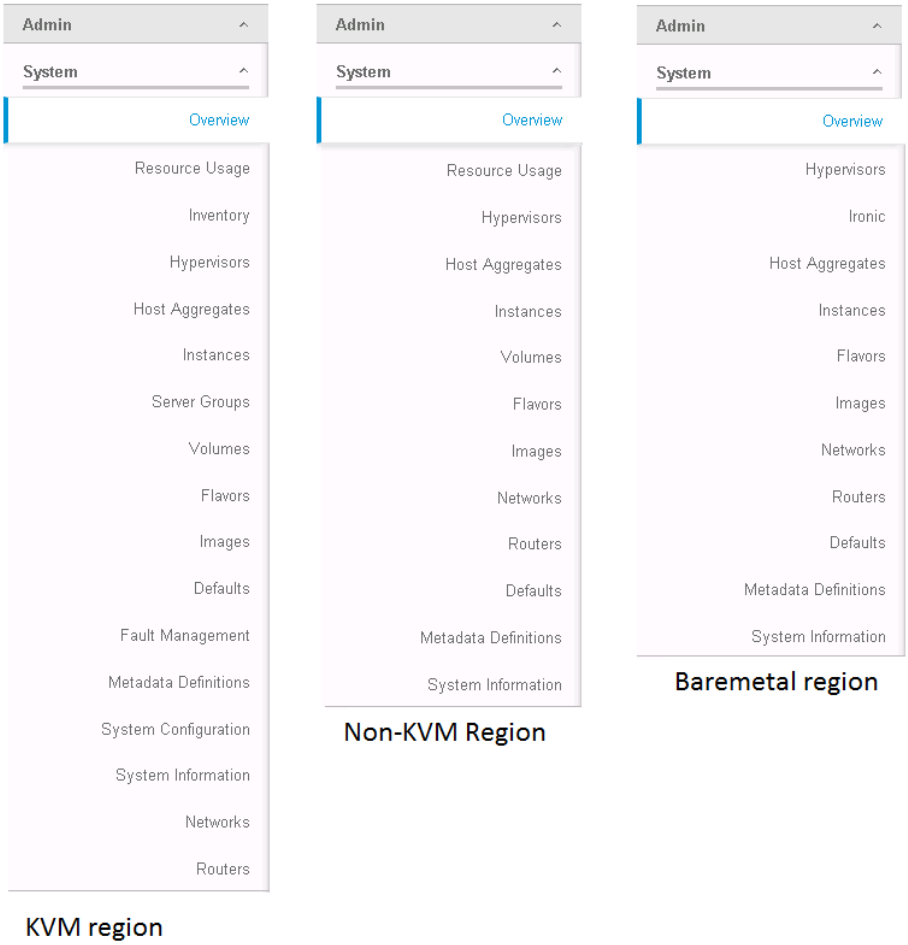
Orchestration

Note: Not available for the baremetal region in the Sacramento deployment.

Tab	Description	Reference
Stacks	Details for existing services (stacks), and controls for creating new services (launching stacks). Service details include topologies, resource allocations, and event histories.	
Resource Types		

HP Helion OpenStack® Carrier Grade 2.1 Beta: Using the Admin Panel

The **Admin** dashboard contains panels for managing projects (tenants), project resources, and users. It is available when an **admin** user is logged in.



The dashboard contains the following panels and tabs.

System

Tab	Description	Notes	Reference
Overview	Performance charts for system health monitoring, including hosts status, provider-network port utilization, and compute node processing, memory, and disk usage.		*Viewing System Status*
Resource Usage	Tools for performing Ceilometer database queries using real-time or collected data, to support detailed performance analysis.	*Not available for the baremetal region in the Sacramento deployment.*	*Resource Usage*
Inventory	Controls for managing systems, hosts, and standardized CPU, port, or storage profiles that can be applied to hosts.	*KVM region servers only*	*Managing Inventory*

Tab	Description	Notes	Reference
Hypervisors	Charts for monitoring hypervisor resource usage on compute nodes.		*Managing Hypervisors*
Ironic	Manage the baremetal region.	*Baremetal region servers only*	*Managing the Baremetal Region*
Host Aggregates	Controls for managing host aggregates and availability zones.		*Managing Host Aggregates*
Instances	Controls for managing virtual-machine instances.		*Managing Instances*
Server Groups	Controls for managing server groups across all tenants. Server groups are collections of instances sharing common attributes.	*KVM region servers only*	*Managing Server Groups*
Volumes	Controls for managing virtual disk volumes available for use with instances. The virtual volumes are implemented using *storage volumes* defined in the system.	*Not available for the baremetal region in the Sacramento deployment.*	*Managing Volumes*
Flavors	Controls for managing standardized processor, disk, and memory complements (flavors) that can be applied to virtual machines.		*Managing Flavors*
Images	Controls for managing disk images used to initialize and configure virtual machines.		*Managing Images*
Networks	Controls for managing tenant networks, provider networks, and QoS (Quality of Service) policies or tenant weightings.		*Managing Networks*
Routers	Controls for managing virtual routers. Administrators can list the virtual routers created for tenants, view router and interface details, and delete routers.		*Managing Routers*
Defaults	Controls for viewing and setting the default quota values for new tenants.		*Managing Default Quotas*
System Information	Status information for services and network agent processes, availability zones, and host aggregates.		*Viewing System Informaton*
Metadata Definitions	Information metadata definitions.		*Viewing Metadate Definitions*
Fault Management	System alarms and customer logs.	*KVM region servers only*	*Managing System Faults*
System Configuration	System configuration updates. *KVM region servers only*	*KVM region servers only*	*Managing System Configuration*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Using the Identity Dashboard

The **Identity** dashboard contains selections for managing projects (tenants) and users. It is available when an **admin** user is logged in.

The dashboard contains the following panels and tabs.

Identity

Tab	Description	Reference
Projects	Controls for managing projects (tenants).	*Managing Projects*
Users	Controls for managing user accounts.	*Managing Users*
Quotas	Controls for managing project quotas.	*Managing Project Quotas*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing System Status (Overview)

When you first log into the Helion interface, the Overview page appears.

The information in the page depends upon which region you are using.

- *memphis/denver*
- *regionone*

The `memphis` or `denver` Overview table contains the Usage Summary, For more information, see *Viewing the memphis/denver Region System Status*.

The `regionkvm` Overview table contains the following:

- Compute vCPU Usage
- Instance CPU Utilization.
- Compute Memory Usage
- Compute Disk Usage
- AVS CPU Utilization
- Provider Network Port Utilization
- Usage Summary

For more information, see *Viewing the regionkvm Region System Status*

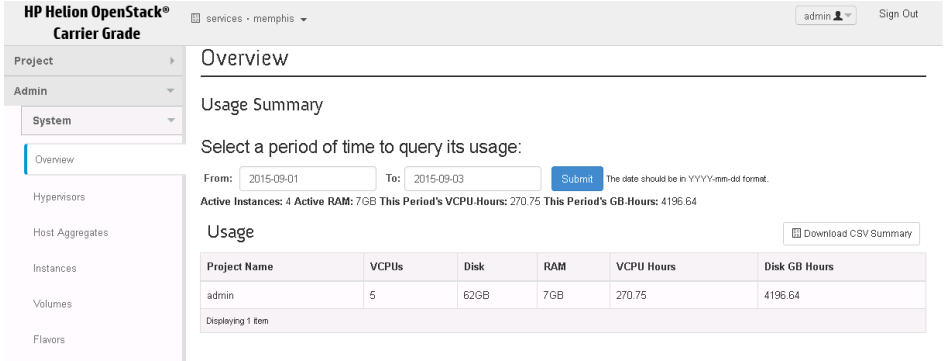
HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Non-KVM Region System Status (Overview)

When you first log into the Helion interface, the Overview page appears.

The information in the page depends upon which region you are using, non-KVM or KVM.

To view information on the servers in the non-KVM region, click *the deployment name in the region selector*.

The following information appears.



The Usage Summary displays information over the specified period of time for the current project.:

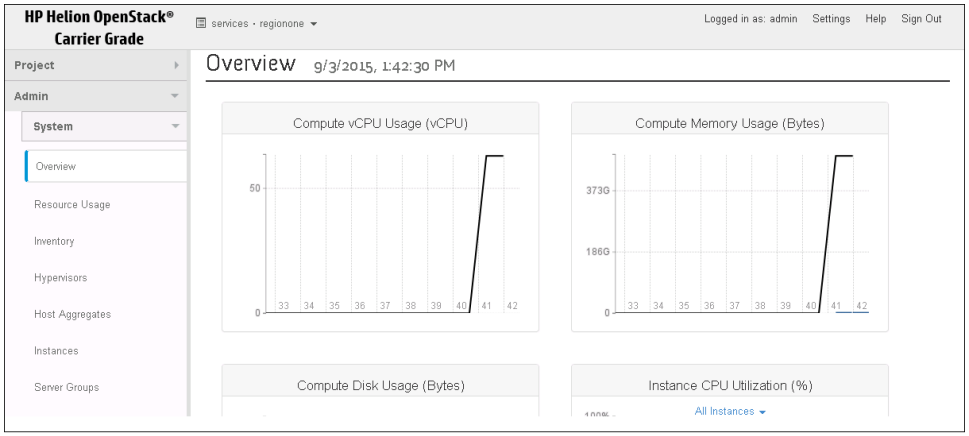
- **VCPUs**. The number of virtual CPUs allocated to the project.
- **Disk GB**. The virtual root disk size in gigabytes.
- **RAM GB** Memory allocated to the project.
- **VCPU Hours**. The VCPU hours for the project.
- **Disk GB Hours**. The total GB-hours for the project.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing KVM Region System Status (Overview)

When you first log into the Helion interface, the Overview page appears.

The information in the page depends upon which region you are using, non-KVM or KVM.

To view information on the servers in the KVM region, click *regionkvm in the region selector*.



The page includes the following features:

- dynamically updated, relocatable resource charts. Click the top of any chart, and drag it to the desired location to customize the presentation as desired. The layout changes are persistent across logins.
- dynamically updated, relocatable Host Server Status summary table. Presents the total number of hosts currently in one of the following states:
    - locked
    - unlocked
    - available
    - unavailable
    - degraded
- dynamically updated, relocatable Alarms summary table. Lists the current count of critical, major, minor, and warning alarms.

Common attributes of the resource pages are:

- All resource charts display resource information in real-time, spanning over a time-window of ten minutes.
- Labels along the X-axis present the number of minutes elapsed since the last full-time hour of the system clock.
- Hovering the mouse over the charts overlays information windows with detailed values.
- History information is lost when the **Overview** page is no longer displayed.

The following information appears:

Compute vCPU Usage. Presents information about the number of virtual CPUs across the entire cluster, available and allocated to virtual machines, and their average level of utilization. Elements in this chart are as follows:

- Y-axis is in units vCPUs.
- A solid black line tracking the number of available vCPUs. This line settles at a constant value at the top of the chart, unless the number of compute nodes changes over time.
- Light blue bars indicating the number of allocated vCPUs, that is, the number of vCPUs in use by virtual machines (one in the example).
- Dark blue bars indicating the average level of utilization of the allocated vCPUs (varies from 30 to 83% in the example), presented as a relative height with respect to the light blue bars.

Instance CPU Utilization. Presents information about virtual CPU utilization levels on virtual machines, across the entire cluster or for individual instances. Elements in this chart are as follows:

- Y-axis displays the virtual CPU utilization level, from 0 to 100%.
- A solid black line tracking the maximum utilization level.
- Dark blue bars indicating the average utilization level.
- A gray line tracking the minimum utilization level.
- A filter drop-down menu to select the virtual machines on which to report utilization levels. The default value for this filter is `All Instances`, and therefore it reports the same utilization levels indicated by the dark blue bars in the Compute vCPU Usage chart.

Compute Memory Usage. Presents information about memory usage levels on the compute nodes across the entire cluster. Elements in this chart are as follows:

- Y-axis is in units of bytes.
- A solid black line tracking the available aggregated compute memory. This line usually settles as a constant value at the top of the chart, unless the number of compute nodes changes over time.
- Dark blue bars indicating the amount of memory allocated to virtual machines (less than 1 GB in the example).

Compute Disk Usage. Presents information about disk usage levels on the compute nodes across the entire cluster. Elements in this chart are as follows:

- Y-axis is in units of bytes.
- A solid black line tracking the available aggregated storage capacity. This line usually settles as a constant value at the top of the chart.
- Dark blue bars indicating the amount of disk space allocated to virtual machines (about 1 GB in the example).

AVS CPU Utilization. Presents information about AVS CPU utilization levels on the compute nodes across the entire cluster. Elements in this chart are as follows:

- Y-axis displays the AVS CPU utilization level, from 0 to 100%.
- A solid black line tracking the maximum utilization level.
- Dark blue bars indicating the average utilization level.

Provider Network Port Utilization. Presents information about network traffic levels on provider networks across the entire cluster. Elements in this chart are as follows:

- Y-axis displays the port utilization level, from 0 to 100%.
- A solid black line tracking the maximum utilization level.
- Pairs of dark blue and dark green bars indicating the average utilization level, egress and ingress (Tx and Rx) traffic respectively.
- A gray line tracking the minimum utilization level.

Usage Summary

See *Overview of the* `memphis/denver` *region*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Resource Usage

Usage of system resources is monitored by Ceilometer, the standard OpenStack mechanism for collecting and distributing performance monitoring samples from the cluster. The HP Helion OpenStack Carrier Grade cluster extends Ceilometer with improved reports and new tools to facilitate offline analysis of the collected data.

Note: This feature applies only to KVM region servers.

Performance Monitor (PM) samples are periodically collected from different resources such as hosts, virtual machine instances, AVS, and others. They include CPU and memory utilization, network traffic counters, storage space, and several more. By default the samples are stored in a database which is used for reporting activities such as:

- command line queries and graphical charts
- triggering of threshold alarms
- triggering of threshold actions. The most common example is Heat actions to scale up and down a resource.

The Ceilometer database is periodically cleaned in order to contain its size and prevent the overuse of storage resources on the controller nodes.

The Ceilometer implementation in the HP Helion OpenStack Carrier Grade improves on several aspects. They are described in the following sections:

- *Optimized Ceilometer Filters*
- *On-Line Ceilometer Reports*
- *CSV Performance Monitoring Backend*
- *Retention Period*

Optimized Ceilometer Filters

The Ceilometer implementation in the HP Helion OpenStack Carrier Grade is specially tuned to allow time-sensitive actions, such as Heat autoscaling, to take place in response to relatively high-frequency sample rates of system events.

The size of both the Ceilometer database and the CSV files are maintained under control at all times, while still enabling the required system actions to take place in real-time.

On-Line Ceilometer Reports

On-line, on-demand, Ceilometer reports in the HP Helion OpenStack Carrier Grade benefit from several improvements over the stock OpenStack reporting tool, including:

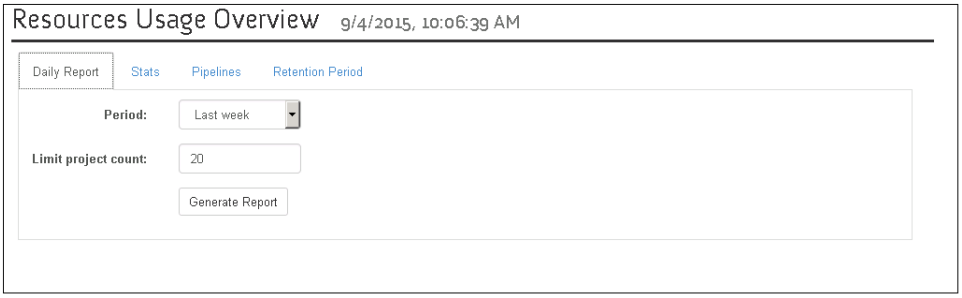
- optimized Ceilometer database queries
- improved naming of menu entries on pull-down menus
- use of brief meter descriptions and human-readable legends on the charts

Additionally, all database queries are user-initiated, as opposed to event-initiated. This provides a different user workflow, whereby all required report parameters and filters are configured first, before the database query is executed.

Access to Ceilometer reports is available from the Stats tab on the Resource Usage Overview page. This page can be accessed from the web management interface by selecting the option **Resource Usage** on the **Admin** tab of the **System** panel.

Daily Report

View a daily usage report per project across services through the OpenStack Dashboard to better understand how system resources are being consumed by individual projects.

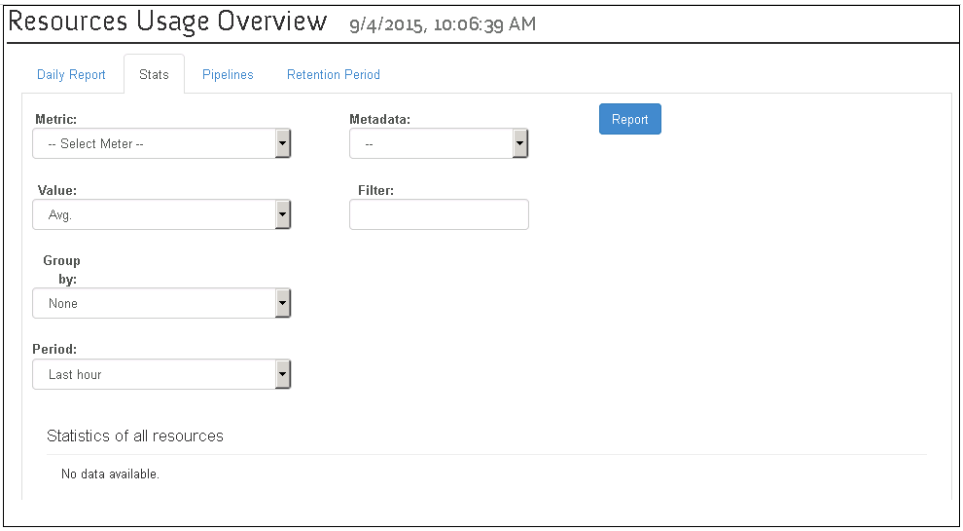


To view the Daily Report:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Resource Usage** tab.
4. Click the **Daily Report** table.
5. Select the date range and a limit for the number of projects, and click **Generate Report**. The daily usage report displays.

Stats

You can view project metrics by selecting the required values and time period using the menus and click Report.



To view stats:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Resource Usage** tab.
4. Click the **Stats** table.
5. Specify the values as needed:
   - **Metric** - The Ceilometer metric you want to query. Metrics are grouped by service, as follows:
     - Average Engine CPU Utilization
     - Average Port Receive Utilization
     - Port Receive Byte Count
     - Port Transmit Byte Count
     - Port Receive Packet Count
     - Port Transmit Packet Count

- **Value** - The particular statistic you want to visualize. Select among Average, Minimum, Maximum, and Summation.
- **Group by** - How to group the displayed charts, as follows:
  - **None** - The selected statistic is presented as a single line chart reporting the aggregate over all resources and projects (tenants).
  - **Projects (Tenants)** - The selected statistic is presented as a multiple line charts over all resources, one line per tenant.
  - **Resource** - The selected statistic is presented as a multiple line charts over all resources, one line per resource (hosts, instances, and so on).
- **Period** - The period of time to be covered by the report. When selecting other, two new fields become available, **Date From** and **Date To**, allowing you to specify a specific time period.
- **Metadata** - Metadata represents additional attributes collected with a metric. In this menu, you can select the specific attribute you want the report on.

  The pull-down menu is auto-populated with the corresponding attributes for the selected metric.
- **Filter** - Use this field to limit the report to show metric samples whose metadata attribute equals the specified value. The filter field is applied only when a specific metadata attribute is selected.

6. Click **Report**.

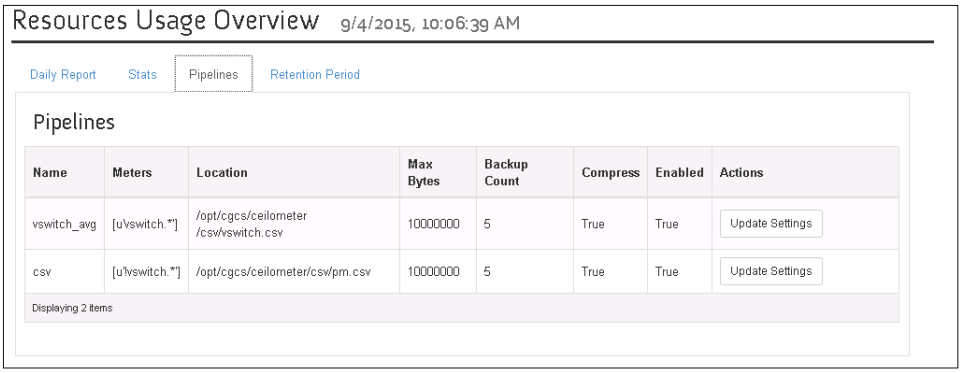
Pipeline (CSV Performance Monitoring Backend)

The HP Helion OpenStack Carrier Grade provides access to performance measurement samples in the form of comma-separated values (CSV) files. They provide the following benefits:

- off-line permanent storage of large samples history
- enables the use of off-line tools for data analysis, accounting, and archiving

The CSV files are expected to be retrieved from the controllers using any suitable file transfer client application such as SFTP or SCP. This can be done manually by the system administrator, or automatically by an operations and support server (OSS/BSS) configured with the appropriate login credentials.

Recording of samples and management of CSV files is done through special Ceilometer pipelines available from the Pipelines tab, as illustrated below:



The csv pipeline collects system information with the exception of AVS switching meters. The latter are collected by the `vswitch_avg` pipeline.

To view stats:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Resource Usage** tab.
4. Click the **Pipelines** table.
5. Click the **Update Settings** button to configure the behavior of a pipeline.
6. In the **Edit Pipeline** window, enter the values as needed:

- **Name** - A read-only field displaying the name of the pipeline.
- **Meters** - An editable field displaying the list of comma-separated meters included in the pipeline. The list must be enclosed in square brackets, as follows:

  ```
  [meter1,meter2,...]
  ```

  The following syntax rules apply to the specified meters:

  - A meter specification is a text string of the form `metergroup.metersubgroup.meter`, for example, `disk.read.bytes`.
  - A meter specification supports a trailing wild-card to include all meters within a `metergroup`. For example, the text `disk.*` matches the meters `disk.read.bytes` and `disk.write.bytes`.
  - A meter specification supports a trailing wild-card to include all `metersubgroups` within a `metergroup`. For example, the text `disk.read.*` matches the meter `disk.read.bytes`.
  - Meter specifications support a leading exclamation mark to exclude the specified meter, as follows:

    ```
    [!meter1,!meter2,...]
    ```

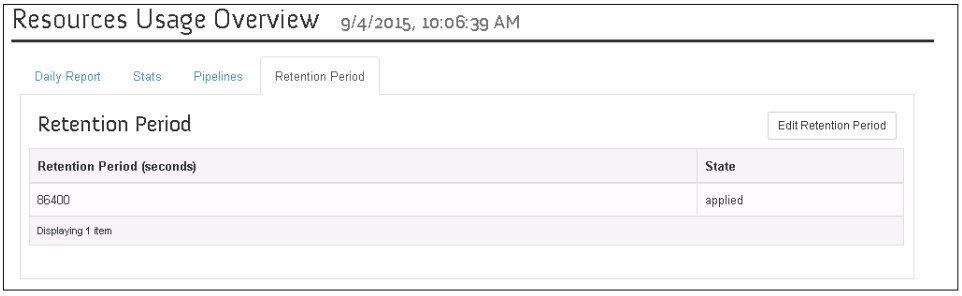
    Such a pipeline includes all meters but the ones in the list.

    Exclamation marks cannot be applied selectively in a list of meters. Either all meters use them or none at all.

    The following list is therefore invalid: [meter1,!meter2,meter3]
- **Location** - The absolute path to the CSV file on the controller.
- **Enabled** - A check box used to enable or disable the pipeline.
- **Max Bytes** - The maximum size, in bytes, of a CSV file. The default value is 10 MB.
- **Backup Count** - The number of concurrent backup CSV files to maintain in a rotation ring, including the currently active file. When a CSV file reaches its maximum size, it is renamed as a backup file, and a new CSV file is opened for writing. Backup files older than the size of the rotation ring are automatically removed.
- **Compress Backups** - A check box used to select whether or not to compress backup files in the rotation ring.

Retention Period

Performance samples are kept in the database for a limited period of time known as the retention period. Its default value is 86400 seconds, or 24 hours.



To modify a retention period:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Resource Usage** tab.
4. Click the **Retention Period** table.
5. Click the **Edit Retention Period** button You must verify that the configured value is equal or higher than the period over which you intend to gather statistics.

Note: Changes to the retention period cause 250.001 Configuration out-of-date alarms to be raised briefly for the controller nodes. During this period, the status `Config out-of-date` might display for the controller nodes on the **Host** tab of the **Inventory** pane. These alarms are resolved and cleared automatically after a few seconds.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Hardware Inventory

The maintenance and inventory component of HP Helion OpenStack Carrier Grade allows the administrator to install, configure, and manage the hosts of the HP Helion OpenStack Carrier Grade cluster.

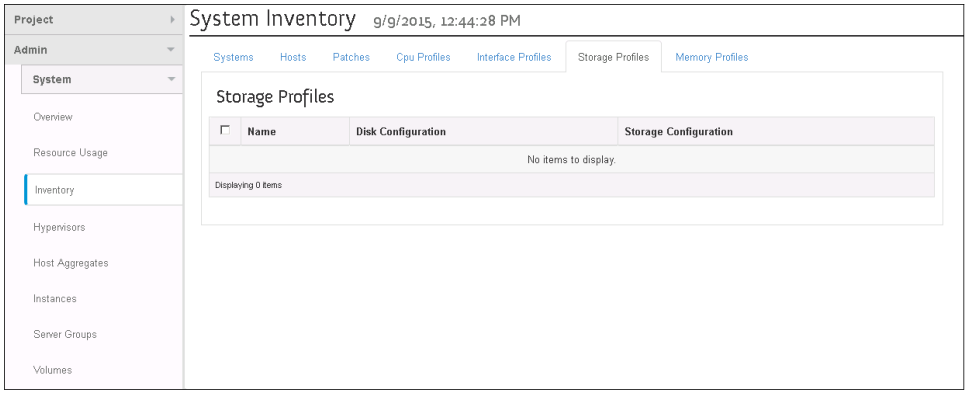
To access the Inventory tab, on the *Horizon interface*, click **Admin**, then **System**, then **Inventory**. You will see links to the following tables:

- *Systems*
- *Hosts*
- *Active Hosts*
- *Patches*
- *CPU Profiles*
- *Interface Profiles*
- *Storage Profiles*
- *Memory Profiles*

You can also get *detailed information on these components*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Hardware Inventory

The HP Helion OpenStack Carrier Grade cluster is represented internally by a unique object referred to as the *system* within this document. Information about this object is available from the **Systems** table on the **System Inventory** page.



By default, the name of the system object is its internal UUID, and it has no description.

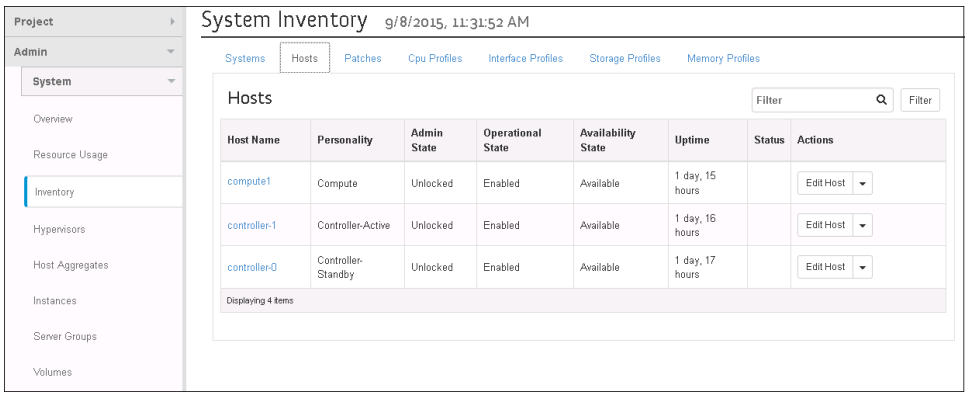
To edit the name of the system:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **System** table.
5. Click **Edit System** to enter a new name and click **Save**

After committing the changes, the **Systems** tab is displayed with the updated information:

HP Helion OpenStack® Carrier Grade 2.1 Beta: Working with Host Inventory

The **Hosts** table on the **Inventory** panel provides an overview of the current state of all hosts in the HP Helion OpenStack Carrier Grade cluster.



From this table, you can obtain detailed information about the hosts, and execute maintenance operations.

Click any of the following links to view information below:

- *Viewing information on Hosts*
- *Locking and Unlocking a Host*
- *Power Off and On a Host*
- *Reboot a Host*
- *Reset a Host*
- *Reinstall a Host*
- *Delete Host*
- *Swact a Host*

Also see the following topics:

- *Initializing and Configuring Compute Nodes*
- *Initializing and Configuring Controller Nodes*
- *Working with Highly Available Controller Nodes*
- *Managing Hosts on an Active System*

Viewing information on Hosts

To view information on a host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.

The information is refreshed periodically to reflect the ongoing changes on the cluster. It consists of the following columns:

- **Host Name** - The name assigned to the host. This is an active link pointing to the detailed inventory page for the host.
- **Personality** - The personality of the host (controller, compute, or storage).
- **Admin State** - The administrative state of the host. It can be in one of two states:
  - **Locked** - The host is administratively prohibited from performing services. This is the initial state for hosts autodiscovered in the cluster.
  - **Unlocked** - The host is administratively in service. A controller node in this state, and not in the failed state, is active in its HA role, and is running the assigned controller services.
- **Operational State** - The operational state of the host. It can be in one of two states:
  - **Disabled** - Indicates that the host is not providing the expected services. This may be due to the fact that it is in the process of being unlocked, a failure has occurred, or it is being automatically recovered due to a failure.

  - **Enabled** - Indicates that the host is providing the expected services, even if its operational environment is compromised. In the latter case, the host is reported to be in the degraded availability state, in which case, state maintenance is constantly trying to recover the host to fully available state through in-service testing.
- **Availability State** - The availability state of the host. It can be in one of the following states:
  - **Offline** - The host is known to the HP Helion OpenStack Carrier Grade, but is not reachable for maintenance purposes.
  - **Online** - The host is reachable and ready to be unlocked.
  - **InTest** - A transient state that occurs when transitioning from locked, or from a failed operational state, to unlocked states. While in this state, the host is executing a series of tests to validate its hardware and software integrity.
  - **Available** - The host is fully operational and providing services.
  - **Degraded** - The host is experiencing compromised operational conditions, such as low memory, but is still providing the expected services. Details about the compromised conditions are available through the alarms subsystem. See System Alarms on page 139 for details.
  - **Failed** - A major fault has occurred and the host is no longer providing any services. The HP Helion OpenStack Carrier Grade maintenance system automatically tries to recover hosts in this state.
  - **Power-off** - The host is known to have been powered off by a previous maintenance action.
- **Uptime** - The uptime of the host, as reported by the system maintenance service.
- **Status** - An indicator of the immediate activity occurring on the host. It reports transitory steps such as booting, initializing, configuration out of date, and in-test, which a host goes through as it transitions from one administrative or availability state to another.

Locking and Unlocking a Host

Unlocking a host brings the host into service. The first step is to reset the target host to ensure that it starts from a wellknown state.

Locking a host brings the host out of service.

Force locking a host takes the host out of service if for the Lock Host option does not work.

For more information, see *Locking and Unlocking a Host*.

Power Off and On a Host

You can use the Hosts page to power on or gracefully power off a host, ensuring that all system processes are properly shut off first.

These selections are available if board management is configured on the system, the host is equipped with an iLO module, and the host is in a powered-on state.

To power on/off a host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.

   In the **Hosts** list, for the system to power on or off, select **Power On** or **Power Off** from the **Edit Hosts** menu.

You can power off and on a host from the controller's command line, as follows:

```
system host-power-off <hostname>
system host-power-off <hostname>
```

Where <hostname> is the name of the system.

Reboot a Host

Gracefully shuts down the host, ensuring that all system processes are properly shut off first. The host then reboots automatically.

To reboot a host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
4. In the **Hosts** list, for the system to reboot, select **Reboot Host** from the **Edit Hosts** menu.

You can reboot a host from the controller's command line, as follows:

```
system host-reboot <hostname>
```

Where <hostname> is the name of the system.

Reset a Host

Use this selection only if Reboot Host fails. It performs an out-of-band reset, stopping and restarting the host without ensuring that all system processes are shut off first.

To reset a host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
4. In the **Hosts** list, for the system to reset, select **Reset Host** from the **Edit Hosts** menu.

> **Note:** This selection is available if board management is configured on the system, the host is equipped with an iLO module, and the host is in a powered-on state.

You can reset a host from the controller's command line, as follows:

```
system host-reset <hostname>
```

Where <hostname> is the name of the system.

Reinstall a Host

Forces a full re-installation of the HP Helion OpenStack Carrier Grade software on the host. The host's hard drive is erased, and the installation process is started afresh.

To reinstall a host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
4. In the **Hosts** list, for the system to reinstall, select **Reinstall Host** from the **Edit Hosts** menu.

Delete Host

Removes the host from the inventory database, and its hard drive is erased.

To delete a host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
4. In the **Hosts** list, for the system to delete, select **Delete Host** from the **Edit Hosts** menu.

You can delete a host from the controller's command line, as follows:

```
system host-delete <hostname>
```

Where <hostname> is the name of the system.

Swact a Host

This operation is available on controller nodes only, and should be run on the active controller to initiate a switch of the active/standby roles.

Swact is an abbreviated form of the term Switch Active (host). When selected, this option forces the other controller to become the active one in the HA cluster. This means that all active system services on this controller move to standby operation, and that the corresponding services on the other controller become active. Use this option when you need to lock the currently active controller, or do any kind of maintenance procedures, for example, when updating hardware or replacing faulty components.

To swact a host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
4. In the **Hosts** list, for the system to switch to active, select **Swact Host** from the **More** menu.

You can swact a host from the controller's command line, as follows:

```
system host-swact --force <hostname>
```

Where <hostname> is the name of the system.

HP Helion OpenStack® Carrier Grade 2.1 Beta: The Life Cycle of a Host System

The life cycle of a host is the set of state transitions the host goes through as its current state changes. The host states in the HP Helion OpenStack Carrier Grade are based on the ITU X.731 State Management Function Specification for Open Systems.

The current state of a host is determined by the allowed combinations of the administrative, operational, and availability states at any given time. The following figure illustrates the life cycle of a host.

The description that follows uses the availability states only.

The life cycle of a new host starts when it is discovered by the active controller on the internal management network.

A new host is initially reported as Offline. As an exception, the first controller, controller-0, is automatically set to available during initial commissioning. The following are the available transitions. Numbers are attached to them for easier reference:

- **Offline to Online** - This transition takes place once the administrator configures the host name and personality of the host. During the transition, the HP Helion OpenStack Carrier Grade software is installed and the host reboots. The transition concludes when the controller establishes maintenance and inventory connectivity with the new host.
- **Online to InTest** - This transition takes place when the administrator requests to move the host from the locked to the unlocked administrative states. The host reboots first. After it finishes booting, it establishes maintenance communication and enters the transient InTest state. While in this state, the configuration is applied, and a set of hardware and software tests are executed to ensure the integrity of the host.
- **InTest to Available, Degraded, or Failed** - The transition is initiated automatically after the activities in the transient state inTest are complete. Depending on the outcome, the host goes into one the three states.
- **Failed to InTest** - This is a value-added maintenance transition that the HA framework executes automatically to recover failed hosts.
- **Available to/from Degraded, Available to Failed, and Degraded to Failed** These are transitions that may occur at any time due to changes on the operational state and faults on unlocked hosts.

- **Available, Degraded, or Failed, to Offline** - These are maintenance transitions that take place automatically to reflect the operational state of a host. On a compute node in Available or Degraded state, the transition triggers the live migration of the active instances to another available compute node.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Initializing and Configuring Compute Nodes

You can assign a new host as a compute node to support virtual machines.

Note: This feature applies only to KVM region servers.

Before initializing a node, ensure that the following conditions are satisfied:

- The node must meet the hardware requirements for the personality to be assigned. For more information, see Hardware Requirements
- `Controller-0` must be installed and operational.
- The node must be connected to the internal management network using an Ethernet interface configured for PXE boot.
- The node must be configured in the BIOS to boot from the internal management network.

To install and configure a compute node:

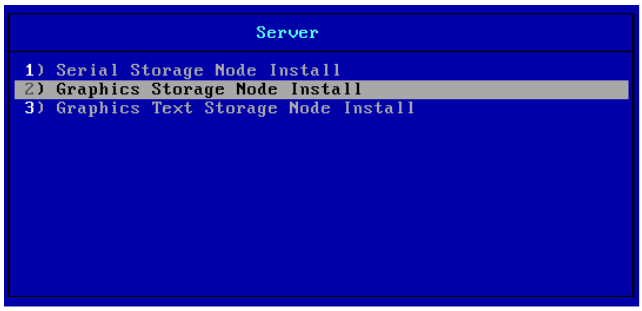
1. *Power on the node* to be configured as a compute host.

   Note: To ensure you can correctly identify hosts as you install them, power on and configure each new node one at a time.
2. *Launch the HP Helion OpenStack Horizon Dashboard*.
3. *Select the appropriate region and project*.
4. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
5. Click the **Hosts** tables

   The new node is listed with an empty `Host Name` and `Personality`.
6. Assign the node's personality:

   1. Click **Edit Host** for the new host.
   2. In the **Edit Host** screen, select **Storage** from the **Personality** list.
   3. **Optional**: Enter a physical Location for the node to help identify it.
   4. Click **Save** to initialize and configure the new node.

   The node is restarted automatically, and a display-device menu appears on the node console.



7. **Optional:** Select the display device to use during initialization. The personality (Controller, Compute, or Storage) is confirmed in the menu. If you do not change the selection, the default is applied automatically after a few seconds.

   - **Serial <personality> Node Install** (default) - Use the serial port to display messages. You can monitor the port using the terminal server.
   - **Graphics <personality> Node Install** - Use the console port in graphics mode to display messages. This selection works with most console displays.

- **Graphics Text <personality> Node Install** - Use the console port in text mode to display messages. This is a safe option for nodes that do not support graphics mode.

8. Wait while the node is configured and rebooted.

After a few minutes, the node is reported as `Locked`, `Disabled`, and `Online` in the **Hosts** list.

Caution: To ensure a successful installation, wait for the node to be reported as Locked, Disabled, and Online, and ensure that the login prompt appears on the host console. If the process is interrupted prematurely, the host installation can fail.

The new host is initialized with an operating system, rebooted, and configured as a storage node. It is automatically assigned the next available consecutive name (`storage-0` or `storage-1`).

9. Configure the host so that it can be unlocked.

Before you can unlock a storage node, you must do the following:

1. Create storage volumes. For details, see Creating Storage Volumes.
2. If using LAG to attach to the management network, change the **Interface Type** for the management network interface to aggregated ethernet For more information, see Editing Interface Settings.
3. Configure the interface to the infrastructure network. For details, see Network Interface Provisioning.

10. *Unlock the node* to make it available for use. Click **More** then **Unlock Host**.

The node is rebooted, and its Availability State is reported as In-Test. After a few minutes, it is reported as `Unlocked`, `Enabled`, and `Available`.

Note: Ensure that you install two storage nodes, as required by the HP Helion OpenStack Carrier Grade architecture.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Initializing and Configuring Controller1

You must assign a host as a second controller to provide redundancy for controller-0.

Note: This feature applies only to KVM region servers.

Before initializing a node, ensure that the following conditions are satisfied:

- The node must meet the hardware requirements for the personality to be assigned. For more information, see Hardware Requirements
- `Controller-0` must be installed and operational.
- The node must be connected to the internal management network using an Ethernet interface configured for PXE boot.
- The node must be configured in the BIOS to boot from the internal management network.

To install and configure `Controller-1`:

1. *Power on the node* to be configured as `Controller-1`.

Note: To ensure you can correctly identify hosts as you install them, power on and configure each new node one at a time.

2. *Launch the HP Helion OpenStack Horizon Dashboard*.

3. *Select the appropriate region and project*.

4. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.

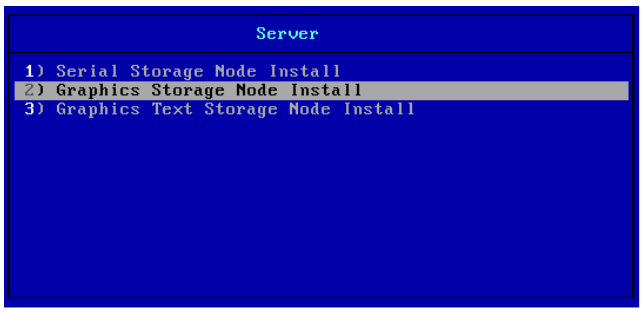
5. Click the **Hosts** tables

6. The new node is listed with an empty **Host Name** and **Personality**.

7. Assign the node's personality:

1. Click **Edit Host** for the new host.
2. In the **Edit Host** screen, select **Controller** from the **Personality** list.
3. **Optional**: Enter a physical Location for the node to help identify it.
4. Click **Save** to initialize and configure the new node.

The node is restarted automatically, and a display-device menu appears on the node console.



8. **Optional:** Select the display device to use during initialization. The personality (Controller, Compute, or Storage) is confirmed in the menu. If you do not change the selection, the default is applied automatically after a few seconds.
   - **Serial <personality> Node Install** (default) - Use the serial port to display messages. You can monitor the port using the terminal server.
   - **Graphics <personality> Node Install** - Use the console port in graphics mode to display messages. This selection works with most console displays.
   - **Graphics Text <personality> Node Install** - Use the console port in text mode to display messages. This is a safe option for nodes that do not support graphics mode.
9. Wait while the node is configured and rebooted.

   After a few minutes, the node is reported as `Locked`, `Disabled`, and `Online` in the **Hosts** list.

   Caution: To ensure a successful installation, wait for the node to be reported as Locked, Disabled, and Online, and ensure that the login prompt appears on the host console. If the process is interrupted prematurely, the host installation can fail.

   The time required to configure and reboot `controller-1` depends on the secondary disk partition size. Larger partitions require more time for synchronization with `controller-0`.

   The host is now configured with a personality.
10. Configure the host so that it can be unlocked.

    Before you can unlock a storage node, you must do the following:

    1. Create storage volumes. For details, see Creating Storage Volumes.
    2. If using LAG to attach to the management network, change the **Interface Type** for the management network interface to aggregated ethernet For more information, see Editing Interface Settings.
    3. Configure the interface to the infrastructure network. For details, see Network Interface Provisioning.
11. *Unlock the node* to make it available for use. Click **More** then **Unlock Host**.

    The node is rebooted, and its Availability State is reported as `In-Test`. After a few minutes, it is reported as `Unlocked`, `Enabled`, and `Available`.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Controller Nodes and High Availability

Services in the controller nodes run constantly in active/standby mode to provide continuity in the event of a controller failure.

Note: This feature applies only to KVM region servers.

This topic covers the following:

- *About controller HA*
- *Viewing the active controller*
- *Taking a controller out of service*

About controller HA

Controller services are organized internally into the following groups:

- Cloud Services - The enhanced OpenStack components, including Nova, Neutron, Cinder, Ceilometer, and Heat
- Controller Services - Core HP Helion OpenStack Carrier Grade services such as maintenance and inventory
- Directory Services - LDAP services
- OAM Services - OAM access services
- Patching Services - Patching alarm services
- Storage Monitoring Services - Storage alarm services
- Storage Services - Storage REST API services
- Web Services - The HP Helion OpenStack Carrier Grade OpenStack Horizon service and web server

Each of these groups is run in 1:1 HA mode by the controllers. This means that while some service groups can be active on controller-0, and in standby on controller-1, others are active on controller-1, and in standby on controller-0.

The high-availability framework constantly monitors and reports on the health of the individual services within each of the service groups on both controllers. When a service fails, a decision is made on whether to restart it on the same controller, or to switch the corresponding service group to the other controller. This decision depends on the criticality and the dependencies of the affected service.

Viewing the active controller

Services in the Controller Services group drive core functionality in the HP Helion OpenStack Carrier Grade. The controller where they are running is referred to as the active controller.

When working from the CLI on a controller node it is often important to ensure that you are working on the active controller, for example, to execute OpenStack admin operations, or to change the password of the wrsroot user account. See Linux User Accounts on page 16 for further details on the wrsroot account.

You can ensure you are working on the active controller by using the OAM floating IP address as the destination address in the SSH command.

To determine which host is the active controller:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Hosts** tables

The **Hosts** tab lists the status of all hosts in the cluster; it reports the active controller as having the `Controller-Active` personality.

Taking a controller out of service

For maintenance purposes, when one of the controller nodes needs to be powered down for service, it is necessary to force all currently active service groups in one controller to switch to the other.

This can be done from the Hosts tab on the Inventory page, by selecting the option swact (switch active) in the More menu of the controller you want to take out of service:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Hosts** tables
5. For the host you want to take out of service, click **Edit Host** then **Swact Host**.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Locking and Unlocking a System

You can lock and unlock a system, for example when you need to make a change to the system.

Note: This feature applies only to KVM region servers.

- *Lock a system*
- *Unlock a system*
- *Forcing a Host Lock*

Lock a system

You can lock a host in order to bring the host out of service.

On a controller node, the state transition only succeeds if there are no services running in active mode on the host.

On a compute node, the state transition only succeeds if all currently running instances on the host can be live-migrated to alternative compute nodes. Live-migration of the virtual machine instances is initiated automatically by the HP Helion OpenStack Carrier Grade as soon as the state transition is requested.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Hosts** tables
5. In the **Hosts** list, for the system to lock, select click **Edit Host** then **Lock Host**.

   Wait for the host to be reported as **Locked**.

You can try to lock a host from the controller's command line, as follows:

```
system host-lock hostname
```

Unlock a host

Used to bring a host into service. The first step is to reset the target host to ensure that it starts from a wellknown state. The host is automatically configured, and any required software patches are applied.

The state transition only succeeds if all the necessary configuration components for the host are already in place. For example, the state transition is rejected on a compute node for which no data interfaces are defined.

To unlock the host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Hosts** tables
5. In the **Hosts** list, for the system to lock, select click **Edit Host** then **Unlock Host**.

   Wait for the host to be reported as unlocked

You can unlock a host from the controller's command line, as follows:

```
system host-unlock hostname
```

Forcing a Host Lock

If for some reason, the Lock Host command does not lock the host, you can force a lock. When selected, the system displays a warning message appropriate to the personality of the host. Use this option with caution.

To force a lock on the host:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Hosts** tables
5. In the **Hosts** list, for the system to lock, select click **Edit Host** then **Force Lock Host**.

Wait for the host to be reported as **Locked**.

You can force lock a host from the controller's command line, as follows: ~(keystone_admin)$ system host-lock --force hostname Note that a force lock operation on a compute node causes an immediate service outage on all hosted virtual machines.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Hosts on an Active System

You can add or remove hosts and change disks without interrupting the HP Helion OpenStack Carrier Grade.

To make changes to a host, you must lock it. Locking a host automatically and seamlessly redirects activity to other available hosts. While the host is locked, you can safely power it down and make disk changes, or remove the host and insert a new one.

After making the required configuration changes, you can unlock the host and begin using it.

- *Replacing Active Controller Nodes*
- *Replacing Active Storage Nodes*
- *Managing Active Compute Nodes*

Managing Compute Nodes The compute nodes in HP Helion OpenStack Carrier Grade form a resource pool for hosting guest instances. You can manage this pool by managing the hosts. You can change the resource pool in several ways:

- Add or remove hosts to increase or decrease the size of the pool.
- Replace a host with another that has different resources (for example, memory, or number of CPU cores).
- Adjust the resources on an existing host.
- Replace a failed compute node host with an equivalent.

Caution: When replacing or adjusting a host, ensure that the overall resource pool still meets the requirements for your system.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Replacing Active Storage Nodes

On systems that use a Ceph backend for Cinder storage, you can add or replace storage disks or swap a storage node while the system is running, even if the storage resources are in active use.

Note: This feature applies only to KVM region servers.

A HP Helion OpenStack Carrier Grade system with a Ceph storage backend uses exactly two storage nodes; you cannot add or remove storage nodes. However, you can add disks to a storage node to increase capacity, and you can replace a faulty host.

Note: The storage node pair in a HP Helion OpenStack Carrier Grade system provides redundancy for High Availability. A balanced storage capacity is recommended, in which each host has sufficient independent resources to meet the operational requirements of the system.

To replace a storage node on an active system:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
   - Use the IP address for the appropriate region where you want to make the change, either: the Non-KVM region or the KVM region.
2. Click the **Admin** dashboard, then the **System** panel, then the **System Inventory** link.
3. Click the **Hosts** tab.
4. *Lock the standby controller* by clicking **More** then **Lock Host** for the controller.

   Wait for the procedure to be completed.
5. *Power down the standby controller* and make any required hardware changes.

   This may involve replacing disks, or replacing the host completely.
6. Place the new or modified controller into service.

   To begin using the new disk, *power up the host* and *unlock* the host.

- For disk replacement, no additional configuration changes are needed.
- For disk addition, you must create a new storage volume (OSD) before you can use the new disk. For more information, see the HP Helion OpenStack Carrier Grade Software Installation Guide: Creating Storage Volumes.
- For host replacement, you must *delete the existing host* using **More** then **Delete Host**. Then you must initialize the new host with a personality as a storage node, configure its interfaces, and create storage volumes.

For more information on initializing and configuring a storage node, see *Initializing and Configuring Storage Nodes*.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Replacing Active Controller Nodes

You can replace controller nodes or disks while the system is running. The HP Helion OpenStack Carrier Grade system uses exactly two controllers; you cannot add or remove a controller. However, you can replace the primary or secondary disks, and you can replace faulty controller nodes.

Note: This feature applies only to KVM region servers.

Note: If you are replacing disks in order to increase the controller storage capacity, follow the instructions for Changing Storage Space Allotments on the Controller.

To replace a controller node on an active system:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
   - Use the IP address for the appropriate region where you want to make the change, either: the Non-KVM region or the KVM region.
2. Click the **Admin** dashboard, then the **System** panel, then the **System Inventory** link.
3. Click the **Hosts** tab.
4. *Lock the standby controller* by clicking **More** then **Lock Host** for the controller.

   Wait for the procedure to be completed.
5. *Power down the standby controller* and make any required hardware changes.

   This may involve replacing disks, or replacing the host completely.
6. Place the new or modified controller into service.

   a. *Power up the controller*.

   Wait until the controller is reported as Locked, Enabled, and Available.

   Wait for the host to be reported as Locked, Disabled, and Online.

   If you are making disk changes to increase storage capacity, you must re-install HP Helion OpenStack Carrier Grade. For more information, see Changing Storage Space Allotments on the Controller

   To reinstall the software on a host , click More > Reinstall.

   Note: If the host does not boot from the management network, ensure that the host BIOS is configured for PXE boot.

   c. *Perform a swact* by clicking **More** then **Swact Host** for the active controller.

   The standby controller becomes the active controller, and the original active controller is placed into standby.
7. *Lock the original active controller*, which is in standby.

   a. Open the Hosts list by clicking Inventory on the System Panel section of the Admin menu, and then selecting the Hosts tab.

   b. Click **More** then **Lock Host** for the controller.

   Wait for the procedure to be completed.
8. Power down the controller and make the same hardware changes.

Caution: The configurations for controller-0 and controller-1, including disk types and sizes, must be identical.

9. *Power up the new or modified controller*.

The updated controllers are now in service. The controller that was formerly active is now the standby controller.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Deleting a System

You can lock and unlock a system, for example when you need to make a change to the system.

Note: This feature applies only to KVM region servers.

You can remove a compute node from the pool of available resources. You may need to remove a compute node in order to replace a failed host, or to change the configuration of a host. If the host is active, you can migrate instances on it by locking the host.

Caution: Before locking a host, ensure that sufficient resources are available on other hosts to migrate any running instances.

Delete a host

To delete a host system from the HP Helion OpenStack Carrier Grade system:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. Click **Inventory** on the **System Panel** section of the **Admin** menu, and then selecting the **Hosts** tab.
3. *Lock the standby controller* by clicking **More** then **Lock Host** for the controller.

   Wait for the host to be reported as Locked
4. Click **More > Delete Host** for the host you want to delete.
5. Power down the host and remove the hardware from the cluster.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Adjusting Resources on a Compute Node

The compute nodes in HP Helion OpenStack Carrier Grade form a resource pool for hosting guest instances. You can manage this pool by managing the hosts.

Note: This feature applies only to KVM region servers.

You can adjust the resources of a compute node while it is offline.

Caution: When replacing or adjusting a host, ensure that the overall resource pool still meets the requirements for your system.

To adjust compute node resources on an active system:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
   - Use the IP address for the appropriate region where you want to make the change, either: the Non-KVM region or the KVM region.
2. Click the **Admin** dashboard, then the **System** panel, then the **System Inventory** link.
3. Click the **Hosts** tab.
4. *Lock the host to be modified* by clicking **More** then **Lock Host** for the controller.

   Wait for the procedure to be completed.
5. *Power down the host*.
6. Make any required resource changes (for example, BIOS changes required for proper operation).

   If you are adding a disk to provide additional local storage for VMs, you can install an unpartitioned disk. New disks are detected by the compute node operating system and automatically configured with a single partition.
7. *Power on the host* and wait for it to reboot fully.

When the host is fully rebooted, it is shown as Locked, Enabled, and Available in the Hosts list.

Note: Do not unlock the host until it is fully rebooted.

8. *Unlock the host*.

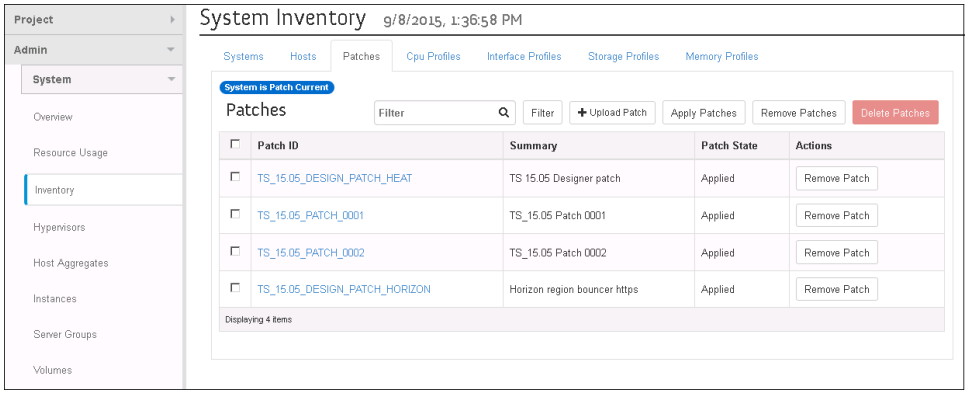
   The host is rebooted a second time.

The host is ready for use with the adjusted resources when reported as `Unlocked`, `Enabled`.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Applying Patches to KVM Region Servers

If there are any patches required or optional to be installed into the KVM region of HP Helion OpenStack Carrier Grade, you can use the Horizon interface to apply the patches.



Note: This feature applies only to KVM region servers.

Apply patches

To apply patches:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
4.
5. Click the **Patches** table.
6. Click **Upload Patches** to locate the patch file and import the patch file into the Horizon interface and click **Upload Patch**.
7. Select the patch in the Patch List and click **Apply Patches**.

   The Patches page is updated to report the patch to be in the Partial-Apply state..
8. In the **Hosts** list, for `controller0`, select **Swact Host** from the **Edit Hosts** menu to transfer active services to the standby controller.

   Wait for the procedure to be completed.
9. For `controller0`, select **Install Patches** from the `Edit Hosts` menu.
10. When the patch in installed, for `controller0`, select **Swact Host** from the **Edit Hosts** menu to transfer active services back to `controller0`.

    Wait for the procedure to be completed.
11. For `controller1`, select **Install Patches** from the `Edit Hosts` menu.

    On the **Patches** table, the patch is now in the `Applied` state.

Back out a patch

If, for some reason, you need to remove, or back out, a patch,

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Hardware Profiles

A hardware profile is a named object that captures a particular host configuration. The profile can be applied to any other host with a similar hardware configuration.

- **Cpu Profiles**. A CPU profile is a named assignment of processors and cores.
- **Interface Profiles**. An interface profile is a named configuration of Ethernet ports and interfaces on a host.
- **Storage Profiles**. A storage profile is a named configuration for a list of storage resources on a computing node.
- **Memory Profiles** A storage profile is a named configuration for a list of storage resources on a computing node.

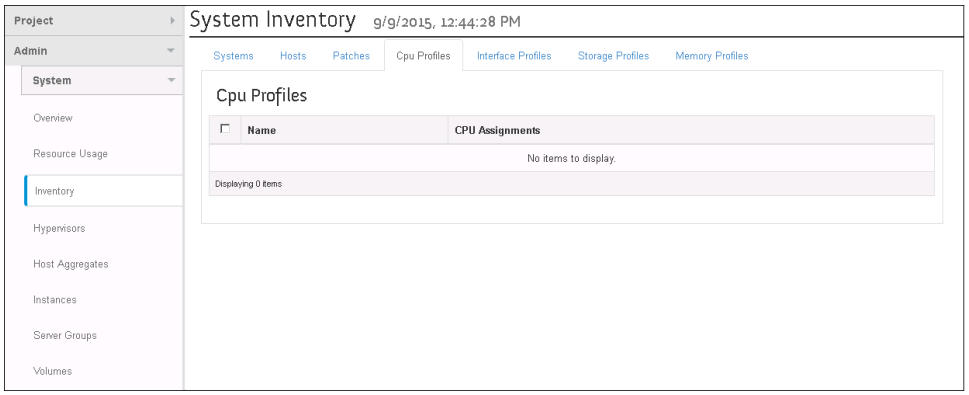
Note: This feature applies only to KVM region servers.

To view hardware profles:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the any of the following tables:
   - CPU profiles
   - interface profiles
   - storage profiles
   - memory profiles

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing CPU Profiles

A CPU profile is a named assignment of processors and cores to one or more of the following types of processing threads:



Note: This feature applies only to KVM region servers.

To view hardware profles:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **CPU Profile** tables.

A list the currently defined CPU profiles displays, including the following information:

Platform. System threads handling the core hosting functionality of the host. Platform threads are always present on all types of hosts in the cluster.

vSwitch. AVS threads dedicated to handling network traffic and packet processing tasks. They exists on the compute nodes only.

Shared. Threads handling low-load or non-real-time virtual machine tasks, implemented on a shared physical CPU in a compute node.

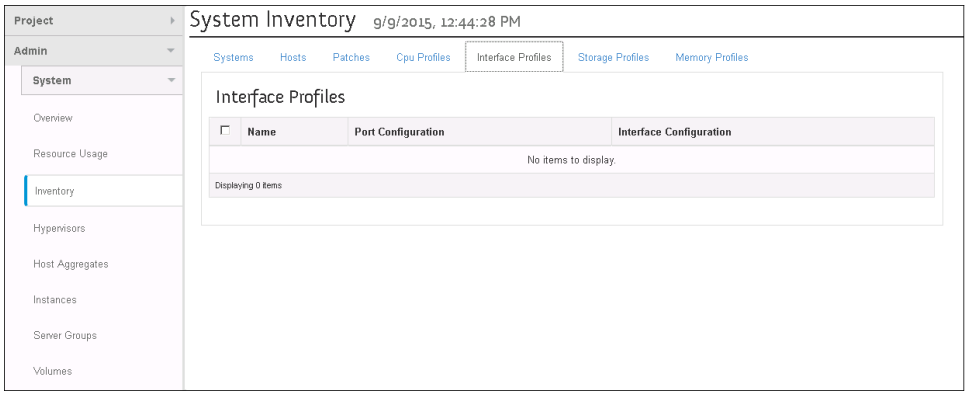
Virtual Machines. Threads handling virtual machines. They exists on the compute nodes only.

On controller nodes, all processors and cores are automatically assigned to platform threads, as they are the only ones available. On compute nodes, which always run a number of threads of all types, a default CPU allocation is done automatically when the system software is initially installed.

See *Working with CPU Profiles* for more information of how to change the CPU allocation for a compute node, and on how to define CPU profiles.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Interface Profiles

An interface profile is a named configuration of Ethernet ports and interfaces on a host, as follows:



Note: This feature applies only to KVM region servers.

To view hardware profles:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Memory Profiles** tables.

A list the currently defined Interface profiles displays, including the following information:

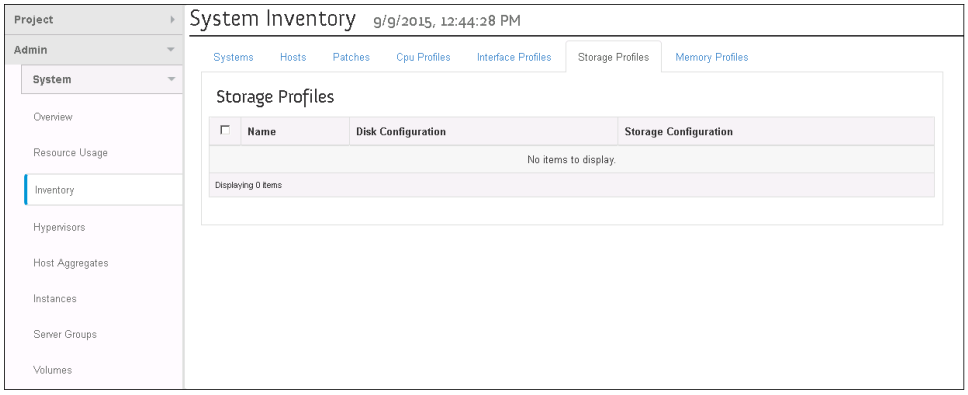
Ethernet Ports The list of physical Ethernet ports that have been allocated to connect to a network.

Interfaces Logical L2 interfaces defined on top of physical Ethernet ports.

For more information on how to create interface profiles, see *Working with Interface Profiles*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Storage Profiles

A storage profile is a named configuration for a list of storage resources on a computing node



Note: This feature applies only to KVM region servers.

To view hardware profles:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Storage Profiles** tables.

Each storage resource consists of the following elements:

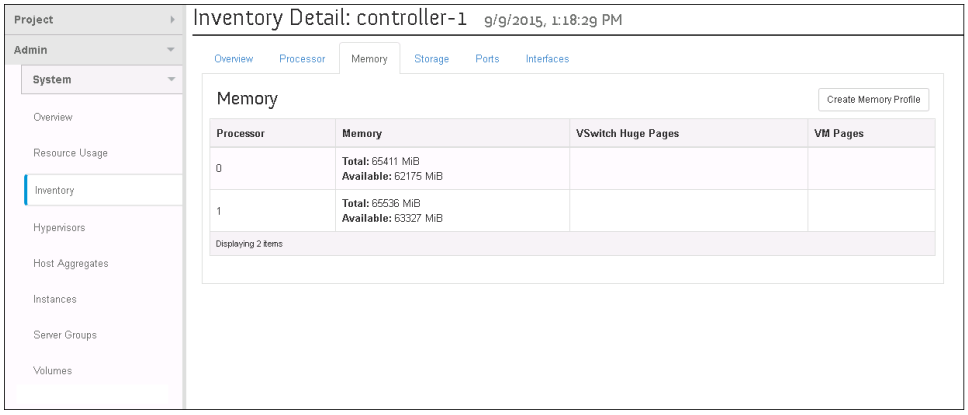
Disks A Linux block storage device, such as `/dev/sdd`, identifying an entire hard drive.

`Storage Volumes` A storage volume consisting of a name and a storage function. The name is used as a human-readable version of the native storage device UUID. The storage function indicates the type of storage backend, such as OSD for a storage system.

For more information on how to create storage profiles, see *Working with Storage Profiles*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Memory Profiles

A memory profile is a named assignment of huge pages for use as VM memory.



Note: This feature applies only to KVM region servers.

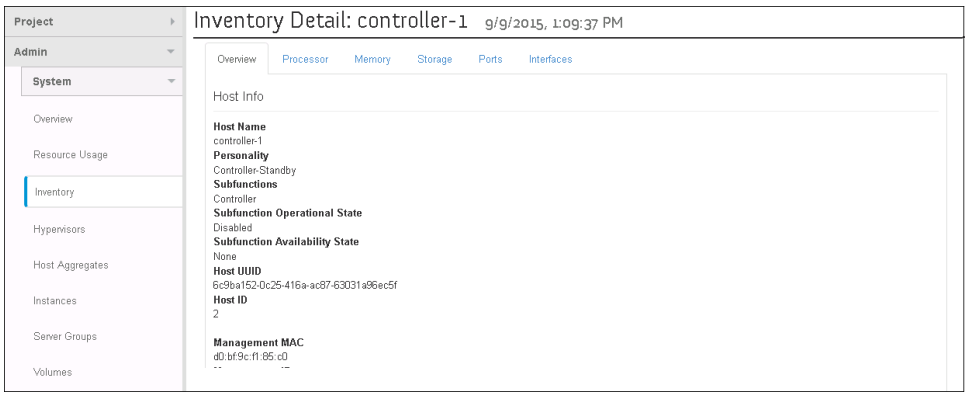
To view hardware profles:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. Click the **Memory Profiles** tables.

For more information on how to create memory profiles, see *Working with Memory Profiles.*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Host Systems

From the **Inventory Detail** page you can see detailed information about a host, and use it to define hardware profiles that can be used across the cluster.



Note: This feature applies only to KVM region servers.

You access the **Inventory Detail** page by clicking the host name on the **Hosts** tab of the **Systems Inventory** page. The inventory detail for a host consists of multiple tabs, each addressing a different aspect of the host.

They include:

- *Working with Host CPUs*
- *Working with Host Memory*
- *Working with Host Storage*
- *Viewing Host Port Details*
- *Working with Host Interfaces*

Overview

The **Overview** tab on the **Inventory Detail** page summarizes core details about a host object.

To view the host CPUs:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.

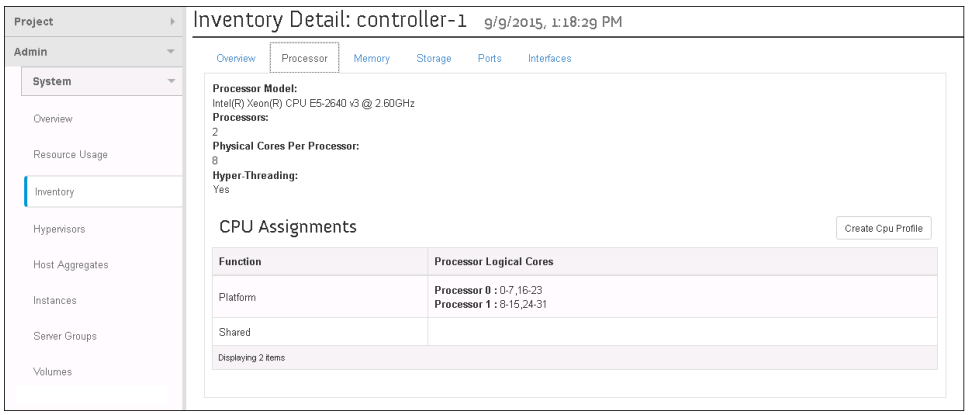
The following items are included in the summary:

- host name, personality, and the internal UUID and host ID reference numbers
- MAC and IP addresses on the internal management network
- serial ID, if known. Use the command system host-modify <hostname> serialid=xxx to update it.
- location, as entered by the operator using the Edit Host window. For more information, see *Host Memory*
- time stamps of when the host was created and last updated
- the host's state
- board management (iLO) information, if available, including controller type, MAC address, and IP address.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Working with Host CPUs Profiles

The **Processor** tab on the **Inventory Detail** page presents processor details for a host.



Note: This feature applies only to KVM region servers.

You access the **Inventory Detail** page by clicking the host name on the **Hosts** tab of the **Systems Inventory** page. The inventory detail for a host consists of multiple tabs, each addressing a different aspect of the host.

This page details:

- *Viewing details of host CPUs*
- *Creating CPU profiles*
- *Editing CPU assignments*
- *Designating shared physical CPUs on a compute host*
- *Viewing NUMA node resources on a host*

Viewing details of a host CPUs

To view the host CPUs:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
5. Select the Processor tab.

The Processor tab includes the following items:

- processor model
- number of processors
- number of cores per processor
- Hyper-Threading status (enabled or disabled)
- CPU assignments

Creating CPU profiles

To create a CPU profile:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
5. Click the **Processor** tab.
6. Click the **Create CPU Profile** button.

   Clicking this button displays the **Create CPU Profile** window, where the current CPU assignment can be given a name.

Editing CPU Assignments

Currently, the number of platform cores is limited to one for each host. This is indicated by the read-only platform fields that allocate one core from processor 0.

AVS cores can be configured for each processor independently. This means that the single logical vSwitch running on a compute node can make use of cores in multiple processors, or NUMA nodes. Optimal data path performance is achieved however, when all AVS cores, the physical ports, and the virtual machines that use them, are all running on the same processor. However, having AVS cores on all processors ensures that all virtual machines, regardless of the core they run on, are efficiently serviced. The example allocates two cores from processor 0 to the AVS threads.

One physical core per processor can be configured as a shared CPU, which can be used by multiple VMs for low-load tasks. To use the shared physical CPU, each VM must be configured with a shared vCPU ID. For more information, see Pinning a vCPU to a Shared Physical CPU.

All other cores are automatically available for allocation to virtual machine threads.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. *Lock the host* to make changes. Click **Edit Host** then select **Lock Host**. Wait for the host to be reported as `Locked`.
5. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
6. Click the **Processor** tab.
7. Click the **Edit CPU Assignments** button.

   This button is available only when the host is in the locked state.

   Clicking this button displays the **Edit CPU Assignments** window, where the current CPU assignment can be changed.

Designating Shared Physical CPUs on a Compute Host

You can designate one shared physical CPU per physical processor on a compute host to run low-load or non-realtime tasks for multiple VMs, freeing other cores on the host for dedicated high-load tasks. You can use the web administration interface or the CLI to set up shared physical CPUs.

To designate shared CPUs:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. *Lock the host* to make changes. Click **Edit Host** then select **Lock Host**.

   Wait for the host to be reported as Locked.
5. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
6. Click the **Processor** tab.
7. Click **Edit CPU Assignments**.

   This control is available only if the host is locked.
8. In the **Edit CPU Assignments** screen, use the **Shared Function** section to enable shared physical CPUs.

   You can designate one core on each physical processor for use as a shared physical CPU. The actual core is assigned from the pool of available cores for the processor.

   For example, to use a core on processor 0 as a shared physical CPU, set the # of Shared Physical Cores on Processor 0 to 1. Valid values are 1 (to assign a core as a shared physical CPU) or 0 (if a shared physical CPU is not required on the processor.)

To configure a VM to use a shared physical CPU, see Pinning a vCPU to a Shared Physical CPU.

To add or remove a shared physical CPU from the CLI, use a command of the following form:

```
system host-cpu-modify -f shared -p<processor> use_shared <hostname>
```

where:

- `processor` is the number of the physical processor (0 or 1)
- `use_shared` specifies whether to use a shared physical CPU (0 for no, 1 for yes)
- `hostname` is the name of the compute host

For example, to set up a shared physical CPU on processor 0 of compute-0:

~(keystone_admin)$ system host-cpu-modify -f shared -p0 1 compute-0

Viewing NUMA Node Resources on a Host

You can use the CLI to display the NUMA node resources for a host.

Host NUMA nodes can be pinned, or assigned for use by VMs.

For example, a VM can be configured to use NUMA node 0, so that when the VM is launched or migrated, the virtual machine scheduler locates a host node with an available NUMA node 0, and dedicates that NUMA node for use by the VM. For more about pinning NUMA nodes, see Pinning a Guest NUMA Node to a Host NUMA Node.

The resources of the pinned NUMA node, including the number of available CPUS and the available memory, must be sufficient to meet the requirements of the VM, which can be specified independently. For more about specifying NUMA node requirements for a VM, see Configuring the NUMA Node Allocations for a VM.

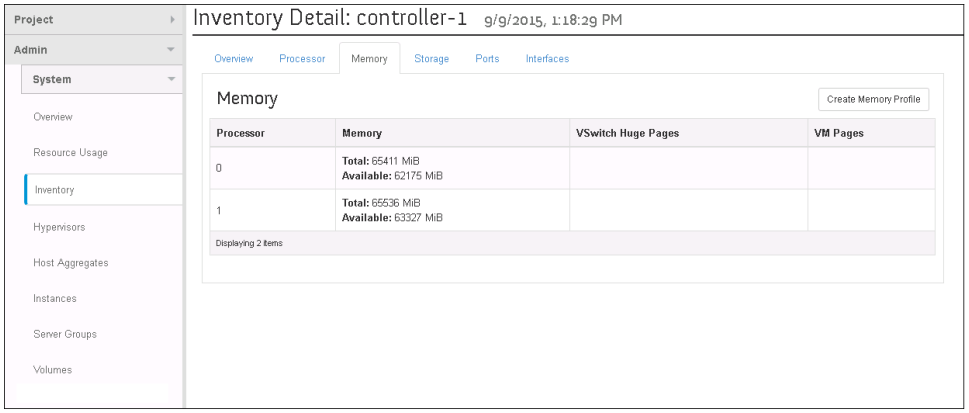
To ensure that a given host NUMA node can support the VM requirements, you can review the CPU and memory complements for host NUMA nodes.

To view the CPU complement for a NUMA Node (that is, for a socketed physical processor), use the vm-topology command.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Working with Host Memory Profiles

The **Memory** tab on the **Inventory Detail** page presents memory details for a host.



Note: This feature applies only to KVM region servers.

To view host memory information:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host

5. Click the **Memory** tab.

The information is presented in three columns, as follows:

- **Memory** - Overall memory on the host. For a controller node it displays the total and available memory figures.

  For a compute node, as in the example above, it displays the amount reserved for the platform (system software), and the total and available figures for use by virtual machines.
- **vSwitch Huge Pages** - This column is relevant on compute nodes only. The size of the huge pages, and the total and available huge page figures.
- **VM Huge Pages** - This column is relevant on compute nodes only. The size of the huge pages, and the total and available huge page figures.

Huge Page Provisioning

You can adjust the number and size of pages to allocate on a host for use as VM memory. For individual VMs, you can specify the page size to use.

In each NUMA node on a host, a fixed amount of memory is reserved for use by VMs. By default, this memory is managed using 2 MiB huge pages. You can change this for individual NUMA nodes to use a combination of 2 MiB and 1 GiB huge pages. Using larger pages can reduce page management overhead and improve system performancefor systems with large amounts of virtual memory and many running processes.

To calculate how many pages of each size you can successfully request, you can use the system host-memorylist and system host-memory-show commands to find out approximately how much memory is available for VMs. Additional memory not included in these totals may also be available.

If the huge page request cannot be allocated from the available memory, an informative message is displayed. If the available memory is greater than the amount required by the huge page request, the unallocated memory is not used for VMs, and is not available for other uses. After setting the memory allocations for a compute node, you can save them as a memory profile, and then apply the profile to other compute nodes. For more information, see [Creating and Using Memory Profiles]{#profiles}.

To specify the page size to use for a VM, see Specifying a Page Size for a VM on page 126.

You can edit the huge page attributes for a NUMA node from the web admin interface using the Memory tab on the Inventory pane.

Before requesting huge pages on a host, ensure that the host has enough available memory.

To provision huge memory:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. *Lock the host* to make changes. Click **Edit Host** then select **Lock Host**. Wait for the host to be reported as `Locked`.
5. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
6. Click the **Memory** tab.
7. Click **Update Hugepage Memory** and set the desired huge pages for each NUMA node.

   For each available NUMA node, two fields are supplied:

   ```
   # of VM 2M Hugepages Node n
   ```

   The number of 2MiB pages to reserve for VM use on the NUMA Node. If no 2MiB pages are required, type 0.

   ```
   # of VM 1G Hugepages Node n
   ```

   The number of 1GiB pages to reserve for VM use on the NUMA Node. If no 1GiB pages are required, type 0.
8. Click **Save**.

If there are insufficient resources to support the requested number of huge pages, a message appears. Review your calculations and submit a revised request.

9. *Unlock the host* and wait for it to be reported as `Available`.

You can edit the huge page attributes for a NUMA node from the CLI.

1. Lock the affected host.

```
system host-lock hostname
```

2. Use the following command to set the huge page attributes.

```
system host-hugepage-update <hostname> processor -2M <2Mpages> -1G
 <1Gpages>
```

where:

- `hostname` - the hostname or id of the compute node processor is the NUMA node of the compute node (0 or 1)
- `2Mpages` - if the optional -2M argument is included, the number of 2MiB huge pages to make available (if none, use 0).
- `1Gpages` - if the optional -1G argument is included number of 1GiB huge pages to make available (if none, use 0).

For example, to allocate four 2 MiB huge pages for use by VMs on NUMA node 1 of compute node compute-0 :

```
system host-hugepage-update compute-0 1 -2M 4
```

3. Unlock the host.

```
system host-unlock hostname
```

4. Wait for the host to be reported as available.

```
system host-list hostname
```

Creating and Using Memory Profiles

You can optionally save the huge pages configuration for a host as a profile, and apply the profile to other hosts.

For more information about huge page configurations, see [Huge Page Provisioning]{#huge}.

To create memory profiles:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of the host to open the **Inventory Detail** page for that host.
5. Click the **Memory** tab.
6. Click **Create Memory Profile**.
7. In the **Create Memory Profile** screen, enter a name for the memory profile.
8. Click **Create Memory Profile** to save the profile and close the dialog box.

You can use the following CLI command to create a memory profile:

```
    system memprofile-add <memoryprofile> <hostid>
```

where:

- `memoryprofile` is the name or UUID of the memory profile

- `hostid` is the name or UUID of the host from which to create the profile.

You can apply this profile to other hosts by editing the host settings in the web administration interface. For information about editing a host, see *Working with Hosts*

You can also use the following CLI command to apply a memory profile to a host:

```
system host-apply-memprofile <memoryprofile> <hostid>
```

where:

- `memoryprofile` is the name or UUID of the memory profile
- `hostid` is the name or UUID of the host.

To manage memory profiles, you can use the Memory Profiles tab on the System Inventory page, or you can use the following CLI commands:

- To list memory profiles:

  ```
  $ system memprofile-list
  ```

- To show details for a memory profile:

  ```
  system memprofile-show <memoryprofile>
  ```

  where `memoryprofile` is the name or UUID of the memory profile.
- To delete a memory profile:

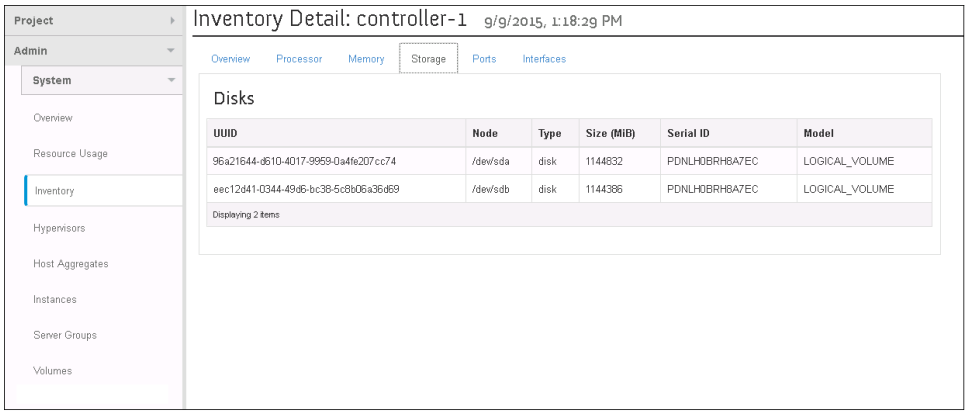
  ```
  system memprofile-delete <memoryprofile>
  ```

  where `memoryprofile` is the name or UUID of the memory profile.

Return to Top

HP Helion OpenStack® Carrier Grade 2.1 Beta: Working with Host Storage Profiles

The **Storage** tab on the **Inventory Detail** page presents storage details for a host.



Note: This feature applies only to KVM region servers.

This page contains the following:

- *Viewing storage details*
- *Managing Local Volume Groups*
- *Managing Physical Volumes*

Viewing storage details

To view host storage information:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of a host to open the **Inventory Detail** page for that host
5. Click the **Storage** tab.

The information is presented in one or more lists, as determined by the host type.

- Disks - This list is presented for all host types. It lists all available hardware devices used for storage. For each device, the following information is included:
  - UUID - The unique identifier for the device.
  - Node - The Linux device name.
  - Type - The type of storage device, typically a hard drive (disk).
  - Size - The capacity of the device in MiB.
  - Serial ID - The device's serial ID number.
  - Model - The manufacturer's model for the device.
- Storage Volumes - This list is presented for storage hosts. It shows a list of logical storage volumes defined on available disks. For each volume, the following information is included:
  - UUID - The unique identifier for the storage volume.
  - Name - The name assigned to the volume, if any.
  - Function - The type of storage backend handling the storage volume. The type OSD indicates that the storage volume is using the Ceph backend.

  For information about creating storage volumes or adding storage profiles, see the HP Helion OpenStack Carrier Grade Software Installation Guide: Creating Storage Volumes.
- Local Volume Groups - This list is presented for compute nodes. It shows groups that provide local storage for use by VMs. For more information, see *Managing Local Volume Groups*.

  For each group, the following information is provided:
  - Name - The name assigned to the local volume group.
  - State - The availability of the local volume group.
  - Access - The access status of the volume group (writeable, readonly, resizeable, exported, partial, or clustered).
  - Size - The capacity of the device in bytes.
  - Current Physical Volumes - The number of physical volumes that define the local volume group.
  - Current Logical Volumes - The number of logical volumes contained by the local volume group.
  - Actions - Available actions that can be performed on the local volume group.
- Physical Volumes - This list is presented for compute nodes. It shows physical volumes that provide local storage for use by VMs. For more information, see *Managing Physical Volumes*.

  For each group, the following information is provided:
  - Name - The device name associated with the physical volume.
  - State - The availability of the physical volume.
  - Type - The device type used for the physical volume.
  - Disk UUID - The unique identifier of the disk used to implement the physical volume.
  - Disk Device Node - The device used to implement the physical volume.
  - LVM Logical Group Name - The name of the local volume group to which the physical volume belongs.
  - Actions - Available actions that can be performed on the physical volume.

Managing Local Volume Groups

You can add, delete, and review local volume groups on a compute host.

Local volume groups are used to designate physical volumes on a compute host as local storage for use by VMs.

You can use the web administration or the CLI to manage them. For web administration interface instructions, see Configuring a Compute Host to Provide Local Storage.

Before you can modify the settings for a host, you must lock the host:

```
host-lock hostname
```

To configure a compute host to provide local storage for use by VMs, add a local volume group with the name novalocal.

The following CLI commands are available for managing local volume groups.

```
host-lvg-add hostname groucodeph
host-lvg-delete hostname nova-local
host-lvg-list hostname
host-lvg-show hostname
```

Where:

- `groucodeph` is the name of the local volume group to which the physical volume is added The only valid `groucodeph` is nova-local.
- where `hostname` is the name of the host system

To complete the configuration of a compute host for local storage, you must also add physical volumes to the `nova-local` local volume group. For more information, see *Managing Physical Volumes*.

Managing Physical Volumes

You can add, delete, and review physical volumes on a compute host.

Physical volumes provide storage using local disks. You can use the web administration or the CLI to manage them.

For web administration interface instructions, see Configuring a Compute Host to Provide Local Storage.

As each physical volume is created, it is added to an existing local volume group. Before you can modify the settings for a host, you must lock the host:

```
host-lock <hostname>
```

where `hostname` is the name of the host system

Before you can add a physical volume, a local volume group must exist on the host. To create one, see *Managing Local Volume Groups*.

The following CLI commands are available for managing physical volumes.

```
host-pv-add hostname <groucodeph> disk_uuid
```

where

- `groucodeph` is the name of the local volume group to which the physical volume is added
- `hostname` is the name of the host system

Note: The only valid group name is `nova-local`.

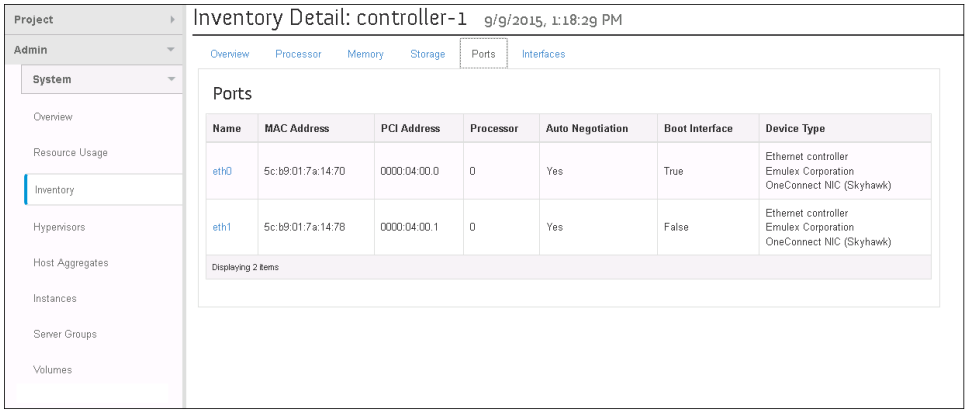
When disk_uuid indicates the root disk, the physical volume uses a system-designated partition on the root disk. For any other disk, the physical volume uses the entire disk.

```
host-pv-delete hostname nova-local disk_uuid
host-pv-list hostname
host-pv-show hostname
```

To configure VMs to use local storage, see Specifying Local Storage for a VM.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Port Details

The **Ports** tab on the **Inventory Detail** page presents information about the physical ports on a host.



Note: This feature applies only to KVM region servers.

Currently none of the port attributes is configurable; they are all read directly from the hardware.

To view the host ports:

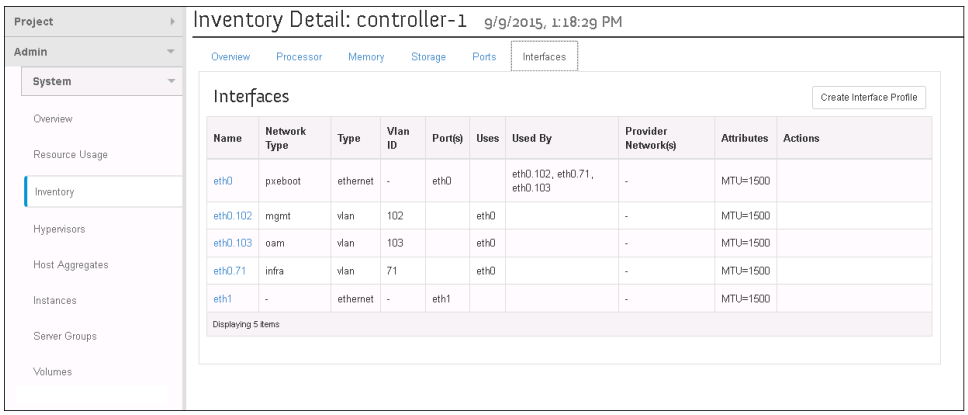
1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. *Lock the host* to make changes. Click **Edit Host** then select **Lock Host**. Wait for the host to be reported as `Locked`.
5. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
6. Click the **Ports** tab.

Port information is presented in several columns, as follows:

- Name - The name of the physical port, as identified by the host's Linux kernel.
- MAC Address - The port's unique MAC address.
- PCI Address - The port's unique address on the PCI bus. Together with the MAC address, this field can be used to uniquely identify a port on the host's hardware platform.
- Processor - The processor node that the port's IO controller is connected to.
- Auto Negotiation - The status of the Ethernet auto-negotiation flag. Currently, auto-negotiation is always enabled.
- Boot Interface - The boot flag, whether or not PXE booting is enabled.
- Device Type - Hardware information about the port type, manufacturer, and model.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Working with Host Interface Profiles

The **Interfaces** tab on the **Inventory Detail** page presents details about the logical L2 network interfaces on a node, as illustrated below for an unlocked controller node.



Note: This feature applies only to KVM region servers.

On a properly configured compute node, the Interfaces tab presents additional logical interfaces, for a locked node.

This topic covers the following:

- *Viewing interface details*
- *Creating an Interface Profile*
- *Creating a new interface*
- *Editing Interface Details*

Viewing interface details

To view host interface information:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of the host to open the **Inventory Detail** page for that host.
5. Click the **Interfaces** tab.

Information about interfaces is presented in several columns, as follows:

- **Name** - The name given to the logical L2 interface.
- **Network Type** - The type of network the logical network interface is connected to. The options are:
  - **data** for a compute node data interface
  - **infra** for the optional infrastructure network
  - **mgmt** for the internal management network
  - **oam** for the OAM network
  - **pci-passthrough** for a PCI passthrough interface
- **Type** - Ethernet, or aggregated Ethernet (LAG).
- **Vlan ID** - The VLAN ID of the network listed in the Network Type column, if the network uses a shared interface. For more information about shared interfaces, see Shared (VLAN) Ethernet Interfaces.
- **Port(s)** - The physical ports on top of which the logical interface is built. Multiple ports are displayed when the logical interface uses LAG.
- **Uses** - The interface used by the network listed in the Network Type column, if the network uses a shared interface. The VLAN ID of the network is shown in the Vlan ID field.
- **Used By** - The networks that share the interface using VLAN tagging, if the interface is shared. For more information about shared interfaces, see Shared (VLAN) Ethernet Interfaces.
- **Provider Networks** - This option is relevant for compute nodes only, and for interfaces of the data network type. It lists the provider networks associated with the data interface.
- **Attributes** The current MTU size for the interface.

- **Actions** - On a locked node, you can modify a logical interface, and execute management operations on it. This is implemented using the buttons Edit Interface and More. These buttons are not available when the node is unlocked.

Creating an Interface Profile

You can create a new interface profile out of the currently defined node interfaces.

To create a host interface profile:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. In the **Host Name** column, click the name of the host to open the **Inventory Detail** page for that host.
5. Click the **Interfaces** tab.
6. Click **Create Interface Profile**.
7. Enter a name for the new profile.

   Available interface profiles are listed, and can be removed, from the System Inventory page, as described in *Working with Hardware Profiles*.
8. Click **Create Interface Profile** to create the profile based on the interface and port configuration of the selected host.

Creating a new interface

You can create new logical interfaces.

To create a host interface:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. *Lock the host* to make changes. Click **Edit Host** then select **Lock Host**. Wait for the host to be reported as `Locked`.
5. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
6. Click the **Interfaces** tab.
7. Click **Create Interface**.

   This button is available only on nodes in the locked state.
8. Specify the following in the **Create Interface** screen:
   - **Interface Name** - Enter the name to be assigned to the new logical interface.
   - **Interface Type** - Select the type of network interface: Ethernet or aggregated Ethernet (LAG).
   - **Ports** - Select the physical ports for the new logical interface. Physical ports already allocated to other interfaces are not listed.
   - **Network Type** - Select the type of network to attach the new logical interface to (`data` or `infra`, for compute node data interfaces and infrastructure network connections respectively). Note that connections to the OAM and internal management networks are auto-provisioned during the software installation process.
   - **Provider Network(s)** - Select one or more provider networks for the new logical interface, for networks of type data. Provider networks already allocated to other data interfaces are not listed, since no provider network can be associated with more than a single data interface.
   - **MTU** - Enter the MTU size in bytes for the interface. For compute nodes, values between 1500 and 9000 are supported. For controller and storage nodes, the MTU size cannot exceed 1500.
9. Click **Create Interface**.

Note: Logical interfaces of network types `oam` and `mgmt` cannot be deleted. They can only be *modified to use different physical ports* when required.

Editing Interface Details

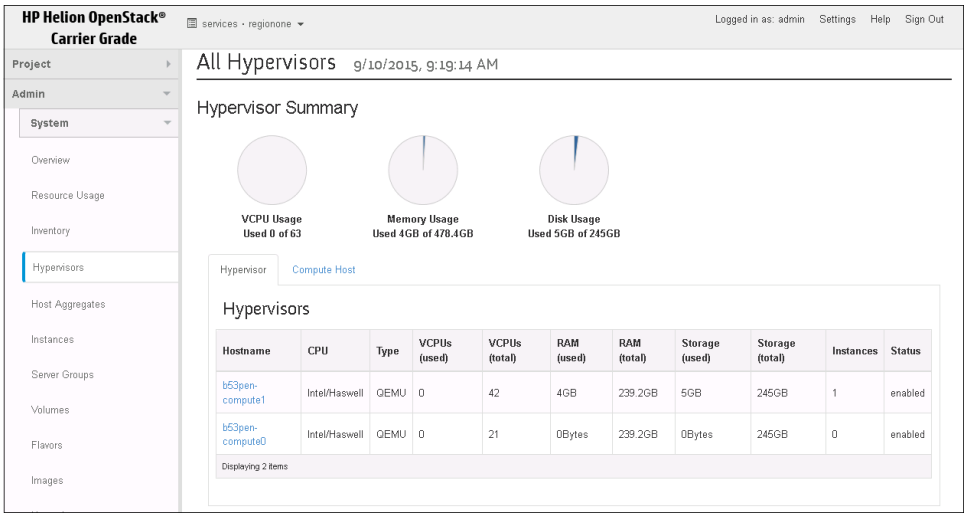
You can edit existing logical interfaces.

To edit a host interface:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab.
4. *Lock the host* to make changes. Click **Edit Host** then select **Lock Host**. Wait for the host to be reported as `Locked`.
5. In the **Host Name** column, click the name of the locked host to open the **Inventory Detail** page for that host.
6. For the interface to change, click **More** then **Edit**.
7. In the **Edit Interface** screen, make changes to the fields, as described in *Creating a new interface details*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Hypervisors

Hypervisors are the compents in HP Helion OpenStack Carrier Grade that creates and runs virtual machines.



To view charts for monitoring hypervisor resource usage on compute nodes:

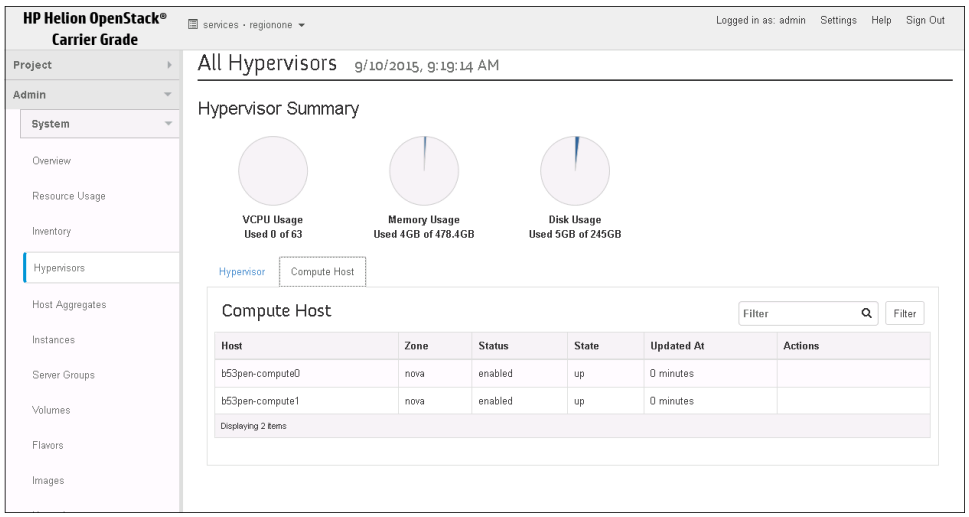
1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Hypervisors** tab.

For each hypervisor, the following information is displayed:

- CPU Type
- VCPUs (used)
- VCPUs (total)
- RAM (used)
- RAM (total)
- Storage (used)
- Storage (total)
- Instances
- Status

Compute Hosts

Click the **Compute Hosts** table to view information on the hosts.

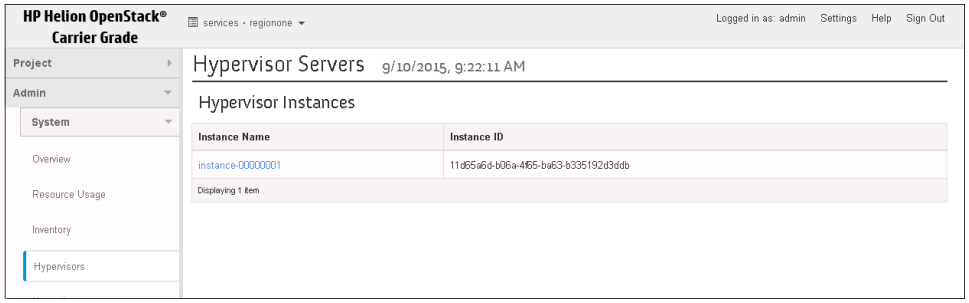


The following infromation appears for each host:

- Zone
- Status
- State
- Updated At
- Actions

Hypervisor Instances

Click the name of a hypervisor to view instances associated with that hypervisor.



In the Hypervisor Instances list, click an instance to see *Instance Details*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Baremetal

You can use HP Helion OpenStack to manage the baremetal region.

As an admin, you can use the dashboards to:

Turn on and off baremetal nodes

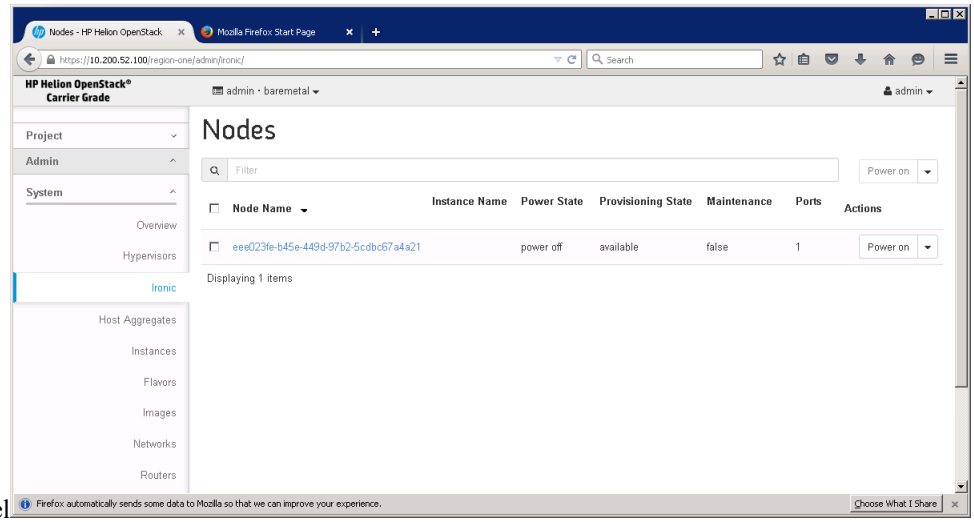
Place nodes in maintenance mode

View node details

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate project* and the `baremetal` region.

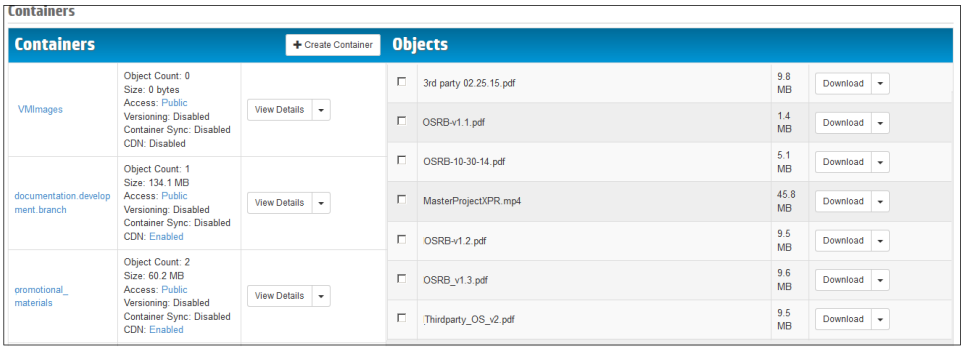
Note: The baremetal region appears for Sacramento deployments only.

3. Click the **System** dashboard, then the **Ironic** panel



HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Object Storage

With object store, objects and files are written to multiple disk drives spread throughout servers in the data center, with the Helion software responsible for ensuring data replication and integrity across the cluster.



You can use the dashboards to create and configure container store instances and move files in and out of store.

How you interact with these store instance depends upon your user type, either an administrative user (admin) or a non-administrative user (user).

Note: The administrative user can perform all of the user tasks in addition to the admin tasks, such as setting a quota for volumes.

Managing object storage as a user

As a user, you can work with any object storage container associated with the active project.

- *Create and delete a container*
- *Upload an object into or download an object from a container*
- *Edit and delete an object in a container*

Managing object storage as an admin

As an admin user, you can work on all of the objects in your domain, regardless of which project the object is associated with.

Access the admin object commands using the **Object Store** panel on the **Project** dashboard.

There are no additional tasks available to the admin user.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating and Deleting Containers

A container is a storage compartment for your data and provides a way for you to organize your data. You can think of a container as a folder in Windows® or a directory in UNIX®. The primary difference between a container and these other file system concepts is that containers cannot be nested. You can, however, create an unlimited number of containers within your account. Data must be stored in a container so you must have at least one container defined in your account prior to uploading data.

Create a container

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Project** dashboard, then the **Object Store** panel, then the **Containers** tab.
4. In the **Create Container** dialog box, enter a name for the container, set the access level and then click **Create Container**.

   Note: A Public Container will allow anyone with the Public URL to gain access to your objects in the container.

Delete a container

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Project** dashboard, then the **Object Store** panel, then the **Containers** tab.
4. From the **More** drop-down list next to a container, select **Delete container**
5. The **Delete Container** dialog box will appear.
6. Click **Delete Container** to confirm. The container and all objects stored within it will be permanently deleted.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Uploading and Downloading Objects

An object is the basic storage entity that represents a file you store in the OpenStack Object Storage system. When you upload data to OpenStack Object Storage, the data is stored as-is (no compression or encryption) and consists of a location (container), the object's name, and any metadata consisting of key/value pairs

Uploading an object into a container

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Project** dashboard, then the **Object Store** panel, then the **Containers** tab.
4. Select the container in which you want to store your object.
5. Click **Upload Object**.
6. The **Upload Object To Container: <name>** dialog box is displayed. <name> is the name of the container to which you are uploading the object.
7. Enter a name for the object.
8. Browse to and select the file that you want to upload.
9. Click **Upload Object** to confirm.

Downloading objects from a container

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Project** dashboard, then the **Object Store** panel, then the **Containers** tab.
4. Select the container from which you want to download the object.
5. Click **Download** next to the object to download the file to your local drive.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Editing and Deleting Objects

An object is the basic storage entity that represents a file you store in the Openstack® Object Storage system. When you upload data to Openstack® Object Storage, the data is stored as-is (no compression or encryption) and consists of a location (container), the object's name, and any metadata consisting of key/value pairs

Edit an object in a container

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Project** dashboard, then the **Object Store** panel, then the **Containers** tab.
4. Select the container in which you want to store your object.
5. From the **More** drop-down list, choose **Edit**.
6. The **Edit Object** dialog box is displayed.
7. Browse to and select the file that you want to upload.
8. Click **Update Object** to confirm.

Delete an object from a container

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Project** dashboard, then the **Object Store** panel, then the **Containers** tab.
4. Select the container from which you want to delete the object.
5. From the **More** drop-down list next to an object, choose **Delete Object**.
6. The **Confirm Delete Object** dialog box is displayed.
7. Click **Delete Object** to confirm.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Using Stacks

A collection of resources created and managed using the Orchestration (Heat) service is called a service (also known as a stack).

Service resources can be flavors, images, instances, tenant networks, volumes, security groups, users, floating IP addresses, or any other entities defined and configured in templates. Most types of resources offered by HP Helion OpenStack Carrier Grade can be defined in templates and included in services.

See the following topics on using stacks:

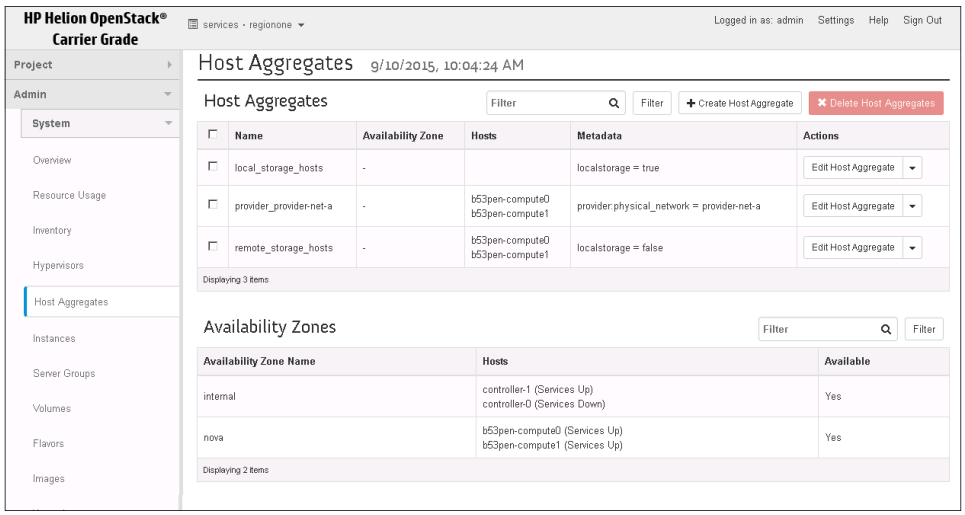
- *Creating a Stack*

For information on peforming the following tasks related to Orchestration stacks, see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

- Customizing Guest Images with User Data
- Resource Scaling (Autoscaling)
- Reporting a Guest Metric
- Sample Templates for HP Helion OpenStack Carrier Grade
- Supported Heat Resource Types

HP Helion OpenStack® Carrier Grade 2.1 Beta: Working with Host Aggregates

Host aggregates are collections of hosts that share common attributes for the purposes of VM scheduling.



To view host aggregates, open the Host Aggregates page from the Admin menu.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Host Aggregates** tab.

When the Nova Scheduler selects a compute node to instantiate a VM, it can use host aggregates to narrow the selection.

For example:

- If the VM requires local storage, the Nova scheduler selects a host from the `local_storage_hosts` host aggregate.
- Or, if the VM requires remote storage, the scheduler selects from the `remote_storage_hosts` host aggregate. This ensures that the instance is instantiated on a host that meets the requirements of the VM.

The Nova scheduler does not always use host aggregates. For example, if a VM does not specify either local or remote storage, the Nova scheduler can instantiate it on any resource.

Some host aggregates are managed automatically by HP Helion OpenStack Carrier Grade.

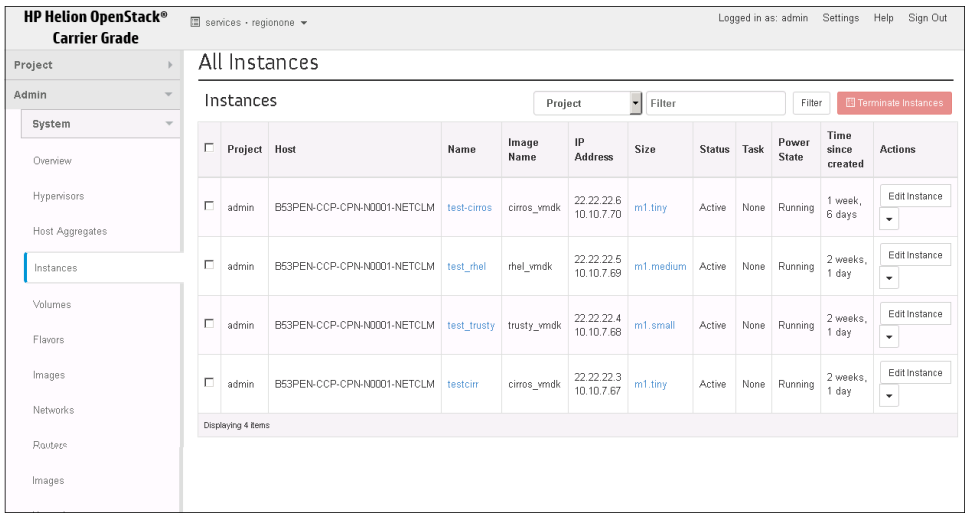
Caution: Do not make manual changes to host aggregates that are managed automatically.

The `local_storage_hosts` and `remote_storage_hosts` memberships are updated automatically whenever a local volume group is added or removed on a compute host. For more information, see Configuring a Compute Host to Provide Local Storage.

You can use host aggregates to meet special requirements. For example, you can create a pool of compute hosts to offer dedicated resources such as pinned NUMA nodes or specific huge page sizes, while grouping the remaining compute hosts to offer shared resources.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Virtual Machine Instances

You can use the dashboards to manage instances created by other users.



Use the **Compute** panel on the **Project** dashboard to:

- *Create a new instance*
- *Terminate an instance*
- *Reboot an instance*
- *Rebuild an instance*
- *Suspend and resume an instance*
- *Pause and resume an instance*
- *Create an instance snapshot*

You can also *associate, or assign, a floating IP address* to an instance. A floating IP address makes the instance available on the external network.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating Virtual Machine Instances

Instances are virtual machines that run inside the cloud.

You can launch an instance from the following sources:

- Images uploaded to the Image Service.
- Image that you have copied to a persistent volume.

Create an instance

To create an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** table, click **Launch Instance**.

   The Launch Instance dialog box opens, with five tabs: **Details**, **Access and Security**, **Networking**, **Post Creation**, and **Advanced Options**. By default, **Details** is the active tab.
5. On the **Details** tab, perform the following tasks:
   - From the **Availability Zone** list, select the AZ this instance will be associated with.
   - In the **Instance Name** field, enter the name for the instance.
   - From the **Flavor** list select the flavor.
   - In the **Instance Count** field, enter the number of instances required.
   - From the **Instance Boot Source** list, select the source to create the image from:

- Image -- create an image from an existing image
- Snapshot -- create an image from an existing snapshot
- Volume -- create an image from an existing volume
- Image (create new volume) -- create an image from an existing image and create a new volume
- Volume snapshot (create new volume) -- create an image from an existing snapshot and create a new volume

- Select the volume, snapshot, or image from the list that appears.

  Additonal fields appear for the boot source option that create a new volume. For more information, refer to *Managing Block Storage Volumes*

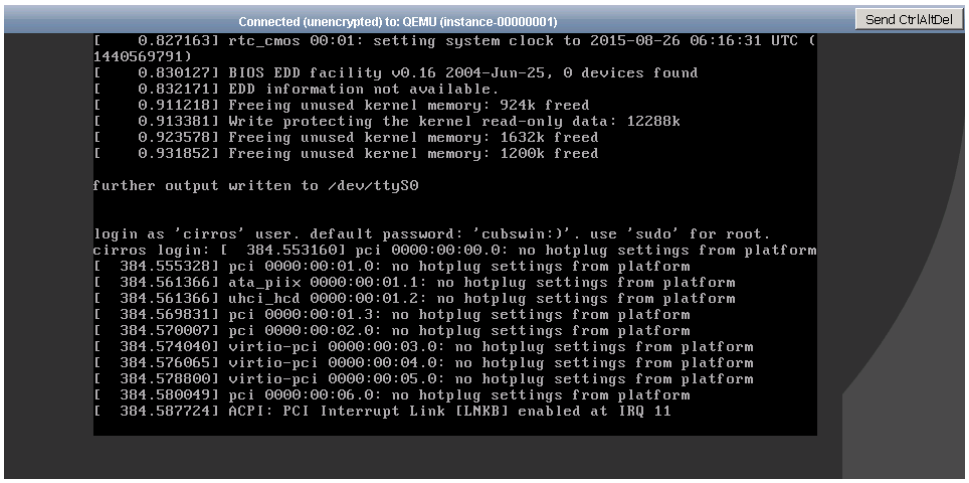
6. On the **Access & Security** tab, perform the following tasks:.
   - From the **Keypair** list, select the **keypair** to use with the instance.
   - Select the security group to use with the instance.
7. On the **Networking** tab, from the **Available Networks** list, select the required network. The network is displayed in the **Selected Networks** box.
8. On the **Post-Creation** tab, optionally, enter a script to pass user data to the instance at launch time.

   For more details, refer to the OpenStack documentation, such as *Configure instances at boot*.
9. On the **Advanced Options** tab, select either **Automatic** or **Manual** in the **Disc Partition** list

   Selecting **Automatic** will resize the partitions on boot to match the size requested by the user. If you select **Manual**, you will need to manually resize the partitions, after the instance boots.
10. Click **Launch** to launch the instance.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Launching a Virtual Machine Console

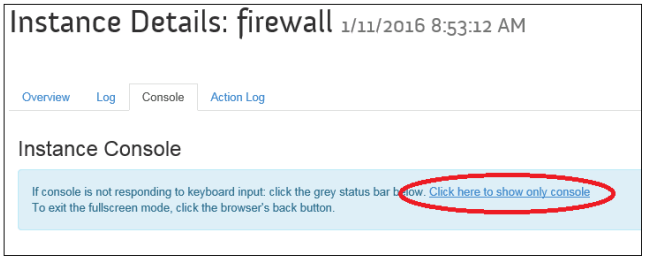
You can launch a console session to a virtual machine directly through the Horizon interface.



To launch a console:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** table, for the instance you want to pause, click **Edit Instance** then **Console**.

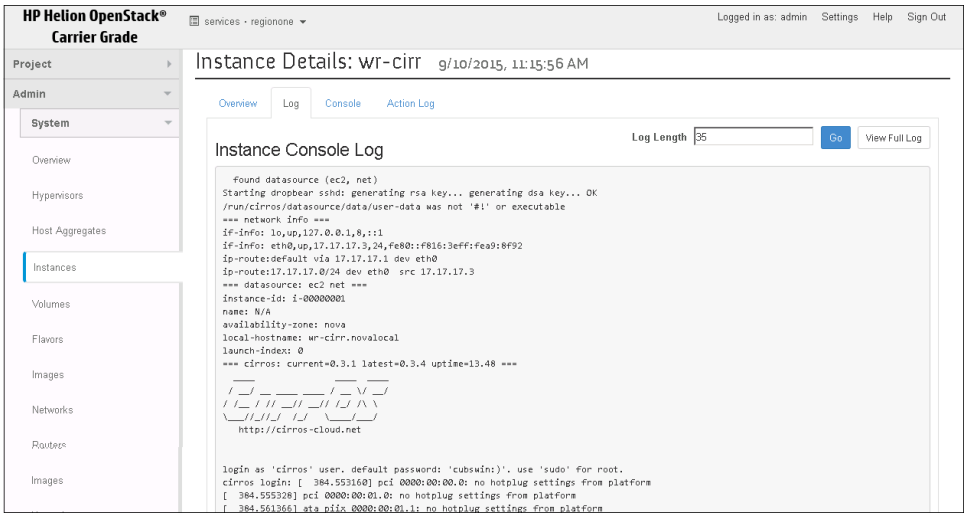
   Note that most browsers block a console session by default. Click the **Click here to show only console** link or configure the browser to allow blocked content.



To exit the full-screen mode, click the browser's back button. Note that you might return to the **Project** dashboard after the console window closes.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing a Virtual Machine Log

You can launch the console log for a virtual machine instance directly through the Horizon interface.



To pause an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** table, for the instance you want to pause, click **Edit Instance** then **Log**.

   Console logs can be viewed directly on compute server at `/var/lib/nova/instances/<instance_id>/console.log`.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Pausing and Un-pausing Instances

When a user *pauses* an instance, the instance remains running, but, in a frozen state. The contents of the instance are stored in memory (RAM). Memory and vCPUs are not released.

Users can suspend an instance, for example, in order to make a back up of an instance to prevent the instance from being used during the process.

Note: Pausing is different from *suspending an instance*. Suspending stops the instance, stores the contents on the disk. the memory and vCPUs become available to create other instances.

Pause an instance

To pause an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** table, for the instance you want to pause, click **Edit Instance > Pause Instance**.

The status of the instance reports *Paused*.

Note that many of the commands on the **More** menu are not available for a paused instance.

Un-pause an instance

To unpause an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** table, for the instance you want to unpause, click **Edit Instance > Unpause Instance**.

   Note that all of the commands on the **More** menu are available.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Rebooting Instances

You can soft or hard reboot a running instance.

With a soft reboot, the operating system is signaled to restart, which allows for a graceful shutdown of all processes. A hard reboot is the equivalent of power cycling the server.

Reboot an instance

To rebooot an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** table, for the instance you want to reboot, click **Edit Instance** then **Soft Reboot Instance** or **Hard Reboot Instance**.

   In the confirmation screen, click **Reboot Instance** to reboot.

   The progress of the reboot is displayed in the **Task** column on the **Instances** screen.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Rebuilding Instances

The rebuild operation removes all data on the server and replaces it with the specified image.

A rebuild operation always removes data injected into the file system through server personality. You can reinsert data into the file system during the rebuild.

Rebuilding an instance

To rebuild an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:

- Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
- Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.

4. In the **Instances** table, for the instance you want to rebuild, click **Edit Instance** then **Rebuild Instance**.
5. In the **Rebuild Instances** screen:
   - Select the image to use to rebuild the instance. You can select the same image or rebuild using a different image.
   - Specify whether the instance will automatically partition, based on the image, or you will manually partition the instance.
6. In the confirmation screen, click **Rebuild Instance**.

   The progress of the reboot is displayed in the **Task** column on the **Instances** screen.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating an Instance Snapshot

A snapshot is a new image based on a running instance. That snapshot can be used as the base for new instances.

Creating a snapshot

To create a snapshot:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** table, for the instance you want to rebuild, click **Edit Instance** then **Create Snapshot**.
5. On the **Create Snapshot** tab, enter a name for the snapshot.
6. Click **Create Snapshot** to launch the instance.

   A snapshot image is created on *the **Images** list*.

You can *make the snapshot public*for use in all projects in the domain and you can *protect the image*from being deleted.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Suspending and Resuming Instances

When a user *suspends* an instance, the contents of the instance are stored on disk and the instance is stopped. Suspending an instance is similar to placing a device in hibernation; memory and vCPUs become available to create other instances.

Users can suspend an instance, for example, to free up the resources used by an instance that is used infrequently or to perform system maintenance.

Note: Suspending is different from *pausing an instance*. Pausing keeps the instance running, (in a "frozen" state) and stores the content of the instance in memory (RAM).

Suspend an instance

To suspend an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** screen, for the instance you want to suspend, click **Edit Instance** then **Suspend Instance**.

   The status of the instance reports *Suspended*.

Resume an instance

To resume an instance:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** screen, for the instance you want to resume, click **Edit Instance** then **Resume Instance**.

   The status of the instance reports *Running*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Terminating Instances

You can terminate an instance, as needed.

Terminate an instance

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Instances** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Instances** tab.
4. In the **Instances** screen, for the instance you want to terminate, click **Edit Instance** then **Terminate Instance**.

   In the confirmation screen that appears, click **Terminate Instance**.

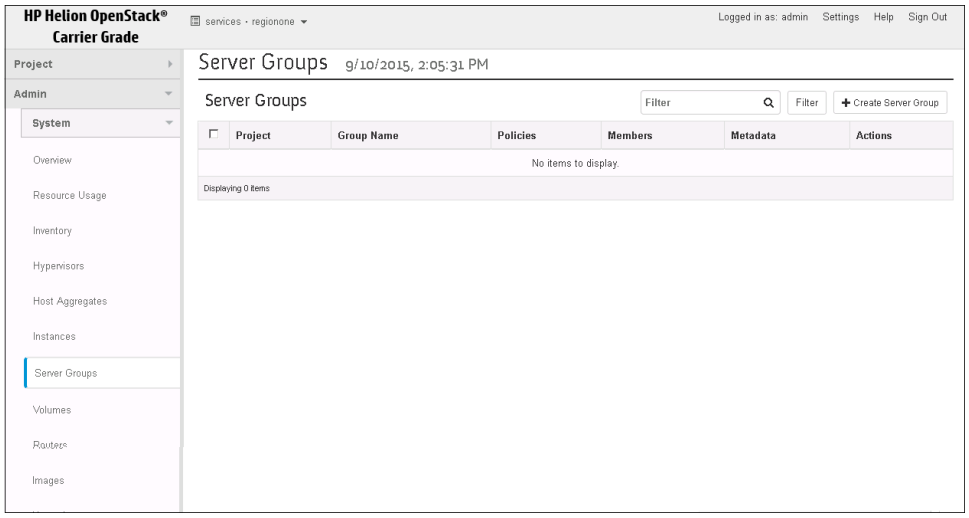
   The instance is terminated and no longer appears in the instance list.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Server Groups

From the Titanium Server Admin Guide

Server Groups is a mechanism to group virtual machines to which a common set of attributes is applied.

Note: This feature applies only to KVM region servers.



To create a server group:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Server Groups** tab.

4. In the **Server Group** table, click **Create Server Group**.
5. In the **Create Server Group** dialog, specify the following information:
   - **Project** Select a project to associate the server group.
   - **Server Group Name** Specify a name for the new server group.
   - **Policy** Select a scheduling policy:
     - **affinity**. When this option is selected, new instances launched as part of this server group are scheduled to run on the same compute node.
     - **anti-affinity**. When this option is selected, new instances launched as part of this server group are scheduled to run on different compute nodes. For example, you can use the anti-affinity option when you have two virtual machines that run in 1:1 HA protection mode, and you want them to be protected against hardware failures.
   - **Best Effort**. Select this option to enforce the policy in place, affinity, or anti-affinity, on a best-effort basis. If for any reason the policy cannot be enforced, then the deployment of the new instance proceeds using the regular scheduling. When cleared, the policy in place must be executable for the new instance to be scheduled. Launching of a new virtual machine fails if there are no resources to comply with the selected policy.
   - **Max Group Size (Instances)**. Determines the maximum number of instances that can co-exist as part of this server group.
6. Click **Create Server Group**.

You can add instance to a server group as you *create the instance*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Block Storage Volumes

Volumes are block storage devices that allow you to expand the storage capacity of an instance. Volumes may only be attached to one server at a time, and will retain data, even when not attached to an instance.

You can create and configure volumes; create snapshots of volumes; update the metadata associated with a volume, extend volumes, and transfer a volume between users, and attach and detach volumes from instances.

You can work with any volume associated with the active project.

- *Create, edit and delete a volume*
- *Create and delete a snapshot from a volume*
- *Extend the size of a volume*
- *Attach a volume to a VM instance and detach a volume from VM instance*
- *Creating and deleting a volume type*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating, Editing, and Deleting Volumes

Volumes are block devices that can be attached to instances.

Create a volume

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. Click **Create Volume**.
5. In the **Create Volume** dialog box, enter the relevant information for the volume:
   - **Volume Name:** Enter a name for the volume
   - **Description:** Provide a brief description (optional).
   - **Type:** Leave this field blank
   - **Size:** Enter the size of the volume in gigabytes
   - **Volume Source:** Select one of the following options:

    - No source, empty volume - creates an empty volume and does not contain a file system or a partition table
    - Image - a new field for Use image as a source displays. You can select the image from the list.
  - **Availability Zone:** Select the availability zone. By default, this value is set to 'any availability zone'.
6. Click **Create Volume** to confirm.

Edit a volume

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. Under the **Actions** column, click **Edit Volume**, next to the volume you want to edit. .
5. In the **Edit Volume** dialog box, modify the name and description.
6. Click **Edit Volume** to confirm.

> **Note:** You can *extend a volume* by using the **Extend Volume** option available in the **More** drop-down list and entering the new value for volume size.

Delete a volume

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. Select the volume(s) that you want to delete.
5. Click **Delete Volume** to confirm.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating and Deleting a Volume Types

A volume type defines the characteristics of a volume. It usually maps to a set of capabilities of the storage back-end driver that is used for this volume. For example: *Backup*,*SSD*, and so forth.

Create a volume type

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. In the **Volume Types** section of the table, click **Create Volume Type**.
5. In the **Create Volume Type** dialog box, enter a name for the volume type.
6. Click **Create Volume Type** to confirm.

Delete a volume type

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. In the **Volume Types** section of the table, select the volume type or types that you want to delete.

5. Click **Delete Volume Types**.
6. In the **Confirm Delete Volume Types** dialog box, click **Delete Volume Types**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Attaching and Detaching Volume Instances

After you've created one or more volumes, you can attach them to instances, one instance at a time.

Attach a volume to an instance

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. Select the volume to add to an instance and click **Edit Attachments**.
5. In the **Manage Volume Attachments** dialog box, select an instance.
6. Enter the name of the device from which the volume is accessible by the instance.

   Note: The actual device name might differ from the volume name because of hypervisor settings.
7. Click **Attach Volume**.

The dashboard shows the instance to which the volume is now attached and the device name. You can view the status of a volume in the Volumes tab of the dashboard. The volume is either Available or In-use. Now you can log in to the instance and mount, format, and use the disk.

Detach a volume from a VM instance

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. Select the volume you want to detach and click **Edit Attachments**.
5. Click **Detach Volume** to confirm your changes.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Extending the Size of a Volume

You can extend the size of a volume, as needed.

Extend a volume

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.
4. From the **Edit Volume** list on the volume you want to extend, select **Extend Volume**.
5. In the **Extend Volume** dialog box, select the size from the drop-down and click **Extend Volume** to confirm.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Compute Flavors

Compute flavors are machine configurations that describe the amount of memory, number of CPUs, and storage capacity of instances. The moment you register a chassis, a flavor is created by default. You can use the default flavor or create a flavor of your choice.

An admin user can create, edit, and delete instances as needed.

- *Create a flavor*
- *Edit a flavor*
- *Delete a flavor*

Create a flavor

To create a flavor:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Flavors** tab.
4. Click **Create Flavor**.
5. In the **Create Flavor** screen, click the **Flavor Info** tab (should be active).
6. Enter the name that you want to assign to the flavor.
   - In the **ID** field, enter a unique string that identifies this flavor.
   - In the **VCPUs** field, enter the required number of virtual CPUs to be included in the flavor.
   - In the **RAM MB** field, enter the virtual machine memory in megabytes to be included in the flavor.
   - In the **Root Disk GB** field, enter the size for the virtual root disk size in gigabytes.
   - From the **Ephemeral disk GB** field, enter the size of a secondary ephemeral data disk in gigabytes. This is an empty, unformatted disk and exists only for the life of the instance.
   - From the **Swap Disk MB** field, enter the amount of swap space allocation for the flavor.
7. Click the **Flavor Access** tab.
8. Add the flavor to a project by clicking the + icon next to each project in the **All Projects** column.

   By default, no project is specified as having access the flavor. If none is specified, all projects can access the flavor.
9. Click **Create Flavor** to create a new the flavor.

   A message is displayed on successful creation.

Edit a flavor

To edit a flavor:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Flavors** tab.

   The flavors in the domain are listed.
4. For the flavor you want to modify, click **Edit Flavor**.
5. In the **Edit Flavor** screen, click the **Flavor Info** tab .
6. Use the **Flavor Info** and **Flavor Access** tabs to modify the flavor as needed. See *Create a flavor* for a description of each field.
7. When done editing, click **Save**.

A message is displayed on successful edit.

Delete a flavor

Instances that use the flavor are not affected when a flavor is deleted.

To delete a flavor:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Flavors** tab.

   The flavors in the domain are listed.

4. For the flavor you want to modify, click **More > Delete Flavor**.
5. In the confirmation screen, click **Delete Flavor**.

A message is displayed on successful delete.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing access to a flavor

Compute flavors are machine configurations that describe the amount of memory, number of CPUs, and storage capacity of instances.

As an admin, you can *allow specific projects to have access to a flavor* or *prevent a project from accessing a flavor*.

Allowing a project to access a flavor

1. *Launch the HPE Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Flavors** tab.

   The flavors in the domain are listed.
4. For the flavor you want to modify, click **More > Modify Access**.
5. Click the + icon next to a project in the **All Projects** column to allow the project to access the flavor.

   By default, no project is specified as having access the flavor. If none is specified, all projects can access the flavor.
6. Click **Save** to create a new the flavor.

   A message is displayed on successful change.

Preventing a project from accessing a flavor

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Flavors** tab.

   The flavors in the domain are listed.
4. For the flavor you want to modify, click **More > Modify Access**.
5. Click the **-** icon next to a project in the **Selected projects** column to remove the flavor from the project.

   By default, no project is specified as having access the flavor. If none is specified, all projects can access the flavor.
6. Click **Save** to create a new the flavor.

   A message is displayed on successful change.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Images

A virtual machine image is a single file that contains a virtual disk with a bootable operating system installed on it. You can use images to create virtual machine instances within the cloud.

To create an image, you upload an ISO image file. After you upload an image, it is considered golden and you cannot change it.

You can use the dashboards to create and configure private virtual machine images, which can be used to create instances.

Note: You can also *create an image based on an instance*, which is called a *snapshot*.

How you interact with these images depends upon your user type, either an administrative user (admin) or a non-administrative user (user).

Note: The admin can perform all of the user tasks in addition to the admin tasks.

Managing images as a user

As a user, you can work with any *private* images associated with the active project.

Access the image commands using the Compute panel on the Project dashboard.

Click **Images** to perform the following tasks:

- *Create and delete images*
- *Modify images*
- *View image details*
- *Protect an image or snapshot from being edited*

Managing images as an admin

As an admin user, you can work on all of the images in your domain, regardless of which project the image is associated with.

Access the admin image commands using the System Panel on the Admin dashboard.

As an admin, you can determine if the snapshot is available only in the current project or to all projects in the domain.

- *Make an image or snapshot public*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating and Deleting Images

You can create and delete virthal machine images as needed.

- *Create an image*
- *Delete an image*

Create an image

Creating a new image for use in HP Helion OpenStack requires two general steps.

The first step is to create an ISO image file outside of your HP Helion OpenStack

When the ISO image file is complete and ready for use, you use HP Helion OpenStack to upload the image to your cloud.

Note: After you upload an image, it is considered *golden* and you cannot change it.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.

   The available images are listed.
4. In the **Images** table, click **Create Image**.
5. In the **Create an Image** screen, provide the image information:
   - **Name** - Enter a name for the image.
   - **Description** - Optionally, enter a brief description of the image.
   - **Image Source** - Choose the image source from the list. Your choices are Image Location and Image File.
   - **Image File or Image Location** - Based on your selection for Image Source, you either enter the location URL of the image in the Image Location field. or browse to the image file on your system and add it.

     Note: The Image Location field must be a valid and direct URL to the image binary. URLs that redirect or serve error pages will result in unusable images.
   - **Format** - Select the correct format (for example, QCOW2) for the image.
   - **Architecture** - Specify the architecture. For example, i386 for a 32-bit architecture or x86-64 for a 64-bit architecture.

- **Minimum Disk** - Enter the minimum disk size required to boot the image. Leave the field blank to specify no minimum.
- **Minimum RAM (MB)** - Enter the minimum memory size required to boot the image. Leave the field blank to specify no minimum.
- **Public** - Select this option to make the image public to all users with access to the current project. Leave the option clear to allow the image to be used in all projects in the domain.
- **Protected** - Select this option to prevent the image from being deleted. Leave the option clear to allow the image to be deleted.

6. Click **Create Image** to launch the image.
7. Optionally, you can click **Launch** to *create a running instance* based on this image.

Delete an image

You can delete images, as needed. A deleted image is no longer available. Any instances launched from the deleted instance are not affected.

To delete a private image:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.

   The available images are listed.
4. In the **Images** screen, click the check box next to the image name you want to delete. To select all images, click the check box next to **Image Name** the top row of the image list.
5. Click **Delete** to delete the image.
6. The image is no longer available. Any instances launched from the deleted instance are not affected.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Modifying Images

You can modify images, as needed, to change the name and description of the image, or protect and un-protect the image.

Modify an image

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.

   The available images are listed.
4. In the **Images** screen, click **More** then click **Edit** next to the image you want to modify.
5. Update the image information:
   - **Name** - Enter a name for the image.
   - **Description** - Optionally, enter a brief description of the image.
   - **Protected** - Select this option to prevent the image from being deleted. Leave the option clear to allow the image to be deleted.

   Note: Fields that cannot be modified are shaded.

5, When complete, click **Update Image**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Image Details

To view image details:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.

   The available images are listed.
4. Click the name of the image.

   Note: When your cursor is on the image name, the name is underlined.
5. The Image Details screen shows detailed information about the image, including:
   - name and ID
   - status
   - creation and modification date(s)
   - size
   - formats
   - size

HP Helion OpenStack® Carrier Grade 2.1 Beta: Protecting Images

A virtual machine image is a single file that contains a virtual disk with a bootable operating system installed on it. You can use images to create virtual machine instances within the cloud.

If you want to prevent an image from being deleted, you can make that image *protected*.

Protect an image

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.

   The available images are listed.
4. In the **Images** screen, for the image you want to protect, click **Edit Image**, then **Edit**.
5. In the **Update Image** screen, select **Protected**.
6. Click **Update Image**.

The image is protected and the **Delete Image** command is removed from the **More** menu.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Making an Image Public

When you*create an image* or an *image snapshot*, as an admin, you can determine if the snapshot is available only in the current project or to all projects in the domain.

Make an image public

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Volumes** tab.
   - Click the **Project** dashboard, then the **Compute** panel, then the **Volumes** tab.

   The available images are listed.
4. In the **Images** screen, for the image you want to protect, click **Edit Image**, then **Edit**.

5. In the **Update Image** screen, select **Public**.
6. Click **Update Image**.

The image is public and available to all projects in the domain.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Networks

You can use the dashboards to create, delete, and configure your HP Helion OpenStack network and subnet(s). You can also manage the ports in your network.

How you interact with your network environment depends upon your user type, either an administrative user (admin) or a non-administrative user (user).

Note: The admin can perform all of the user tasks in addition to the admin tasks.

Managing your network as a user

As a user, you can work with the network(s) in the active project.

Access the networking commands using the **Networks** panel on the **Project** dashboard.

The **Network** panel contains commands to view a visual representation of your network and to enable you to work with your network.

- *View your network*
- *Create or delete a network*
- *Enable or disable a network*

Managing your network as an admin

As an admin user, you can work on all of the network(s) in your domain, regardless of which project the network is associated with.

In addition to all of the user tasks, you can also make a network a shared network and make a network accessible externally.

Access the networking commands using the **System** panel on the **Admin** dashboard.

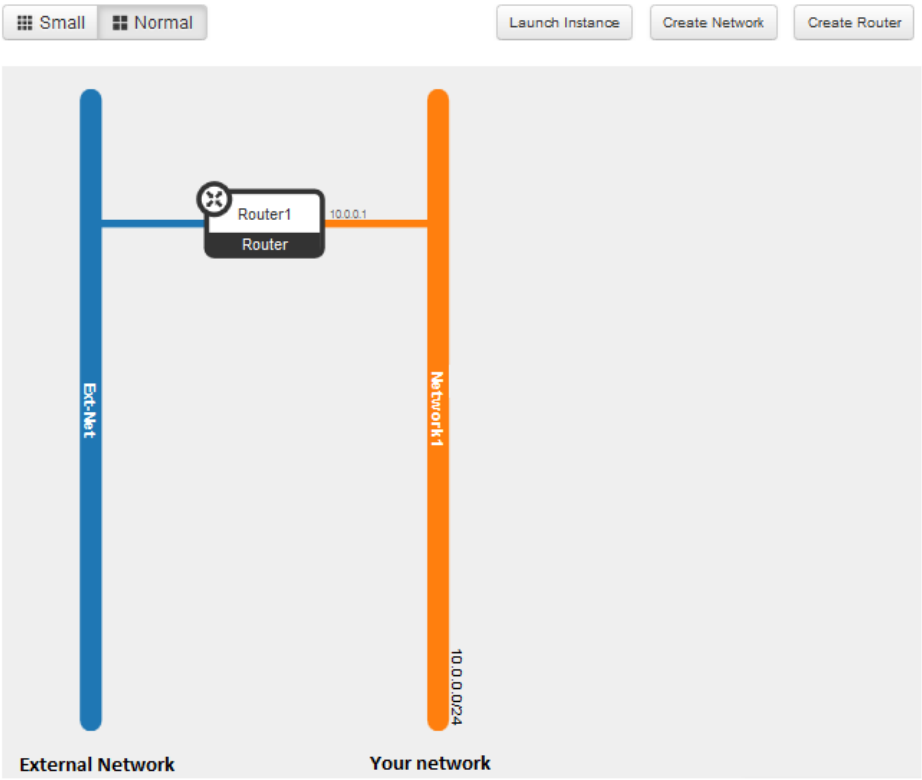
- *Creating externally available networks*
- *Creating a shared network*
- *Add or remove a subnet to/from a Network*
- *Create, Modify, or Delete a port on a Network*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Your Network

The **Network Topology** screen is a physical representation of your network configuration.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Networks** tab.
   - Click the **Project** dashboard, then the **Network** panel.
4. Click the **Network Topology** tab.

   Your network looks similar to the following diagram.



A router (here, labeled *Router 1*) is attached to the external network (labeled *Ext-Net*) so the internal network (labeled *Network1*) can be reached from the Internet. A *Network1* is attached to the router.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating or Deleting Networks

A network is a pluggable, scalable and API-driven system for managing networks and IP addresses.

A non-admin user or admin user can *create* and *delete* networks as needed.

Create a network

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Networks** tab.
   - Click the **Project** dashboard, then the **Network** panel, then the **Networks** tab.

   The available network(s) appear.
4. Click **Create Network**.
5. On the **Network** table:
   - Enter a name for the network.
   - Leave **Admin State** selected to launch the network in the enabled state or clear the field to disable the new network.
6. Click **Next** to configure a subnet for the network.
7. On the **Subnet** tab:
   - Enter the subnet name.
   - Enter a network address range for the subnet in CIDR (Classless Inter-Domain Routing) format in the **Network Address** field, for example: 192.168.0.0/24.

- Select IPv4 or IPv6, as appropriate, in the IP Version field.
- Enter a gateway IP address from the subnet or leave the **Gateway IP** field blank to use the default value for the gateway IP address; for example, 192.168.0.1 for 192.168.0.0/24.
- Leave **Disable Gateway** clear to enable the default gateway for this network, or select **Disable Gateway** to create the network with no default gateway.
- Determine if the network is to be available in all projects in the domain or only the selected project:
  - Select **Shared** to make the network available in all projects.
  - Leave the **Shared** option clear to limit the network to the selected project.
- Determine if the network is to be available externally or only internally:
  - Select **External Network** to make the network an externally accessible.
  - Leave the **External Network** option clear to make the network internal, only accessible from the external network through a network router.

8. Click **Next**.

9. On the **Subnet Details** tab:

- Clear the **Enable DHCP** option, as needed, to not use the network as a DCHP. DHCP is enabled by default. If enabled, the subnet will serve as your DHCP server. Instances associated with the subnet will be assigned an IP address from this pool. .
- Optionally, enter the starting and ending IP addresses you want for your DHCP allocation pool in the **Allocation Pools** field, in the format IP*ADDR,IP*ADDR. For example: 192.168.1.10,192.168.1.120. By deafult, the server has an application pool starting with 10.0.0.0/24.
- Optionally, enter the IP Address of your subnet in the **DNS Name Servers** field. If blank, your subnet will default to using HP's internal DNS which uses DNSMASQ.
- Optionally, enter the Destination CIDR and Next Hop for your subnet in the Host Routes field to create host routes.

10. Click **Create**.

Delete a network

1. *Launch the HP Helion OpenStack Horizon Dashboard*.

2. *Select the appropriate region and project*.

3. Based on whether you are *working on a project or the domain*:

- Click the **Admin** dashboard, then the **System** panel, then the **Networks** tab.
- Click the **Project** dashboard, then the **Network** panel, then the **Networks** tab.

The available network(s) appear.

4. For the network to delete, click **Edit Network** then **Delete Network**.

5. In the confirmation screen, click **Delete Network**.

The network is deleted and any instances attached to the networks are disconnected.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Enabling and Disabling Networks

A network is a pluggable, scalable and API-driven system for managing networks and IP addresses. You can *enable* or *disable* networks, as needed.

Enable a network

1. *Launch the HP Helion OpenStack Horizon Dashboard*.

2. *Select the appropriate region and project*.

3. Based on whether you are *working on a project or the domain*:

- Click the **Admin** dashboard, then the **System** panel, then the **Networks** tab.
- Click the **Project** dashboard, then the **Network** panel, then the **Networks** tab.

The available network(s) appear.

4. For the network to enable or disable, click **Edit Network**.
5. In the **Edit Network** screen, select **Admin State** to enable the port
6. Click **Save Changes**.

Disable a network

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Networks** tab.
   - Click the **Project** dashboard, then the **Network** panel, then the **Networks** tab.

   The available network(s) appear.
4. For the network to disable, click **Edit Network**.
5. In the **Edit Network** screen, clear **Admin State** to disable the port.
6. Click **Save Changes**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating Externally Available Networks

A network is a pluggable, scalable and API-driven system for managing networks and IP addresses.

A non-admin user or admin user can *create* and *delete* networks as needed.

Create an externally available network

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.

   The network(s) for the selected project appear.
4. Click **Create Network**.
5. On the **Network** tab:
   1. Enter a name for the network.
   2. Leave **Admin State** selected to launch the network in the enabled state or clear the field to disable the new network.
   3. Determine if the network is to be available in all projects in the domain or only the selected project:
   4. Select **Shared** to make the network available in all projects.
   5. Leave the **Shared** option clear to limit the network to the selected project.
6. Determine if the network is to be available externally or only internally:
   1. Select **External Network** to make the network an externally accessible.
   2. Leave the **External Network** option clear to make the network internal, only accessible from the external network through a network router.
7. Click **Create Network**.

To configure a subnet and ports for the network, see:

- *Add or remove a subnet to/from a Network*
- *Create, Modify, or Delete a port on a Network*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating a Shared Network

A shared network is visible to all projects in the domain. Instances have a single NIC, and receive a fixed IP address from the subnet(s) associated with that network.

An admin user can create a shared network as needed.

Create a network

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.

   The network(s) for the selected project appear.
4. Click **Create Network**.
5. On the **Create Network** screen:
   1. Enter a name for the network.
   2. Select a project to associate with the network.
   3. Leave **Admin State** selected to launch the network in the enabled state or clear the field to disable the new network.
   4. Select **Shared** to make the network available to all projects in the domain.
   5. Leave **External Network** clear to make the network internally accessible only.
6. Click **Create Network**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Adding and Removing Subnets

When a *network is created*, a subnet (short for *subnetwork*) can be assigned upon creation. However, you might need to add a subnet to a network at a later time.

A subnet is a logically visible subdivision of a network. A subnet enables you to group instances logically, while maintaining a single network address to connect to the Internet.

An admin user can create and delete subnets as needed.

Note: Before you delete a subnet, you must first *delete all ports* associated with the subnet.

Add a subnet

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.

   The network(s) for the selected project appear.
4. Click the name of the network you want to work with.
5. On the **Network Detail** page click **Create Subnet**.
6. On the **Subnet** tab of the **Create Network** screen:
   1. Enter the subnet name.
   2. Enter a network address range for the subnet in CIDR (Classless Inter-Domain Routing) format in the **Network Address** field, for example: `192.168.0.0/24`.
   3. Select IPv4 or IPv6, as appropriate, in the IP Version field.
   4. Enter a gateway IP address from the subnet or leave the **Gateway IP** field blank to use the default value for the gateway IP address; for example, `192.168.0.1` for `192.168.0.0/24`.
   5. Leave **Disable Gateway** clear to enable the default gateway for this network, or select **Disable Gateway** to create the network with no default gateway.
7. Click **Next**.
8. On the **Subnet Details** tab:
   1. Clear the **Enable DHCP** option, as needed, to not use the network as a DCHP. DHCP is enabled by default. If enabled, the subnet will serve as your DHCP server. Instances associated with the subnet will be assigned an IP address from this pool.
   2. Optionally, enter the starting and ending IP addresses you want for your DHCP allocation pool in the **Allocation Pools** field, in the format `IPADDR,IPADDR`. For example: `192.168.1.10,192.168.1.120`. By deafult, the server has an application pool starting with `10.0.0.0/24`.

   3. Optionally, enter the IP Address of your subnet in the **DNS Name Servers** field. If blank, your subnet will default to using HP's internal DNS which uses DNSMASQ.
   4. Optionally, enter the Destination CIDR and Next Hop for your subnet in the **Host Routes** field to create host routes.
9. Click **Create**.

Delete a subnet

Before you delete a subnet, you must first *delete all ports* associated with the subnet.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.

   The network(s) for the selected project appear.
4. Click the name of the network you want to work with.
5. On the **Network Detail** page, for the subnet you want to delete, click **Edit Network** then **Delete Subnet**.
6. In the confirmation screen, click **Delete Subnet**.

   A message appears indicating if the subnet was deleted successfully.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Adding or Removing Ports

A port is a connection point for attaching a single device, such as the NIC of a virtual server, to a virtual network. You can configure rich network topologies by creating and configuring networks and subnets, and then instructing other OpenStack services like Compute to attach virtual devices to ports on these networks.

As an admin you can add ports to an existing subnet. Non-admin users can create subnets, but cannot create ports.

You can edit the device associated with a port and change the admin state, as needed.

As an admin, you can:

- *create and delete a port*
- *change the device associated with the port*
- *change the admin state between Up or Down*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating and Deleting Ports

A port is a connection point for attaching a single device, such as the NIC of a virtual server, to a virtual network. You can configure rich network topologies by creating and configuring networks and subnets, and then instructing other OpenStack services like Compute to attach virtual devices to ports on these networks.

As an admin, you can:

- *create a port*
- *delete a port*

Create a port

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.
4. Click the name of the network you want to work with.
5. On the **Network Detail** page, click **Create Port**.
6. On the **Create Port** screen:

   1. Enter a descriptive name for the port.
   2. Leave the **Admin State** field selected to create a port in the active state. Or, clear the field to create a non-active port.
   3. Optionally, specify a device ID to assign the port to that device.

4. Optionally, specify a device name to assign the port to that device.

   Note: If you do not know the device ID and name, you can create the port and later edit the port to add the ID and name.

7. Click **Create Port**.

   A message appears indicating if the port was successfully created. When the port is created, an available fixed IP address out of one the designated subnets is associated with the port.

Edit a port

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.
4. Click the name of the network you want to work with.
5. On the **Network Detail** page, for the port you want to delete, click **Edit Port**.
6. On the **Edit Port** screen:
   1. Leave the **Admin State** field selected to create a port in the active state. Or, clear the field to create a non-active port.
   2. Specify a device ID to assign the port to that device.
   3. Specify a device name to assign the port to that device.
7. Click **Save Changes**.

   A message appears indicating if the port was successfully modified.

Delete a port

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.
4. Click the name of the network you want to work with.
5. On the **Network Detail** page, for the port you want to delete, click **Edit Port** then **Delete Port**
6. In the confirmation screen, click **Delete Port**.

   A message appears indicating if the port was deleted successfully.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Changing the Admin State of Ports

You can edit the admin state, as needed, to make a port active or non-active.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.
4. Click the name of the network you want to work with.
5. On the **Network Detail** page, for the port you want to delete, click **Edit Port**.
6. On the **Edit Port** screen, leave the **Admin State** field selected to create a port in the active state. Or, clear the field to create a non-active port.
7. Click **Save Changes**.

   A message appears indicating if the port was successfully modified.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Change the Device Associated with a Port

You can edit the device associated with a port, as needed.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Network** panel.
4. Click the name of the network you want to work with.

5. On the **Network Detail** page, for the port you want to delete, click **Edit Port**.
6. On the **Edit Port** screen:
   1. Specify a device ID to assign the port to that device.
   2. Specify a device name to assign the port to that device.
7. Click **Save Changes**.

   A message appears indicating if the port was successfully modified.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Routers

Each network can be assigned a router, which provides a gateway to external networks.

- *Create a Router*
- *Delete a Router*
- *Connect a network to a router*
- Add / Remove an external network to/from a Router

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating and Deleting Routers

A network connects to the router through an interface.

You can:

- *create a router*
- *delete a router*

Create a router

You must create an interface between the network and router to remotely connect to the network and any instances on that network through the router.

When you create a new router, the router does not have any internal interface and it is not associated to any subnet. You can optionally specify an external gateway after creating the router.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Routers** tab.
   - Click the **Project** dashboard, then the **Network** panel, then the **Routers** tab.

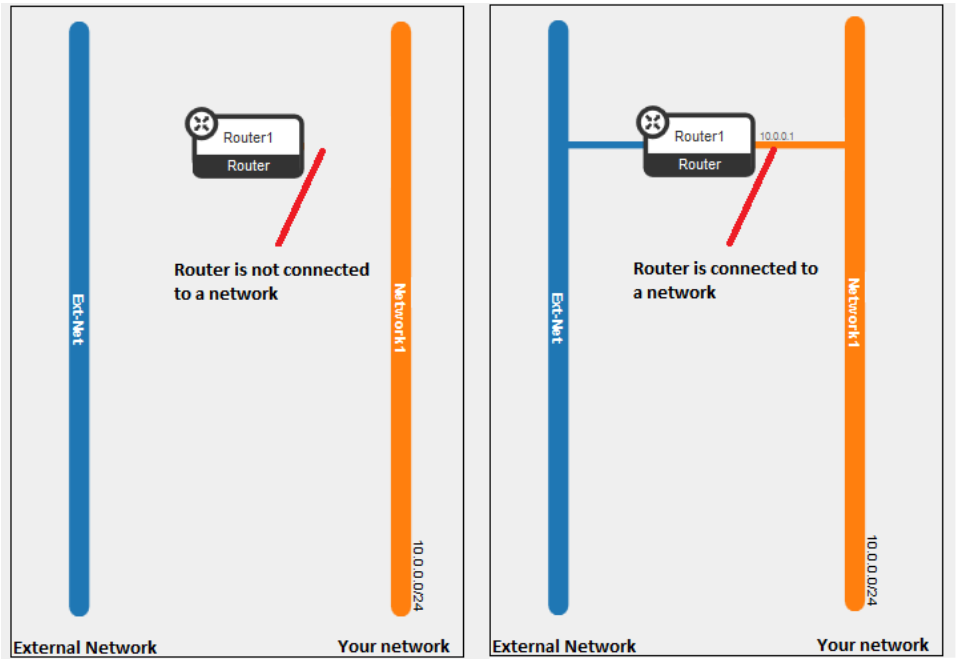
   The available router(s) appear.
4. Click **Create Router**.
5. On the **Create Router** tab enter a name for the network.
6. Click **Create Router**.

Deleting a router

You must remove all router interfaces before deleting the router, by removing all internal interfaces.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:
   - Click the **Admin** dashboard, then the **System** panel, then the **Routers** tab.
   - Click the **Project** dashboard, then the **Network** panel, then the **Routers** tab.

   The available router(s) appear.
4. Determine if the router is connected to a network using the *Network Topology screen*:



5. Click the **Routers** link on the **Project** dashboard **Network** panel.

   The routers for the selected project appear.

   If the router is connected to a network:

   a. Click the name of the router you want to delete.
   b. On the **Router Details** screen, select the interface(s) for the router and click **Delete Interface**.
   c. Return to the **Routers** screen.
6. For the router you want to delete, click **Edit Router** then **Delete Router**
7. In the confirmation window, click **Delete Router**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Connecting a Network to a Router

A network connects to the router through an interface. You must create an interface between the network and router to remotely connect to the network and any instances on that network through the router.

When you create a new router, the router is not associated to any subnet. You can optionally connect the router to an internal network.

Connect a network to the router

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Based on whether you are *working on a project or the domain*:

   - Click the **Admin** dashboard, then the **System** panel, then the **Routers** tab.
   - Click the **Project** dashboard, then the **Network** panel, then the **Routers** tab.

   The available router(s) appear.
4. Click the name of the router you want to connect to the network.
5. On the **Router Details** tab, click **Add interface**.
6. On the **Add Interface** screen:

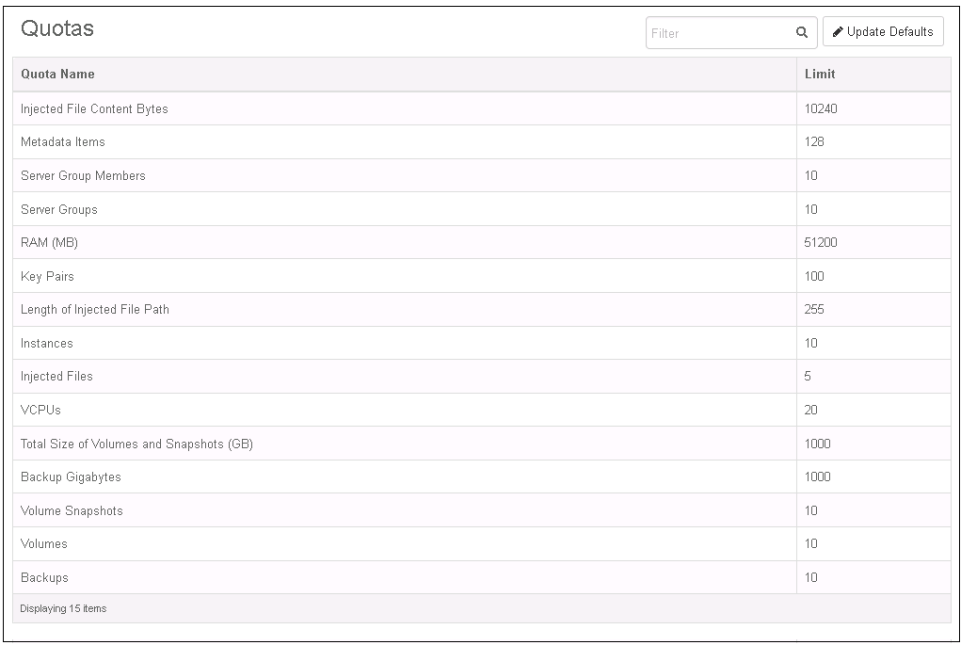
   - Select a subnet associated with the network you want to connect with from the **Select** list.
   - Optionally, specify an IP address for the interface that is in the IP range.
7. Click **Add Interface**

The network is connected to the router.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Default Quotas

Quotas are operational limits enforced on each project.

To prevent system capacities from being exhausted without notification, you can set up quotas.



Quotas

Filter | Update Defaults

Quota Name	Limit
Injected File Content Bytes	10240
Metadata Items	128
Server Group Members	10
Server Groups	10
RAM (MB)	51200
Key Pairs	100
Length of Injected File Path	255
Instances	10
Injected Files	5
VCPUs	20
Total Size of Volumes and Snapshots (GB)	1000
Backup Gigabytes	1000
Volume Snapshots	10
Volumes	10
Backups	10

Displaying 15 items

For example, the number of gigabytes allowed per project can be controlled to make sure that a single project does not consume all of the disk space.

To modify quotas:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Defaults** tab.
4. In the **Quotas** table, click the **Update Defaults**.

   Edit any of the following fields:

   - **Injected File Content Bytes** - Enter the maximum number of content bytes allowed per injected file for the project.
   - **Metadata Items** - Enter the maximum number of metadata items allowed for the project.
   - **Server Group Members** - Enter the maximum number of members allowed in a security group, per project.
   - **Server Groups** - Enter the maximum number of security groups allowed per project.
   - **RAM** - Enter the maximum megabytes of instance RAM allowed for the project.
   - **Key Pairs** - Enter the maximum number of key pairs allowed per user..
   - Length of Injected File Path
   - **Instances** - Enter the maximum number of instances allowed for the project.
   - **Injected Files** - Enter the maximum number of injected files allowed for the project.
   - **VCPUs** - Enter the maximum number of instance cores allowed for the project.
   - **Total Size of Volumes and Snapshots**- Enter the maximum total size for all volumes and snapshots allowed for the project.
   - **Backup Gigabytes** - Enter the maximum number of storage, in gigabytes, for backup files, per project.
   - **Volumes** - Enter the maximum number of volumes allowed for the project.
   - **Volume Snapshots** - Enter the maximum number of volume snapshots allowed for the project.

- **Backups** - - Enter the maximum number of backup files, per project.

5. Click **Save**.

   A message is displayed on successful modification.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing System Faults

You can examine and filter the alarms and logs generated by HP Helion OpenStack Carrier Grade in order to monitor and respond to fault conditions.

Note: This feature applies only to KVM region servers

Using the Fault Management page on the Admin menu, you can access the following system records:

- **Active Alarms**—Alarms that are currently set, and require user action to clear them. See *Viewing System Alarms*.
- **Historical Alarms**—Alarms that have been raised in the past, including those that have been cleared. See *Viewing System Alarms*.
- **Customer Logs**—Events that do not require user action, but may provide useful information for fault management. See *Viewing Customer Logs*.

For more information on alarms, see the *HP Helion OpenStack® 2.0 Carrier Grade: Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Alarms and Logs

You can examine and filter the alarms and logs generated by HP Helion OpenStack Carrier Grade in order to monitor and respond to fault conditions.

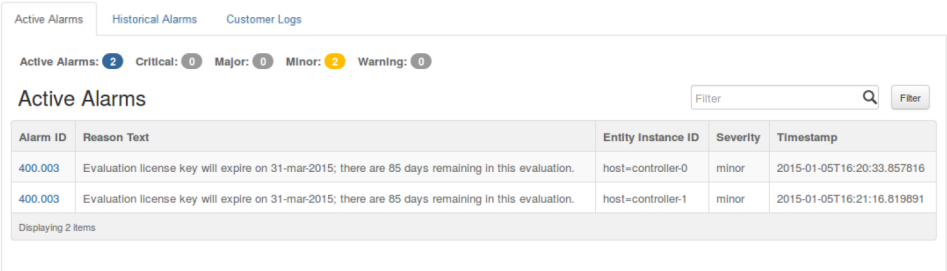
Note: This feature applies only to KVM region servers.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Fault Management** panel.
4. Click one of the tabs to view specific alarms:
   - *Active Alarms*
   - *Historic Alarms*

For more information on alarms, see the *HP Helion OpenStack® 2.0 Carrier Grade: Administrator Guide*.

Viewing Active Alarms

A list of all active or set alarms in the system.



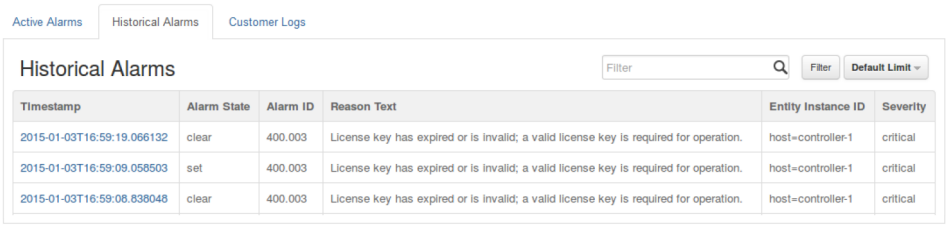
Each entry in the table includes the following variables:

- UUID
- AlarmID
- EntityInstanceID
- DateAndTime
- AlarmSeverity
- ReasonText

- EventType
- ProbableCause
- ProposedRepairAction
- ServiceAffecting
- SuppressionAllowed

Historic Alarms

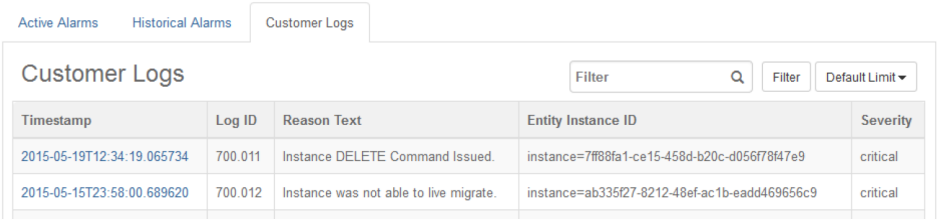
A history of set and clear alarm operations in the system. The table includes the same variables as the *Active Alarm Table*, plus the variable `AlarmState`, used to indicate whether the table entry is a SET or a CLEAR operation.



Timestamp	Alarm State	Alarm ID	Reason Text	Entity Instance ID	Severity
2015-01-03T16:59:19.066132	clear	400.003	License key has expired or is invalid; a valid license key is required for operation.	host=controller-1	critical
2015-01-03T16:59:09.058503	set	400.003	License key has expired or is invalid; a valid license key is required for operation.	host=controller-1	critical
2015-01-03T16:59:08.838048	clear	400.003	License key has expired or is invalid; a valid license key is required for operation.	host=controller-1	critical

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Customer Logs

You can obtain information about transient events using Customer Logs. Certain system events that do not result in node state changes and typically do not require immediate customer action, such as instance deletions or failed migration attempts, are recorded in Customer Logs.



Timestamp	Log ID	Reason Text	Entity Instance ID	Severity
2015-05-19T12:34:19.065734	700.011	Instance DELETE Command Issued.	instance=7ff88fa1-ce15-458d-b20c-d056f78f47e9	critical
2015-05-15T23:58:00.689620	700.012	Instance was not able to live migrate.	instance=ab335f27-8212-48ef-ac1b-eadd469656c9	critical

Note: This feature applies only to KVM region servers.

Each log describes a single event. The logs are held in a buffer, with older logs discarded as needed to release logging space.

The following types of events are included in the Customer Logs. The severity of the events is represented in the table by one or more letters, as follows:

- C: Critical
- M: Major
- m: Minor
- W: Warning

To view customer logs:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **Fault Management** panel.
4. Click the Customer Logs tabs.

   The logs are displayed in chronological order, beginning with the most recent.

   By default, 20 items are shown per page. To see older items, scroll to the bottom of the list and click **Next**. You can change the number of items displayed per page using the **Default Limit** drop-down list.

   You can also filter the items using the **Filter** text box. Type the filter string, and then click the search icon. The results include only those logs that contain the string in the **Customer Log Detail**.

5. To see specific details on a log, click the time stamp identifier for the log.

For more information on customer logs, see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing System Configuration

You can make changes to the HP Helion OpenStack Carrier Grade's initial configuration at any time after installation. The HP Helion OpenStack Carrier Grade's initial configuration is defined during software installation. After installation, you can make changes using the web administration interface or the CLI. For most types of changes, you can do this without interrupting system operations.

Note: This feature applies only to KVM region servers.

You can change the initial configuration as follows:

- Reconfigure aspects of the External OAM network, including the subnet, controller IP addresses, gateway IP address, and floating IP address.
- Change the DNS server IP addresses.
- Change the NTP server IP addresses.
- Change the disk allocations for database storage, image storage, backup storage, and Cinder volume storage.
- Add an infrastructure network if one is not already configured

Immediately before making a change, ensure the following:

- All hosts are unlocked.
- No Major or Critical alarms are shown for the system on *the Fault Management page*.
- No 250.001 Configuration out-of-date alarms are shown for the system on *the Fault Management page*.

During these changes, the HP Helion OpenStack Carrier Grade can remain online and operational.

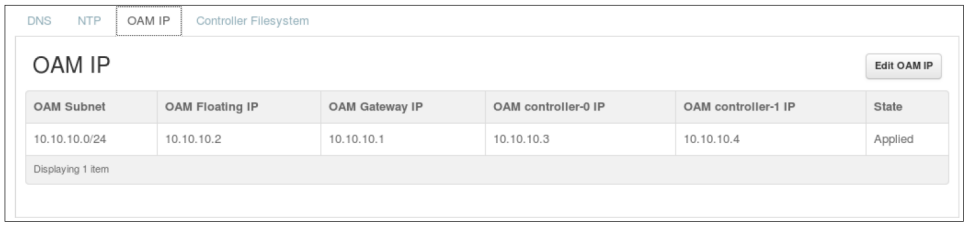
You can make the following changes:

- *Change the OAM IP address*.
- *Configure a new DNS server*.
- *Configure a new NTP server*.
- *Change storage space allotments on the controller*. For important information and instructions for changing storage allotments, see the *HP Helion OpenStack® 2.0 Carrier Grade: Administrator Guide*.

For more information on system configuration, see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Changing the OAM IP Configuration

You can change the External OAM subnet, floating IP address, controller addresses, and default gateway at any time after installation.



Note: This feature applies only to KVM region servers.

During software installation, the HP Helion OpenStack Carrier Grade is configured with an OAM network subnet and related IP addresses. You can change these addresses using the web administration interface or the CLI.

Caution: Access to the OAM network is interrupted during this procedure. When a swact is performed on the controllers, the newly active controller uses the changed OAM IP addresses. The existing OAM IP addresses are no

longer valid, and you must use the new OAM IP addresses to reconnect to the controller. Changes to external OAM access routing settings may also be required. In addition, VNC console access to computenode hosts is interrupted until the hosts are locked and unlocked.

Before changing the OAM IP configuration, review the Fault Management page and ensure that any existing system alarms are cleared.

To change the OAM IP:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System Configuration** panel.
4. Click the **OAM IP** tab.

   The OAM IP page displays the currently defined OAM network configuration.
5. Click **Edit OAM IP**.
6. In the **Edit OAM IP** dialog box, replace the IP addresses with different ones as required.
7. Click Save.

   Changing this IP raises major alarms against the controllers and services. You can view the alarms on *the Fault Management page*.

Clear the alarms

Changing the OAM IP causes major alarms against the controllers and services.

Use the Hosts table to determine which hosts requiring attention (indicated with the status `Config out-of-date`). Perform the following steps to lock and unlock the controllers to clear the alarms:

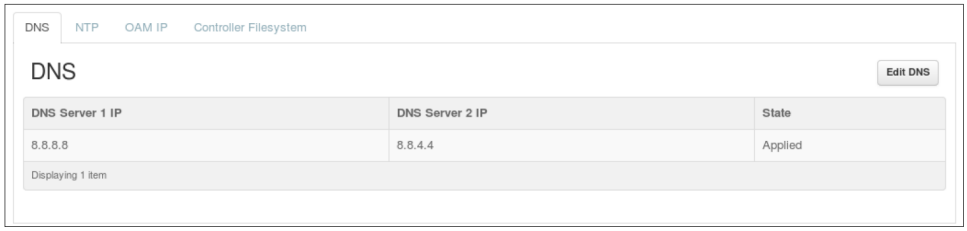
1. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
2. *Lock the standby controller*. Wait for the lock operation to be completed.
3. *Unlock the standby controller*. Wait for the host to become available. It is updated with the new OAM configuration, and its error message is cleared.
4. *Perform a swact on the active controller*.

   Note: After the swact, the HP Helion OpenStack Carrier Grade begins using the new OAM network configuration. If you have changed the OAM subnet or the OAM floating IP address, the current web session is terminated. To continue using the web administration interface, you must start a new session and log in using the new IP address. You may also need to update router tables to establish a connection.
5. *Lock the original controller* (now in standby mode). Wait for the lock operation to be completed. e) Unlock the original controller. Wait for it to become available. It is updated with the new OAM configuration, and its error message is cleared.
6. *Lock and unlock each compute node*.

For more information on system configuration, see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Changing the DNS Server Configuration

You can change the DNS servers defined for the HP Helion OpenStack Carrier Grade at any time after installation. During software installation, the HP Helion OpenStack Carrier Grade is configured with up to two DNS server IP addresses.



Note: This feature applies only to KVM region servers.

To change the DNS configuration:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System Configuration** panel.
4. Click the **DNS** tab.

   The DNS page displays the currently defined DNS servers and their IP addresses.
5. Click **Edit DNS**.
6. In the **Edit DNS** dialog box, replace the **DNS Server IP** addresses with different ones as required.
7. Click **Save**.

   Upon completion of the DNS configuration change, a 250.001 Configuration out-of-date alarm is raised temporarily, and then cleared automatically by the system..

For more information on system configuration, see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Changing the NTP Server Configuration

You can change the NTP server addresses defined for the HP Helion OpenStack Carrier Grade at any time after installation. During software installation, you configured the HP Helion OpenStack Carrier Grade with NTP server IP addresses. You change these addresses using the web administration interface or the CLI.

Note: This feature applies only to KVM region servers.

Before changing NTP server addresses, review *the Fault Management page* and make sure that any existing system alarms are cleared.

Caution: For the HP Helion OpenStack Carrier Grade system to use FQDN servers instead of IPv4 servers, at least one valid DNS server must be specified.

To change the NTP configuration:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System Configuration** panel.
4. Click the **NTP** tab.

   The NTP page displays the currently defined NTP servers and their IP addresses.
5. Click **Edit NTP**.
6. In the **Edit NTP** dialog box, replace the NTP server address(es) with different ones as required.

   If you specify the NTP servers using FQDNs you must have at least one valid DNS server defined on your system. You must use IP addresses otherwise.
7. Click **Save**.

Changing this IP raises major alarms against the controllers and services. You can view the alarms on *the Fault Management page*.

Clear the alarms

Changing the OAM IP causes major alarms against the controllers and services.

Use the Hosts table to determine which hosts requiring attention (indicated with the status `Config out-of-date`). Perform the following steps to lock and unlock the controllers to clear the alarms:

1. Click the **Admin** dashboard, then the **System** panel, then the **Inventory** tab. Click the **Hosts** table.
2. *Lock the standby controller*. Wait for the lock operation to be completed.
3. *Unlock the standby controller*. Wait for the host to become available. It is updated with the new NTP server addresses, and its error message is cleared.
4. *Perform a swact on the active controller*.

   Note: After the swact, the HP Helion OpenStack Carrier Grade begins using the new OAM network configuration. If you have changed the OAM subnet or the OAM floating IP address, the current web session is terminated. To continue using the web administration interface, you must start a new session and log in using the new IP address. You may also need to update router tables to establish a connection.
5. *Lock the original controller* (now in standby mode). Wait for the lock operation to be completed. e) Unlock the original controller. It is updated with the new NTP server addresses, and its error message is cleared.
6. *Lock and unlock each compute node*.

For more information on system configuration, see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Changing Storage Space Allotments on the Controller

You can change the allotments for controller-based storage at any time after installation. This includes the space allotted for database, image, and backup storage, and for clusters using an LVM backend, the space allotted for Cinder volume storage.

Note: This feature applies only to KVM region servers.

During software installation, the HP Helion OpenStack Carrier Grade is configured with the following storage allotments.

- **Database storage**. The storage allotment for the OpenStack database.
- **Image storage**. The size of the partition to use for image storage.
- **Backup storage**. The storage allotment for backup operations.
- **Volume storage**. For a system using LVM storage, the storage allotment for all Cinder volumes used by guest instances.

For important information and instructions for changing storage allotments, see the *HP Helion OpenStack® Carrier Grade 2.1 Beta: Administrator Guide*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing System Information

As an administrative user, you can view information for OpenStack services.

System Information

Services | Compute Services | Block Storage Services | Orchestration Services

Filter

Name	Service	Host	Status
cinderv2	volumev2	10.10.2.102	Enabled
nova	compute	10.10.2.51	Enabled
neutron	network	10.10.2.51	Enabled
power_mgmt	power	10.10.2.51	Enabled
novav3	computev3	10.10.2.51	Enabled
glance	image	10.10.2.102	Enabled
ceilometer	metering	10.10.2.51	Enabled
heat-api-cfn	cloudformation	10.10.2.51	Enabled
cinder	volume	10.10.2.102	Enabled
sysinv	platform	10.10.2.51	Enabled
nova_ec2	ec2	10.10.2.51	Enabled
heat	orchestration	10.10.2.51	Enabled
swift	object-store	10.10.2.102	Enabled
patching	patching	10.10.2.51	Enabled
keystone	identity (native backend)	10.10.2.102	Enabled
attis	backupandrestore	-	-

Displaying 16 items

To view system information:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **System Information** tab.

   View the following information on these tabs:

   - **Services** - Displays the internal name and the public OpenStack name for each service, the host on which the service runs, and whether or not the service is enabled.
   - **Compute Services** - Displays information specific to the Compute Service. Both host and zone are listed for each service, as well as its activation status.
   - **Block Storage Services** - Displays information specific to the Block Storage Service. Both host and zone are listed for each service, as well as its activation status.
   - **Orchestration Services** - Displays information specific to the Orchestration Service. Name, engine id, host and topic are listed for each service, as well as its activation status.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing Metadata Definitions

As an administrative user, you can view information metadata definitions.

To view system information:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Admin** dashboard, then the **System** panel, then the **Metadata Definitions** tab.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Identity

You can use HP Helion OpenStack to manage users.

You can manage access to projects by assigning users and setting primary projects. You can also control resources by managing operational quotas.

Working with Users

As an admin, you can use create projects and allow specific users to access each project:

- *Create and delete users*
- *Disable and enable a user*

- *Change a user password*
- *Specify a primary project for a user*

Working with projects

As an admin, you can use create projects and allow specific users to access each project:

- *Create and delete projects*
- *Specifying a Primary Project for a User*
- *View details on a project*

Managing quotas

Quotas are operational limits that you can configure to prevent system capacities from being exhausted without notification.

Use the **Identity** panel on the **Admin** dashboard to set maximum limits for metadata, instances, CPUs, memory, and other settings for each project.

- *Modify the quota of a project*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Users

You can use HP Helion OpenStack to manage users.

As an admin, you can use the dashboards to:

You can manage access to projects by assigning users and setting primary projects. You can also control resources by managing operational quotas.

Working with Users

As an admin, you can use create projects and allow specific users to access each project:

- *Create and delete users*
- *Disable and enable a user*
- *Change a user password*
- *Specify a primary project for a user*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating and Deleting Users

As an admin, you can *create* and *delete* users.

Create a user

To create a user:

Note: At least *one project must exist* before you can create users.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Users** panel.
4. In the **Users** table, click **Create User**.
5. In the **Create User** screen, enter the following:
   - **User Name** - Enter a name for the user. The user will need this name to log in.
   - **Email** - Enter an email associated with this user.
   - **Password** - Enter a password for the user. The user will need the password to log in.
   - **Confirm Password** - Re-enter the password to confirm.
   - **Primary Project** - Select a primary project for the user. The primary project is simply the first project the user is associated with.

- **Role** - Select a role for the user. The role determines many of the tasks that the user can perform.

6. Click **Create User**.

   The user is created and appears in the user list.

Delete a user

To delete a user:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Users** panel.
4. In the **Users** table, for the user you want to delete, click **Edit User** then **Delete User**.
5. In the confirmation dialog that appears, click **Delete User**.

   The user is removed and no longer available in the domain.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Disabling and Enabling Users

Users can be disabled in the domain. After you disable a user, the user account remains in the domain, but cannot be used to log in.

As an admin, you can *disable* and *enable* users, as needed.

Disable a user

To disable a user:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Users** panel.
4. In the **Users** table, for the user you want to disable, click **Edit User** then **Disable User**.

   The user is disabled and cannot be used to log in.

Enable a user

To enable a user:

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Users** panel.
4. In the **Users** table, for the user you want to enable, click **Edit User** then **Enable User**.

   The user is enabled and can be used to log in.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Changing a User Password

As an admin, you can change the password for a user, as needed. You do not need to know the current password in order to assign a new password.

Change a Password

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Users** panel.
4. In the **Users** table, for the user you want to delete, click **Edit User** then **Update User**.
5. In the **Update User** screen, enter a new password in the Password field and re-enter the password in the **Confirm Password** field to confirm.
6. Click **Update User**.

You must relay the new password information to the user in a secure manner under the rules of your organization.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing Projects

You can manage access to projects by assigning users and setting primary projects. You can also control resources by managing operational quotas.

Creating projects

As an admin, you can use create projects and allow specific users to access each project:

- *Create and delete projects*
- *Specifying a Primary Project for a User*
- *View details on a project*

Managing quotas

Quotas are operational limits that you can configure to prevent system capacities from being exhausted without notification.

Use the **Identity** panel on the **Admin** dashboard to set maximum limits for metadata, instances, CPUs, memory, and other settings for each project.

- *Modify the quota of a project*

HP Helion OpenStack® Carrier Grade 2.1 Beta: Viewing all projects in the domain

As an admin, you can view a list of all projects in a domain and view information on each project.

View projects

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Projects** panel.

   A list of all projects in the current domain is displayed. You can see the name, ID and status (enabled or disabled).
4. To view information on a project, click **Edit Project**.

   The project name and details; users associated with the project, and project quotas are displayed.

   For information on modifying these settings, see *Managing Projects*.
5. Click **Cancel** to exit the screen.
6. To view usage information on a project, click **Edit Projects** then **View Usage**.

   The instances associated with the project are listed, with memory and uptime information.
7. Click **Cancel** to exit the screen.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Creating and Deleting Projects

As an admin user can *create* and *delete* networks as needed..

Create a project

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Projects** panel.
4. In the **Projects** table, click **Create Project**.
5. On the **Project Info** tab of the **Create Project** screen:

   1. Enter a unique name for the project.
   2. Enter an identifying description for the project.
   3. Leave **Enabled** selected to create an active project or clear the option to create a non-active project

6. Click the **Project Members** tab.
7. On the **Project Members** tab select the users who can access the project by clicking the + icon for each user.
8. Click the **Quotas** tab.
9. Optionally, specify operational quotas for the project. Metadata Items - Enter the maximum number of metadata items allowed per instance.
   - VCPUs Enter the maximum number of instance cores allowed for the project.
   - Instances Enter the maximum number of instances allowed for the project.
   - Injected Files Enter the maximum number of injected files allowed for the project.
   - Injected File Content Bytes Enter the maximum number of content bytes allowed per injected file.
   - RAM Enter the maximum megabytes of instance RAM allowed for the project.
10. Click **Create Project**.

Delete a project

As an admin, you can delete projects. Compute instances associated with a project will not be deleted.

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Projects** panel.
4. In the **Projects** table, for the project you want to delete, click **Edit Project** then **Delete Project**.
5. In the confirmation screen, click **Delete Project**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Adding and removing users to a project

As an admin, you can add and remove user access to each project.

Editing users associated with a project

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Projects** panel.

   A list of all projects in the current domain is displayed.
4. For the project you want to modify, click the **Modify Users** button.

   On the **Project Members** tab of the **Edit Project** screen that displays, the users in the **Project Members** column can access and work with the current project.
   - **Add a user to the project**. Click the + icon next to that user name in the **All Users** column.

     The user name is added to the **Project Members** column and can now access the project.
   - **Remove a user to the project**, click the **-** icon next to that user name in the **Project Members** column.

     The user name is moved to the **All Users** column and can no longer access the project.
5. Click **Save**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Specifying a Primary Project for a User

When you create a user account, you must assign the account to a *primary* project. The primary project is simply the first project the user is associated with and must exist prior to creating the user.

Optionally, you can assign the account to additional projects. Before you can delete a user account, you must remove the user account from its primary project.

As an admin, you can specify a *primary* project for each user.

Specify a primary project

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.

3. Click the **Identity** dashboard, then the **Users** panel.
4. In the **Users** table, for the user you want to delete, click **Edit User**.
5. In the **Update User** screen, select a project from the **Primary Project** list.
6. Click **Update User**.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Managing project quotas

Quotas are operational limits enforced on each project.

To prevent system capacities from being exhausted without notification, you can set up quotas.

For example, the number of gigabytes allowed per project can be controlled to make sure that a single project does not consume all of the disk space.

Modify a quotas

1. *Launch the HP Helion OpenStack Horizon Dashboard*.
2. *Select the appropriate region and project*.
3. Click the **Identity** dashboard, then the **Projects** panel.
4. For the project you want to modify, click **Edit Project**then **Modify Quotas**.
5. In the **Edit Project** screen, click the **Quota** tab (should be active).
6. Edit and of the following fields:
   - Metadata Items - Enter the maximum number of metadata items allowed for the project.
   - VCPUs - Enter the maximum number of instance cores allowed for the project.
   - Instances - Enter the maximum number of instances allowed for the project.
   - Injected Files - Enter the maximum number of injected files allowed for the project.
   - Injected File Content Bytes - Enter the maximum number of content bytes allowed per injected file for the project.
   - Volumes - Enter the maximum number of volumes allowed for the project.
   - Volume Snapshots - Enter the maximum number of volume snapshots allowed for the project.
   - Total Size of Volumes and Snapshots- Enter the maximum total size for all volumes and snapshots allowed for the project.
   - RAM - Enter the maximum megabytes of instance RAM allowed for the project.
7. Click **Save**.

   A message is displayed on successful modification.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Troubleshooting

This topic describes all the known issues that you might encounter:

- *Baremetal Control plane RDBMS recovery after reboot* on page 198
- *Unable to create an instance in the non-KVM region*
- *Backup storage size should be at least 120GB* on page 199
- *Glance/Swift not recovering after failure* on page 200
- *Two controllers have failed* on page 200

Baremetal Control plane RDBMS recovery after reboot

System Behavior/Message

The controller in the baremetal region of the Sacaramento deployment is designed to be a single control plane. If the controller reboots, the MySQL database installed into the controller crashes and the `mysql` service does not restart.

Resolution

Perform the following steps:

1. From the lifecycle manager VM, log in to the baremetal controller after reboot.

   ```
   ssh cghelion@<BM_Controller_IP>
   ```

   The `BM_Controller_IP` address can be obtained from the `nodes.json` file in `/var/hlm/clouds/<cloud_name>/` directory on the lifecycle manager.
2. Switch to the root user:

   ```
   sudo su -
   ```
3. Execute the following command to manually restart the `mysql` service:

   ```
   /etc/init.d/mysql bootstrap-pxc
   ```

Validation

1. Execute the following command to check status of mysql service:

   ```
   service mysql status
   ```

   This status should be `active`.
2. Log in to MySQL.

   ```
   sudo su -
   ```
3. Execute the following command to log into the MySQL database:

   ```
   mysql
   ```
4. Exit after logging in:

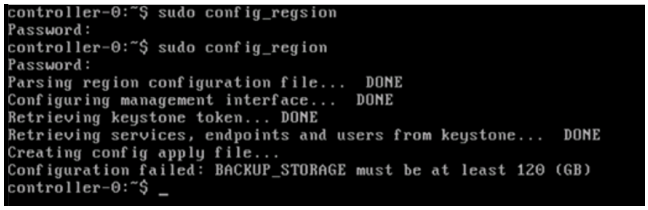
   ```
   exit
   ```
5. Check that the previous data is intact: Example commands:
   - **ironic node-list** should display the nodes registered before reboot
   - **neutron net-list** should display the created networks

Unable to create an instance in the non-KVM region

When trying to create a virtual machine instance in the non-KVM region, the user receives a `No valid host found` error. Check that all ESX host machines in the cluster are configured with the ESX compute proxy. If one or more hosts in the cluster is configured with the proxy, disconnect the host(s) from the cluster or *install the ESX compute proxy*.

Backup storage size should be at least 120GB

If you experience the following error, you can edit the `region_config` file for the KVM region to increase the default storage.



```
controller-0:~$ sudo config_regsion
Password:
controller-0:~$ sudo config_region
Password:
Parsing region configuration file...  DONE
Configuring management interface...  DONE
Retrieving keystone token... DONE
Retrieving services, endpoints and users from keystone...  DONE
Creating config apply file...
Configuration failed: BACKUP_STORAGE must be at least 120 (GB)
controller-0:~$ _
```

1. Log into the KVM region controller-0.
2. Edit the `./<cloud name>/clouds/<cloud name>/001/stage/windriver-config/region_config` file to update the `backup_storage` value to 120 or higher.

Glance/Swift not recovering after failure

The HP Helion OpenStack Carrier Grade Image Operations (Glance) service is based on OpenStack Glance, which uses embedded OpenStack Swift for back-end storage.

In the event of an embedded Swift node failing, Swift may take longer to report correctly the addition of new files and containers. This delay can be mitigated by replacing the failed node as soon as possible, or by removing the failed node from the ring. See the swift documentation, *Swift Administrator's Guide, Handling Server Failure* for further details on coping with single node failure.

Two controllers have failed

A restore procedure is required when two controllers have failed. HA Services are not guaranteed to be resilient after a second failure. See *Backup and Restore Configuration Files and MySQL Clusters*.

See Also

For troubleshooting tips related to the HP Helion OpenStack cloud, see *HP Helion OpenStack: Troubleshooting*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Installation Troubleshooting

This topic describes all the known issues that you might encounter:

- *Node fails to boot during HLM provision* on page 200
- *Installation fails due to Ansible errors* on page 200
- *HP Helion OpenStack Carrier Grade installation (hlm deploy) fails at the Reload apache2 configuration task* on page 201
- *HP Helion OpenStack Carrier Grade installation (hlm deploy) fails at the install ntp client task* on page 202
- *Installation fails at Ansible playbook* on page 202
- *VM fails to get private/Fixed IP address* on page 204
- *VRSvAPPs missing in VSD dashboard* on page 204

Node fails to boot during HLM provision

System Behavior/Message

In rare situations, a node might not boot during the HLM provisioning process due to an issue with network configuration.

Resolution

If this happens, log into that console. If you see a message stating that the boot failed at network configuration, use the Retry Auto Configuration option to attempt a re-boot. It might take more than one attempt to get the node to boot.

Installation fails due to Ansible errors

System Behavior/Message

The installation fails during `hlm deploy`, and you see any of the following errors:

- Any error with the following message: `Failed to launch the accelerated daemon on 10.10.2.102 (reason: failed to connect to the local socket file)` . For example:

```
GATHERING FACTS
 ***************************************************************
fatal: [BASE-CCP-T1-M1-NETCLM] => Failed to launch the accelerated daemon
 on 10.10.2.102 (reason: failed to connect to the local socket file)
ok: [BASE-CCP-T1-M2-NETCLM]
ok: [BASE-CCP-T1-M3-NETCLM]
```

- Any error mentioning 10001 port

- Any error that contains the "`OSError: [Errno 17] File exists: '/root/.fireball.keys'`" string. For example:

```
fatal: [BASE-CCP-T1-M1-NETCLM] => Traceback (most recent call last):
.
.
.
OSError: [Errno 17] File exists: '/root/.fireball.keys'
```

These are errors internal to Ansible and are random in occurrence.

Resolution

Secnario 1

If you experience one of these errors on any tiers except the HP Helion OpenStack controller tiers (which is `T1` in the Denver deployment and `T2` in Tahoe, Memphis and Sacramento deployments), do the following:

1. Kill the ansible run if its still going on using `Ctrl C`.
2. Execute the following from the lifecycle manager to remove the Ansible accelerate daemon, which runs on the nodes:

```
hlm deploy -c <cloudname> -t accelerate-mode
```

3. Execute the following command to restart the installation:

```
hlm deploy -c <cloudname> -r
```

Secnario 2

If you hit this issue at the very beginning of the HP Helion OpenStack controller tiers (which is `T1` in the Denver deployment and `T2` in Tahoe, Memphis and Sacramento deployments), **before** the `FND-MDB` or the `FND-RMQ` roles have run, do the following:

1. Kill the ansible run if its still going on using `Ctrl C`.
2. Execute the following from the lifecycle manager to remove the Ansible accelerate daemon, which runs on the nodes:

```
hlm deploy -c <cloudname> -t accelerate-mode
```

3. Execute the following command to restart the installation:

```
hlm deploy -c <cloudname> -r
```

Secnario 3

If you hit this issue at HP Helion OpenStack controller tiers (which is `T1` in the Denver deployment and `T2` in Tahoe, Memphis and Sacramento deployments), **after** the `FND-MDB` or the `FND-RMQ` roles have run, follow the steps in Scenario 1.

HP Helion OpenStack Carrier Grade installation (hlm deploy) fails at the Reload apache2 configuration task

System Behavior/Message

The installation of HPE Helion OpenStack Carrier Grade (the hlm deploy command) fails, with the following message:

```
Job for apache2 service failed
```

```
TASK: [Reload apache2 configuration] ****************************************
failed: [BASE-CCP-T2-M2-NETCLM] => {"failed": true}
msg: Job for apache2.service failed. See 'systemctl status apache2.service' and 'journalctl -xn' for details.

failed: [BASE-CCP-T2-M3-NETCLM] => {"failed": true}
msg: Job for apache2.service failed. See 'systemctl status apache2.service' and 'journalctl -xn' for details.

failed: [BASE-CCP-T2-M1-NETCLM] => {"failed": true}
msg: Job for apache2.service failed. See 'systemctl status apache2.service' and 'journalctl -xn' for details.


FATAL: all hosts have already failed -- aborting
```

Resolution

1. Execute the following command on each controller to restart apache2:

```
service apache2 restart
```

2. Execute the following command on the lifecycle manager to restart the installation:

```
hlm deploy -c <cloud_name> -r"
```

HP Helion OpenStack Carrier Grade installation (hlm deploy) fails at the install ntp client task

System Behavior/Message

The installation of HPE Helion OpenStack Carrier Grade (the hlm deploy command) fails, with the following message:

```
TASK: [Install ntp client]
 ******************************************************
Failed to launch the accelerated daemon on 10.200.187.105 (reason: failed to
 connect to the local socket file)
FATAL: all hosts have already failed - aborting
```

```
TASK: [Start iptables] ******************************************************
changed: [BASE-CCP-T2-M3-NETCLM]
changed: [BASE-CCP-T2-M1-NETCLM]
changed: [BASE-CCP-T2-M2-NETCLM]

TASK: [Start ufw] ***********************************************************
changed: [BASE-CCP-T2-M2-NETCLM]
changed: [BASE-CCP-T2-M3-NETCLM]
changed: [BASE-CCP-T2-M1-NETCLM]

TASK: [NTP-CLI] *************************************************************
changed: [BASE-CCP-T2-M1-NETCLM -> 127.0.0.1]

TASK: [Install ntp client] **************************************************
fatal: [BASE-CCP-T2-M3-NETCLM] => Failed to launch the accelerated daemon on 10.200.187.106 (reason: failed to connect to the local socket file)
fatal: [BASE-CCP-T2-M1-NETCLM] => Failed to launch the accelerated daemon on 10.200.187.104 (reason: failed to connect to the local socket file)
fatal: [BASE-CCP-T2-M2-NETCLM] => Failed to launch the accelerated daemon on 10.200.187.105 (reason: failed to connect to the local socket file)

FATAL: all hosts have already failed -- aborting
################################################
```

Resolution

1. Execute the following command on all nodes that failed, to disable firewall:

```
ufw disable
```

2. Execute the following from the lifecycle manager to remove the Ansible accelerate daemon, which runs on the nodes:

```
hlm deploy -c <cloudname> -t accelerate-mode
```

3. Execute the following command to restart the installation:

```
hlm deploy -c b30 -r
```

Installation fails at Ansible playbook

System Behavior/Message

The HP Helion OpenStack Carrier Grade installation fails during the HLM deployment (after executing the `ansible-playbook` command) with an error similar to the following.

```
TASK: [HLM-CREATE-ON-BM | Add hlm to the in-memory inventory of playbook]
 *****
ok: [192.168.122.1]
PLAY [hlm]
********************************* GATHERING FACTS
 ****************************
previous known host file not found
fatal: [192.168.122.240] => SSH encountered an unknown error during the
 connection.
We recommend you re-run the command using -vvvv, which will enable SSH
 debugging output to help diagnose the issue
TASK: [HLM-CFG | Delete existing interfaces file]
***************************** FATAL: no hosts matched or all hosts have
 already failed -- aborting
PLAY RECAP
 ********************************************************************
to retry, use: --limit @/root/setup_hlm_onBM.retry
192.168.122.1 : ok=18 changed=8 unreachable=0 failed=0
192.168.122.240 : ok=0 changed=0 unreachable=1 failed=0
```

Resolution

Perform the following steps:

1. Execute the following command to determine if the HLM VM was created:

   ```
   virsh list –all
   ```

   If the HLM VM appears in the output, delete the VM using the following commands:

   ```
   virsh destroy hlm
   virsh undefined hlm
   ```

2. Edit the `/root/infra-ansible-playbooks/setup_hlm_onBM.yml` file to comment the second role. The file contains two roles: the first one creates the VM and the second one configures the VM.

   ```
   hosts: hlm_kvm_host
   sudo: yes
   user: root
   roles:
   HLM-CREATE-ON-BM
   hosts: hlm
   #sudo: yes
   #user: root
   #roles:
   HLM-CFG
   ```

3. Again, run the `ansible-playbook –i hosts setup_hlm_onBM.yml`.
4. After the command completes, execute the following command to obtain the vibr0 IP address for the HLM

   ```
   arp | grep aa
   ```

   Copy the IP address you get in the output. 192.168.122.XXX
5. Edit the `/root/infra-ansible-playbooks/hosts` file to add the vibr0 IP address in the following manner:

   ```
   [vsd]
   10.10.10.10 ansible_ssh_user=root ansible_ssh_pass=Alcateldc
   ```

```
[hlm]
192.168.122.240 ansible_ssh_user=root ansible_ssh_pass=cghelion

[hlm_kvm_host]
192.168.122.1 #ansible_ssh_user=root ansible_ssh_pass=root
```

6. Edit the `setup_hlm_onBM.yml` to comment-out the first role and un-comment the second role.

```
hosts: hlm_kvm_host
sudo: yes
user: root
roles:
- HLM-CREATE-ON-BM
hosts: hlm
sudo: yes
user: root
roles:
HLM-CFG
```

7. Run `ansible-playbook -i hosts setup_hlm_onBM.yml` `HCG-909`

VM fails to get private/Fixed IP address

System Behavior/Message

After *configuring the VRS-G* during installation, the VRS-G VM is assigned with private and floating IP ddress, when seen on the VSD dashboard. However, if you launch a console session to the VM, there is no networking.

Resolution

Make sure the Glance image has the correct properties set. For example, check that the adapter type is `ide`. Also, check if gateway and subnet values are correctly assigned to VRSvAPPs.

VRSvAPPs missing in VSD dashboard

System Behavior/Message

While performing basic verification of cloud deployment, the VRSvAPPs might not appear in the VSD dashboard and the associated TUL addresses are not pingable from VRS-G node.

Resolution

This issue occurs if the VRSvAPP is not configured correctly.

Make sure all properties are populated corectly for the VRSvAPP VMs running in the ESX environment. Make sure there is a one-to-one mapping between each ESX host and a VRSvAPP.

See Also

For troubleshooting tips related to the HP Helion OpenStack cloud, see *HP Helion OpenStack: Troubleshooting*.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Set NoGway For Multi-NIC Subnets

VSD managed subnets:

1. Execute the following command to retreive the `APIKey` for VSD:

```
curl -k -s -u csproot:csproot -H "X-Nuage-Organization: csp" -X GET
 https://<VSD IP>:8443/nuage/api/v3_2/me | python -mjson.tool
```

For example:

```
curl -k -s -u csproot:csproot -H "X-Nuage-Organization: csp" -X GET
 https://10.10.4.21:8443/nuage/api/v3_2/me | python -mjson.tool
```

The output appears similar to:


```
[
    {
        "APIKey": "d7126af3-b8a4-42e4-b77b-d99308c1e83b",
        "APIKeyExpiry": 1447495809143,
        "ID": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "avatarData": null,
        "avatarType": null,
        "email": "csproot@CSP.com",
        "enterpriseID": "76046673-d0ea-4a67-b6af-2829952f0812",
        "enterpriseName": "CSP",
        "entityScope": null,
        "externalID": null,
        "externalId": null,
        "firstName": "csproot",
        "lastName": "csproot",
        "licenseCapabilities": [],
        "mobileNumber": null,
        "password": null,
        "role": "CSPROOT",
        "userName": "csproot"
    }
]
```


2. Use the following command to retrieve the subnets:

```
curl -k -s -u csproot:d7126af3-b8a4-42e4-b77b-d99308c1e83b -H "X-Nuage-
Organization: csp" -X GET https://10.10.4.21:8443/nuage/api/v3_2/subnets |
 python -mjson.tool
```

For example, the subnets in the following sample output are: `multinic1`, `multinic2`, and `multinic3` in the following example. The UUID for multinic2 is: `3370ba9e-17b4-4cec-86f0-6bfe63fc6989` and the UUID for multinic3 is: `176972b4-c532-4ceb-869a-a50990146bdb`


```
[
    {
        "ID": "3194f7ca-5952-4d3e-a62b-7986586fb6bb",
        "IPType": "IPV4",
        "PATEnabled": "INHERITED",
        "address": "10.29.51.0",
        "associatedApplicationID": null,
        "associatedApplicationObjectID": null,
        "associatedApplicationObjectType": null,
        "associatedMulticastChannelMapID": null,
        "associatedSharedNetworkResourceID": null,
        "children": null,
        "creationDate": 1447458421000,
        "description": null,
        "encryption": "INHERITED",
        "entityScope": "ENTERPRISE",
        "externalID": null,
        "gateway": "10.29.51.1",
        "gatewayMACAddress": "68:54:ED:00:00:07",
        "lastUpdatedBy": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "lastUpdatedDate": 1447458421000,
        "maintenanceMode": "DISABLED",
```

```
        "multicast": "INHERITED",
        "name": "multinicsub1",
        "netmask": "255.255.255.0",
        "owner": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "parentID": "cf9d99fa-24f6-4e1d-8451-823221f575d7",
        "parentType": "zone",
        "policyGroupID": 15,
        "proxyARP": false,
        "public": false,
        "routeDistinguisher": "65534:27816",
        "routeTarget": "65534:34072",
        "serviceID": 20034,
        "splitSubnet": false,
        "templateID": null,
        "underlayEnabled": "DISABLED",
        "vnId": 907660
    },
    {
        "ID": "3370ba9e-17b4-4cec-86f0-6bfe63fc6989",
        "IPType": "IPV4",
        "PATEnabled": "INHERITED",
        "address": "10.107.86.0",
        "associatedApplicationID": null,
        "associatedApplicationObjectID": null,
        "associatedApplicationObjectType": null,
        "associatedMulticastChannelMapID": null,
        "associatedSharedNetworkResourceID": null,
        "children": null,
        "creationDate": 1447458448000,
        "description": null,
        "encryption": "INHERITED",
        "entityScope": "ENTERPRISE",
        "externalID": null,
        "gateway": "10.107.86.1",
        "gatewayMACAddress": "68:54:ED:00:00:08",
        "lastUpdatedBy": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "lastUpdatedDate": 1447458448000,
        "maintenanceMode": "DISABLED",
        "multicast": "INHERITED",
        "name": "multinicsub2",
        "netmask": "255.255.255.0",
        "owner": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "parentID": "cf9d99fa-24f6-4e1d-8451-823221f575d7",
        "parentType": "zone",
        "policyGroupID": 16,
        "proxyARP": false,
        "public": false,
        "routeDistinguisher": "65534:61383",
        "routeTarget": "65534:30946",
        "serviceID": 20035,
        "splitSubnet": false,
        "templateID": null,
        "underlayEnabled": "DISABLED",
        "vnId": 590844
    },
    {
        "ID": "176972b4-c532-4ceb-869a-a50990146bdb",
        "IPType": "IPV4",
        "PATEnabled": "INHERITED",
        "address": "10.120.59.0",
        "associatedApplicationID": null,
        "associatedApplicationObjectID": null,
        "associatedApplicationObjectType": null,
        "associatedMulticastChannelMapID": null,
```

```
        "associatedSharedNetworkResourceID": null,
        "children": null,
        "creationDate": 1447458467000,
        "description": null,
        "encryption": "INHERITED",
        "entityScope": "ENTERPRISE",
        "externalID": null,
        "gateway": "10.120.59.1",
        "gatewayMACAddress": "68:54:ED:00:00:09",
        "lastUpdatedBy": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "lastUpdatedDate": 1447458467000,
        "maintenanceMode": "DISABLED",
        "multicast": "INHERITED",
        "name": "multinicsub3",
        "netmask": "255.255.255.0",
        "owner": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "parentID": "cf9d99fa-24f6-4e1d-8451-823221f575d7",
        "parentType": "zone",
        "policyGroupID": 17,
        "proxyARP": false,
        "public": false,
        "routeDistinguisher": "65534:49410",
        "routeTarget": "65534:33996",
        "serviceID": 20036,
        "splitSubnet": false,
        "templateID": null,
        "underlayEnabled": "DISABLED",
        "vnId": 739391
    }
]
```

Set the No Gateway Option on a Subnet

1. Get the dhcp options for a specific subnet:

```
curl -k -s -u csproot:d7126af3-b8a4-42e4-b77b-d99308c1e83b -H "X-
Nuage-Organization: csp" -X GET https://10.10.4.21:8443/nuage/api/v3_2/
subnets/3370ba9e-17b4-4cec-86f0-6bfe63fc6989/dhcpoptions | python -
mjson.tool
Blank output to begin with since we haven't set any dhcpoptions yet

POST - No default router (3)
curl -k -s -u csproot:d7126af3-b8a4-42e4-b77b-d99308c1e83b -
H "X-Nuage-Organization: csp" -H "Content-Type:application/
json" -d '{"type":"03","length":"01", "value":"00"}'
 -X POST https://10.10.4.21:8443/nuage/api/v3_2/
subnets/3370ba9e-17b4-4cec-86f0-6bfe63fc6989/dhcpoptions | python -
 mjson.tool
```

2. GET command to double check that dhcpoptions are set:

```
root@LR4TB1:~# curl -k -s -u csproot:d7126af3-b8a4-42e4-b77b-d99308c1e83b
 -H "X-Nuage-Organization: csp" -X GET https://10.10.4.21:8443/nuage/api/
v3_2/subnets/3370ba9e-17b4-4cec-86f0-6bfe63fc6989/dhcpoptions | python -
mjson.tool
[
    {
        "ID": "4db72abb-1f5e-438a-abb2-a98d075eb6ef",
        "actualType": 3,
        "actualValues": [
            "00"
        ],
        "children": null,
```

```
        "creationDate": 1447468134000,
        "entityScope": "ENTERPRISE",
        "externalID": null,
        "lastUpdatedBy": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "lastUpdatedDate": 1447468134000,
        "length": "01",
        "owner": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "parentID": "3370ba9e-17b4-4cec-86f0-6bfe63fc6989",
        "parentType": "subnet",
        "type": "03",
        "value": "00"
    }
]
```

3. Repeat on the multinic2

```
curl -k -s -u csproot:d7126af3-b8a4-42e4-b77b-d99308c1e83b -H "X-
Nuage-Organization: csp" -X GET https://10.10.4.21:8443/nuage/api/v3_2/
subnets/176972b4-c532-4ceb-869a-a50990146bdb/dhcpoptions | python -
mjson.tool

root@LR4TB1:~# curl -k -s -u csproot:d7126af3-b8a4-42e4-b77b-d99308c1e83b
 -H "X-Nuage-Organization: csp" -H "Content-Type:application/
json" -d '{"type":"03","length":"01", "value":"00"}' -X POST
 https://10.10.4.21:8443/nuage/api/v3_2/subnets/176972b4-c532-4ceb-869a-
a50990146bdb/dhcpoptions | python - mjson.tool
root@LR4TB1:~# curl -k -s -u csproot:d7126af3-b8a4-42e4-b77b-d99308c1e83b
 -H "X-Nuage-Organization: csp" -X GET https://10.10.4.21:8443/nuage/api/
v3_2/subnets/176972b4-c532-4ceb-869a-a50990146bdb/dhcpoptions | python -
mjson.tool
[
    {
        "ID": "7a9b15d2-bed2-44c7-8f27-4ed5ac642cc3",
        "actualType": 3,
        "actualValues": [
            "00"
        ],
        "children": null,
        "creationDate": 1447468321000,
        "entityScope": "ENTERPRISE",
        "externalID": null,
        "lastUpdatedBy": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "lastUpdatedDate": 1447468321000,
        "length": "01",
        "owner": "8a6f0e20-a4db-4878-ad84-9cc61756cd5e",
        "parentID": "176972b4-c532-4ceb-869a-a50990146bdb",
        "parentType": "subnet",
        "type": "03",
        "value": "00"
    }
]
```

Now multinicsub3 and multinicsub3 are set to NO DEFAULT GW entry.

4. Post this operation launch a VM with multinicsub1,multinicsub2,multinicsub3 only multinicsub1 should get GW route entry for the VM.
5. Assign FIP to this multinicsub1 IP.

HP Helion OpenStack® Carrier Grade 2.1 Beta: Open Source and Third-Party Software License Agreements

HP Helion OpenStack® Carrier Grade: Open Source and Third-Party Software License Agreements

The Open Source and Third-Party Software License Agreements for HP Helion OpenStack Carrier Grade are available as a PDF download:

Download the PDF Document

HP Helion OpenStack® Carrier Grade 2.1 Beta: Software License Terms

HP Helion OpenStack® Carrier Grade: Software License Terms

The HP Helion OpenStack Carrier Grade end user license agreement is available as a *PDF download*.

HP Helion OpenStack® Carrier Grade 2.0

File for attaching linked topics not in TOC