HP Helion OpenStack® Carrier Grade 1.1: Installation Guide

Contents

HP Helion OpenStack® Carrier Grade 1.1: Installation Guide

This document describes the process for installing HP Helion OpenStack Carrier Grade in a baremetal environment in the Non-KVM region.

About the installation

The HP Helion OpenStack Carrier Grade installation installs HP Helion Lifecycle Management, creates a base HP Helion OpenStack cloud, and configures network virtualization through HP Distributed Cloud Networking. Using a separate installation, you integrate KVM servers into the HP Helion OpenStack Carrier Grade environment.

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

Installation process

Use the following process to install HP Helion OpenStack Carrier Grade in a baremetal environment.

1. Review the *Technical Overview* for information on the HP Helion OpenStack Carrier Grade environment.
2. Review the *Support Matrix* to make sure your environment meets the minimum requirements.
3. Perform any required or optional *Installation Prerequisites*.
4. *Preparing the Network for Installation*
5. Install the *Non-KVM region*.
6. Install the *KVM region*.
7. *HLM Post-Installation Tasks*

About Installation Logging

For all scripts that are executed (including `hlm-build` and `h*` scripts below), separate log files are generated on `/var/log/hlm/` folder.

For example, if you run the `hprovsion` command, all command line output will also be logged in `/var/log/hlm/hprovision.log` file.

The following is the list of scripts for which logging is implemented:

- hlm_updatepackages.sh
- hlm_initcobbler.sh
- hlm_importiso.sh
- hlm_prepareenv.sh
- hnewcloud
- hprovision
- hcfgproc
- hnetinit

First Step

Before you start, make sure your environment meets the hardware and software requirements. See the *Technical Overview*.

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Installation Guide

This document describes the process for installing HP Helion OpenStack Carrier Grade in a baremetal environment in the Non-KVM region.

About the installation

The HP Helion OpenStack Carrier Grade installation installs HP Helion Lifecycle Management, creates a base HP Helion OpenStack cloud, and configures network virtualization through HP Distributed Cloud Networking. Using a separate installation, you integrate KVM servers into the HP Helion OpenStack Carrier Grade environment.

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

Installation process

Use the following process to install HP Helion OpenStack Carrier Grade in a baremetal environment.

1. Review the *Technical Overview* for information on the HP Helion OpenStack Carrier Grade environment.
2. Review the *Support Matrix* to make sure your environment meets the minimum requirements.
3. Perform any required or optional *Installation Prerequisites*.
4. *Preparing the Network for Installation*
5. Install the *Non-KVM region*.
6. Install the *KVM region*.
7. *HLM Post-Installation Tasks*

About Installation Logging

For all scripts that are executed (including `hlm-build` and `h*` scripts below), separate log files are generated on `/var/log/hlm/` folder.

For example, if you run the `hprovsion` command, all command line output will also be logged in `/var/log/hlm/hprovision.log` file.

The following is the list of scripts for which logging is implemented:

- hlm_updatepackages.sh
- hlm_initcobbler.sh
- hlm_importiso.sh
- hlm_prepareenv.sh
- hnewcloud
- hprovision
- hcfgproc
- hnetinit

First Step

Before you start, make sure your environment meets the hardware and software requirements. See the *Technical Overview*.

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Support Matrix

To ensure the performance and stability of the HP Lifecycle Management environment, it is very important to meet the requirements and conform to the recommendations listed in *Support Matrix for the KVM Host*.

Support Matrix for the Non-KVM Region Region

To ensure the performance and stability of the Non-KVM servers running the HP Lifecycle Management environment and HP Helion OpenStack it is important to meet the requirements and conform to the recommendations listed in *Support Matrix for the Non-KVM Region*.

Support Matrix for the KVM Region

To ensure the performance and stability of the systems running KVM region of the HP Helion OpenStack Carrier Grade environment, it is very important to meet the requirements and conform to the recommendations listed in *Support Matrix for the KVM Region*.

Next Step

Installation Prerequisites

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Support Matrix for the Non-KVM Region

Support Matrix for the HLM Host

▲ *HP Helion OpenStack Carrier Grade 1.1: Support Matrix* | *Support Matrix for the KVM Region #*

To ensure the performance and stability of the HP Lifecycle Management, it is very important to meet the requirements and conform to the following recommendations.

Software Requirements

The HLM Host is a computer running Ubuntu Server 14.04.2 LTS. The following packages are also required:

- ntp
- firefox
- gedit
- xrdp
- xfce4
- qemu-kvm
- libvirt-bin
- openvswitch-switch
- openvswitch-common
- python-libvirt
- qemu-system-x86
- libssl-dev
- libffi-dev
- git
- python-virtualenv
- python-dev virt-manager

Supported Hardware

The following servers are supported for use as the HLM host in the current release.

Node Type	Role	Required Number	Server Hardware	Minimum Requirements and Recommendations
HLM Host	Installation/ Management	1	Disk	20 GB
			Memory	4,096 MB
			Network	
			CPU	

Return to Top

Support Matrix for HP Helion OpenStack

To ensure the performance and stability of the HP Helion OpenStack environment, it is very important to meet the requirements and conform to the following recommendations.

This page provides an overview of the hardware and software that is supported for HP Helion OpenStack including setup and configuration information.

Supported Hardware

The following hardware has been tested and verified to work with HP Helion OpenStack

HP Helion OpenStack Region

For the HP Helion OpenStack Region, the following servers are supported for the current release.

HP ProLiant BladeSystem

- *BL460c Gen8*
- *BL460c Gen9*

HP ProLiant Rack Servers

- *DL360 Gen9*
- *DL380 Gen9*
- *DL360 Gen8*
- *DL380 Gen8*

Gen 8 or Gen 9 versions of DL360's or DL380s are required for the nodes that make up the control plane (including non-KVM region related control plan). If you are using Gen9 systens, you must update the Snap3 firmware.

For compute nodes the either Gen 8 or Gen9 : DL360's BL460's are required.

Hardware Requirements for the Non-KVM Region

You must have the following hardware configuration:

- 3 baremetal systems meeting the requirements as listed below.
- For systems with multiple NICs, only one NIC may be active or connected. Compute nodes need to have Intel 82599 10G NICs
- Capable of hosting VMs
- For Compute nodes, Intel or AMD hardware virtualization support required. The CPU cores and memory requirements must be sized based on the VM instances hosted by the Compute node.

Important: Since the installer currently uses only the first available disk, all servers must have RAID controllers pre-configured to present their storage as a single, logical disk. RAID across multiple physical discs is strongly recommended for both performance and resilience.

On the controller and compute nodes, make sure the RAID array is configured to reflect a total size of less than 4TB.

The following table lists the minimum requirements required for installation of each type of node. See the *Technical Overview* for an architecture diagram.

For a GEN9 Rackmount Base

Component	Description
16 x DL360 G9 (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) • 1 x FlexFabric 10Gb 2-port 556FLR-SFP • 1 x Smart Array P440ar/2G FIO Controller • 2 x Ethernet 10Gb 2P 560SFP
6 x DL360 G9(Control)	• 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
TOR Switches	• 6 x 5920AF-24XG Switch • 2 x FF 5930-32QSFP+ Switch
Storage	1 x 3PAR 7400

HP Helion Carrier Grade Platform

GEN9 Enclosure Based

Component	Description
2 x C7000 Enclosure (Compute)	• 2 x Virtual Connect FlexFabric-20/40 F8 Module • 4 x 6125XLG Blade Switch
16 x BL460 G9 (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 FlexFabric 20Gb 2-port 650FLB • 2 x Ethernet 10Gb 2P 560M
6 x DL360 G9 (Control)	• 2 x Intel Xeon® E5-2640v3 • 8 x 16GB (1x16GB) Dual Rank x4 DDR4-2133 memory

Component	Description
	• 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
TOR Switches	• 6 x 5920AF-24XG Switch • 2 x FF 5930-32QSFP+ Switch
Storage	• 1 x 3PAR 7400

Notes:

- For installations with HLM hypervisor support, one or more additional nodes are required for VSA block storage.
- After the installation is complete, you can use the Block Storage and Object Operation services to add further storage capacity as allowed by your hardware.

Software Requirements

There are no software requirements for the servers where the HP Helion OpenStack region will be installed because all required software is contained within the images deployed on the system.

The servers should be baremetal before installation.

Guest OS Support Matrix

For HP Helion OpenStack Guest OS. See *Support Matrix for the KVM region*.

Next Step

Review the *Technical Overview*.

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Support Matrix for the KVM Region

▲ *HP Helion OpenStack Carrier Grade 1.1: Support Matrix* | *Support Matrix for the Non-KVM Region #*

To ensure the performance and stability of the systems running in the KVM region of the HP Helion OpenStack Carrier Grade environment, it is very important to meet the requirements and conform to the following recommendations.

Supported Hardware Platforms

The following is the list of certified platforms for running HP Helion OpenStack Carrier Grade in the KVM region:

Table 1: HP Helion OpenStack Carrier Grade Certified Hardware Platforms

Manufacturer	Platform
Hewlett-Packard	HP360 Proliant DL360P Gen8 Server
	HP360 Proliant DL360P Gen9 Server
	HP380 Proliant DL380P Gen8 Server
	HP380 Proliant DL380P Gen9 Server

The following NICs have been verified for PXE booting:

- Broadcom 1G
- Broadcom 10G
- Emulex 10G
- Intel 82599
- Intel i350

Supported Hardware Configuration

HP Helion OpenStack Carrier Grade has been verified to work using the following hardware configuration:

- The required number of controller nodes is two.
- The required number of storage nodes is two. Storage nodes are optional, depending on storage needs.
- The verified number of compute nodes is 20.
- For predictable performance, it is recommended to disable hyper-threading in the BIOS of all nodes in the cluster.

Supported System Configuration

HP Helion OpenStack Carrier Grade has been verified to work using the following system configuration:

- two controllers
- 20 compute nodes with dual Intel(R) Xeon(R) CPU E5-2670 v2 and E5-2640v3
- 200 virtual machine instances
- up to four physical ports per compute node
- maximum eight AVP vNICs per guest
- maximum eight SR-IOV vNICs per guest
- maximum 32 VFs per NIC

Supported Guest OSs

The following Guest OSs are supported by HP Helion OpenStack Carrier Grade:

- KVM 6.0
- KVM 5.0
- CentOS 6.4
- Fedora 19
- RHEL 6.5
- OpenSUSE 12.3

Requirements for specific guest OSs are included in the SDK README files.

Performance Considerations

The nature of the guest applications, their processing and storage demands, and other configuration factors can affect the overall performance of the HP Helion OpenStack Carrier Grade cluster.

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Technical Overview

This page introduces you to HP Helion OpenStack Carrier Grade, a carrier-grade distribution of OpenStack the leading open source cloud computing platform.

For more information on the HP Helion OpenStack Carrier Grade environment, also see the Reference Logical Architecture section in the *HP Helion OpenStack Carrier Grade 1.1: Administrator Guide*.

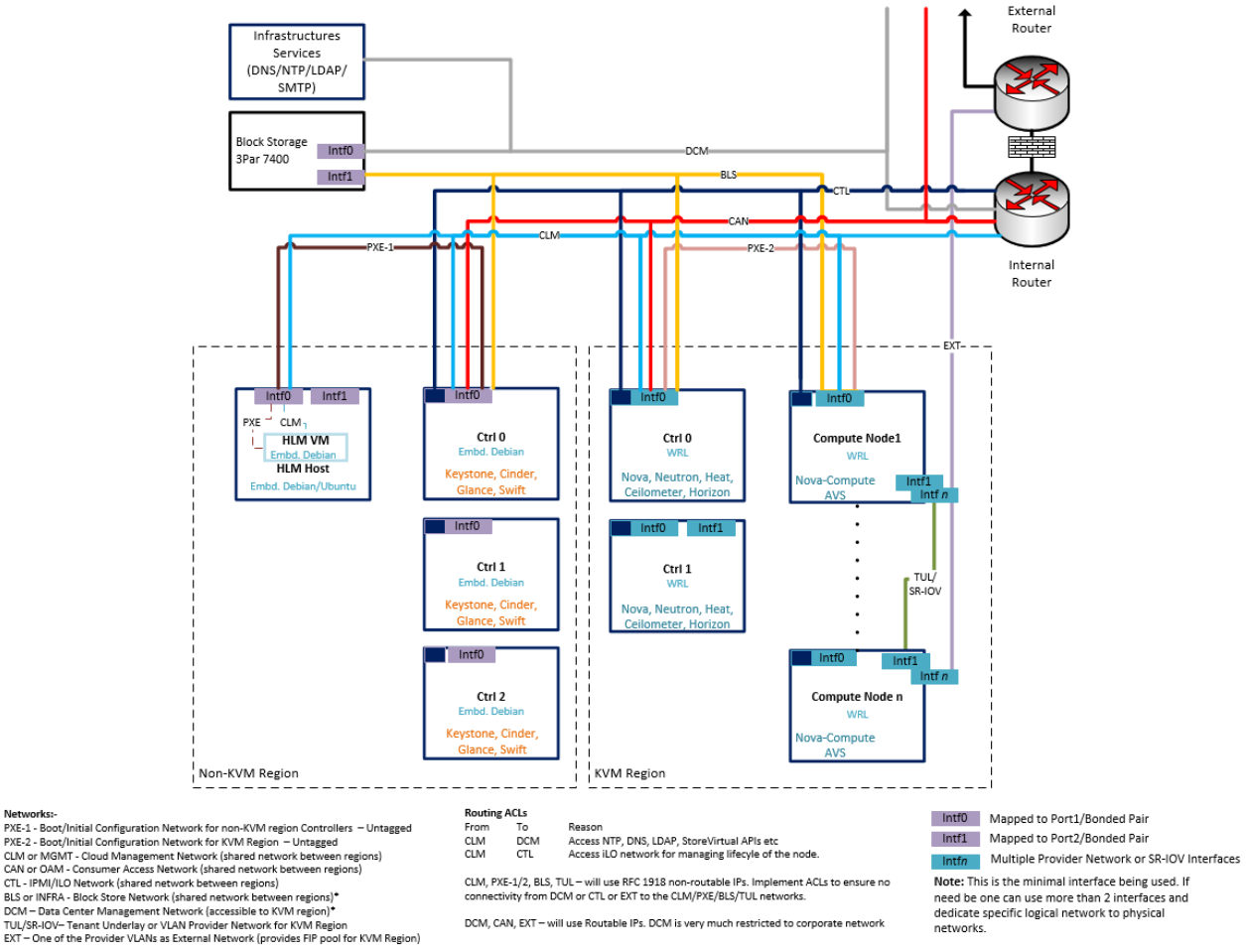
HP Helion OpenStack Carrier Grade services- functional overview

The following table outlines the functionality of HP Helion OpenStack Carrier Grade services based on the type of users - Users and Administrators. For a complete description of these services, see the *Services Overview* page.

Deployment architecture

You can deploy HP Helion OpenStack Carrier Grade on a *KVM hypervisor*.

The following diagram depicts a simplified deployment scenario using KVM.



Networks:-
PXE-1 - Boot/Initial Configuration Network for non-KVM region Controllers – Untagged
PXE-2 - Boot/Initial Configuration Network for KVM Region – Untagged
CLM or MGMT - Cloud Management Network (shared network between regions)
CAN or OAM - Consumer Access Network (shared network between regions)
CTL - IPMI/ILO Network (shared network between regions)
BLS or INFRA - Block Store Network (shared network between regions)*
DCM – Data Center Management Network (accessible to KVM region)*
TUL/SR-IOV– Tenant Underlay or VLAN Provider Network for KVM Region
EXT – One of the Provider VLANs as External Network (provides FIP pool for KVM Region)

Routing ACLs

From	To	Reason
CLM	DCM	Access NTP, DNS, LDAP, StoreVirtual APIs etc
CLM	CTL	Access iLO network for managing lifecyle of the node.

CLM, PXE-1/2, BLS, TUL – will use RFC 1918 non-routable IPs. Implement ACLs to ensure no connectivity from DCM or CTL or EXT to the CLM/PXE/BLS/TUL networks.

DCM, CAN, EXT – will use Routable IPs. DCM is very much restricted to corporate network

Intf0 Mapped to Port1/Bonded Pair
Intf1 Mapped to Port2/Bonded Pair
Intfn Multiple Provider Network or SR-IOV Interfaces

Note: This is the minimal interface being used. If need be one can use more than 2 interfaces and dedicate specific logical network to physical networks.

Network architecture

The following information describes the network configuration for the *physical networks* and *virtual networks*, which must be configured by the network administrator.

Network	Description
CLM / OBS	Cloud Management and Object Store Network -- Untagged (Private)
PXE	Boot/initial configuration network. Untagged

Network	Description
CAN	Consumer Access Network (shared with WR - OAM)
CTL	IPMI/iLO network (shared with WR)
BLS	Block Storage Network; can be on a separate interface (`intf*`)
DCM	Data Center Management network (accessible to WR region) and route across multi-DC
WR-TUL/SR-IOV (Swift)	Tenant Underlay Network from WR region
WR-PXE	Boot/Cloud Management network for WR Cloud/Region -- Untagged
WR-EXT	External network (FIP network for WR region)

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.

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, PXE, OBS, BLS, WR-PXE, WR-INFRA, WR-TUL will use RFC 1918 non-routable IPs to prevent access to the CLM network from DCM, CLT, or EXT.

Ethernet Interfaces

All hosts in the server 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. It assumes that the ports used to connect to the internal management network are on-board 1 GB ports.

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 1G on-board interface (Internal management network)	• Two 1G on-board interfaces (Internalmanagement network)

Personality	Basic Scenario	LAG Scenario
	• One 1G interface (OAM) • One optional 1G or 10G interface (Infrastructure network)	• Two 1G interfaces (OAM) • Two optional 1G or 10G interfaces (Infrastructure network) NOTE: The controller-0 and controller-1 port configurations must be identical.
Compute Node	• One 1G on-board interface (Internal management network) • One 1G (Intel i350) or 10G (Intel 82599) interface per additional Provider Network	• Two 1G on-board interfaces (Internal management network) • Two 1G (Intel i350) or 10G (Intel 82599) interfaces per additional 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, HP360 or HP380 servers equipped with HP 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 of the Titanium Server incorporates up to five 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 BOOTP, 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 1Gb or 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

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 1Gb or 10 Gb Ethernet network. In its absence, all infrastructure traffic is carried over the internal management network.

OAM Network

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

- DNS Service - Needed to facilitate the name resolution of servers reachable on the 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 de-facto 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.

Next step

For more information of Hardware configurations see the *Support Matrix*.

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Installation Prerequisites

This document describes the prerequisite steps and one time setup on your HLM host 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 baremetal systems

Perform the following tasks on each baremetal system before starting the install:

- Configure the boot order with Network/PXE boot as the first option:
  - For example, to set the boot order for a HP SL390, from the iLO prompt enter `set system1/bootconfig1/bootsource5 bootorder=1`.
  - To unset, enter `set system1/bootconfig1/bootsource5 bootorder=5`.

- Configure the BIOS:
  - to the correct date and time
  - HLM host configured in 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 formware.

Preparing the HLM host

The following tasks need to be performed on the HLM host, the system where the you will launch the HP Helion OpenStack Carrier Grade installation.

- Install Ubuntu Server 14.04.2 LTS
- Configure SSH
- Obtain a public key
- Install Debian/Ubuntu packages
- Configure the xrdp display
- Install and configure NTP
- Configure proxy information
- Set DNS servers name-resolution
- Disabling SR-IOV

Install Ubuntu Server 14.04.2 LTS

The HLM 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 HLM host, if necessary configure the proxy information for your environment using the following steps:

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

   ```
   sudo su -
   ```

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

   ```
   PATH="/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,<HLM_host_IP_address>,<provider_network>
   ```

   Where:

   ```
   <web_proxy_IP> is your web proxy IP address.
   <HLM_host_IP_address is the IP address of the HLM Host
   ```

3. Source the `environments` file:

   ```
   source /etc/environment
   ```

Install Ubuntu packages

Before starting the installation, you must first install Ubuntu.

1. Run the following all in one command to install packages:

```
sudo su -l -c "apt-get install -y ntp firefox gedit xrdp xfce4 qemu-kvm
 libvirt-bin openvswitch-switch openvswitch-common 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 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 HLM host to activate the proxy configuration.

Configure the XRDP remote desktop display

Configure XRDP for the remote desktop connection to access the server remotely as follows.

1. Edit the `sesman.ini` file:

   vi /etc/xrdp/sesman.ini

   a. Update the `MaxSessions=1` to `MaxSessions=50`.

   b. Configure the system to use XRDP:

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

   c. Save and close the file.
2. Restart the XDRP service:

   sudo /etc/init.d/xrdp restart

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

Make sure you add a space after "." then restart XDRP:

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

Install and configure NTP

NTP is a networking protocol for clock synchronization between computer systems.

The HP Helion OpenStack cloud nodes must be configured as NTP clients and point to the same NTP server.

You can install NTP on the HLM host and configure it as an NTP server. Or, you can use a pre-existing NTP server that is reachable from the management network. You will also need to configure the undercloud and overcloud systems as NTP clients pointing to the NTP server you have chosen to use during the installation process.

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

Download and unpack the installation packages

Before you begin, you must download the required HP Helion OpenStack installation package(s):

1. Download and extract the `cg-hlm.qcow2` file to the images folder: `/var/lib/libvirt/images`.
2. Download and extract the `cg-infra-playbooks.tar.gz.gpg` file to the `/root` directory.
3. Decrypt and untar the PGP file using password cghelion when prompted.

```
gpg -d cg-infra-playbooks.tar.gz.gpg | tar -xzvf
```

4. Copy the `cg-hos.tar.gz.gpg` to the `/root/cg/` directory.

Configure SSH

On the HLM 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`:

```
PermitRootLogin yes
```

2. In the `sshd_config` file, set the following variables:

```
# Authentication:
LoginGraceTime 120
#PermitRootLogin without-password
StrictModes no
```

3. Disable strict host key checking:

   a. Navigate to the `config` file:

```
cd ~/.ssh/config
```

   b. Set the `StrictHostKeyChecking` variable to No:

```
StrictHostKeyChecking no
```

4. Restart SSH service

```
service ssh restart
```

5. 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 for passphrase

   d. Press enter again 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.

Next Step

Preparing the Network for Installation

HP Helion OpenStack® Carrier Grade 1.1: Preparing the Network for Installation

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

Configure VLAN networking on the KVM host

1. Edit `/etc/network/interfaces` file to provide network details on the each interface:

```
auto lo
iface lo inet loopback

# The primary network interface
auto br-pxe
allow-ovs br-pxe
iface br-pxe inet static
address <IP_address>
netmask <Netmask>
gateway <IP_address>
ovs_type OVSBridge
ovs_ports em1

#Bring up interface online
allow-br-pxe em1
iface em1 inet manual
ovs_bridge br-pxe
ovs_type OVSPort

auto br-clm
allow-ovs br-clm
iface br-clm inet manual
ovs_type OVSBridge
ovs_ports em1.<CLM_VLAN_ID>

allow-br-clm em1.<CLM_VLAN_ID>
iface em1.<CLM_VLAN_ID> inet manual
ovs_bridge br-clm
ovs_type OVSPort

auto br-bls
allow-osv br-bls
iface br-bls inet manual
ovs_type OVSBridge
ovs_ports em1.<BLS_VLAN_ID>

allow-br-bls em1.<BLS_VLAN_ID>
iface em1.<BLS_VLAN_ID> inet manual
ovs_bridge br-bls
ovs_type OVSPort

auto br-dcm
allow-osv br-dcm
iface br-dcm inet manual
ovs_type OVSBridge
ovs_ports em1.1550
```

```
allow-br-dcm em1.1550
iface em1.1550 inet manual
ovs_bridge br-dcm
ovs_type OVSPort
```

Example:

```
auto lo
iface lo inet loopback

# The primary network interface
auto br-pxe
allow-ovs br-pxe
iface br-pxe inet static
address 10.200.183.11
netmask 255.255.255.0
gateway 10.200.183.1
ovs_type OVSBridge
ovs_ports em1

#Bring up interface online
allow-br-pxe em1
iface em1 inet manual
ovs_bridge br-pxe
ovs_type OVSPort

auto br-clm
allow-ovs br-clm
iface br-clm inet manual
ovs_type OVSBridge
ovs_ports em1.1551

allow-br-clm em1.1551
iface em1.1551 inet manual
ovs_bridge br-clm
ovs_type OVSPort

auto br-bls
allow-osv br-bls
iface br-bls inet manual
ovs_type OVSBridge
ovs_ports em1.1554

allow-br-bls em1.1554
iface em1.1554 inet manual
ovs_bridge br-bls
ovs_type OVSPort

auto br-dcm
allow-osv br-dcm
iface br-dcm inet manual
ovs_type OVSBridge
ovs_ports em1.1550

allow-br-dcm em1.1550
iface em1.1550 inet manual
ovs_bridge br-dcm
ovs_type OVSPort
```

2. Execute the following command to check the output

```
ovs-vsctl show
```

706add53-21a4-4062-9149-d7bd77896076 ovs_version: "2.0.2"

Create the networks for associating with the HLM virtual machine

The installation process will create a virtual machine for HP Helion Lifecycle Management.

Perform the following steps to enable networks that will be associated with HLM VM.

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

   sudo su -
2. Create the `br-clm` network by creating an XML definition file:

   a. Create the XML file

```
cat br-clm.xml
    <network>
        <name>br-clm</name>
        <forward mode='bridge'/>
        <bridge name='br-clm'/>
        <virtualport type='openvswitch'/>
    </network>
```

   b. Execute the following commands to create and start the network, and configure the network to auto-start

```
virsh net-define br-clm.xml
virsh net-start br-clm
virsh net-autostart br-clm
```

3. Create the `br-bls` network by creating an XML definition file:

   a. Create the XML file

```
cat br-bls.xml
    <network>
        <name>br-bls</name>
        <forward mode='bridge'/>
        <bridge name='br-bls'/>
        <virtualport type='openvswitch'/>
    </network>
```

   b. Execute the following commands to create and start the network, and configure the network to auto-start

```
virsh net-define br-bls.xml
virsh net-start br-bls
virsh net-autostart br-bls
```

4. Create the `br-pxe` network by creating an XML definition file:

   a. Create the XML file

```
cat br-pxe.xml
    <network>
        <name>br-pxe</name>
        <forward mode='bridge'/>
        <bridge name='br-pxe'/>
        <virtualport type='openvswitch'/>
    </network>
```

b. Execute the following commands to create and start the network, and configure the network to auto-start

```
virsh net-define br-pxe.xml
virsh net-start br-pxe
virsh net-autostart br-pxe
```

5. Create the `br-dcm` network by creating an XML definition file:

   a. Create the XML file

```
cat br-dcm.xml
    <network>
        <name>br-dcm</name>
        <forward mode='bridge'/>
        <bridge name='br-dcm'/>
        <virtualport type='openvswitch'/>
    </network>
```

   b. Execute the following commands to create and start the network, and configure the network to auto-start

```
virsh net-define br-dcm.xml
virsh net-start br-dcm
virsh net-autostart br-dcm
```

6. Use the `virsh net-list` command to view information on the new networks:

```
virsh net-list

Name         State       Autostart       Persistent
----------------------------------------------------------
br-bls       active      yes             yes
br-clm       active      yes             yes
br-dcm       active      yes             yes
br-pxe       active      yes             yes
default      active      yes             yes
```

7. Execute the following command to make sure the `br-pxe` network has been assigned an IP address:

```
ifconfig br-pxe
```

   Run following command if the `br-pxe` does not indicate the IP address has been assigned.

```
ifdown br-pxe
ifdown <interface>
ifup br-pxe
ifup <yourinterface>
```

8. Execute the following command to make sure the `br-pxe` network was assigned the IP address of the primary interface.

```
ifconfig | more
```

9. Reboot the setup.
10. Execute the following command to make sure the primary interface does not have IP address and confirm the IP address of the `br-pxe` network:

```
ifconfig | more
```

11. Execute the following command to view the routing table. Make sure all of the networks are configured as expected.

```
Route -n
```

12. Execute the following command to
13. Execute the following command to make sure the VLAN ID is as expected.

    ovs-vsctl show
14. The output should apprea similar to the following:

```
Bridge br-clm
    Port "vnet2"
        Interface "vnet2"
    Port "em1.1551"
        Interface "em1.1551"
    Port br-clm
        Interface br-clm
            type: internal
Bridge br-pxe
    Port br-pxe
        Interface br-pxe
            type: internal
    Port "vnet1"
        Interface "vnet1"
    Port "em1"
        Interface "em1"
Bridge br-dcm
    Port br-dcm
        Interface br-dcm
            type: internal
    Port "em1.1550"
        Interface "em1.1550"
    Port "vnet3"
        Interface "vnet3"
Bridge br-bls
    Port "em1.1554"
        Interface "em1.1554"
    Port br-bls
        Interface br-bls
            type: internal
ovs_version: "2.0.2"
```

Note: If `ovs-vsctl show` does not show all the required bridges, bring up the interface where the bridge does not appear:

```
ifup br-bls
ifup br-dcm
ifup br-clm
```

Networking Issues Ubuntu 14.04

Open vSwitch 2.0.x with bridge is not able to ping or SSH after reboot or running Anisble playbooks to create new bridges. This is a known issue in the Ubuntu community. For more details on the issue, see *Networking does not restart*.

1. Use the `ifdown` command to make sure the routing table is clean for all interfaces and only the `virbr0 192.168.122.0 net` displays.
2. Manually assign the IP addresses used previously, as shown in the following examples:

```
ip addr add 10.10.10.10/24 dev em1
ip link set em1 up
route add -net default gw 10.10.10.1
apt-get purge openvswitch-switch openvswitch-common
apt-get update
apt-get install openvswitch-switch
ip addr flush dev em1
ifup br-pxe
ifup br-bls
ifup br-clm
ifup br-dcm
```

Networking will be restored through thE OVS Bridge

Next Step

Configuring NTP

Return to Top

HP Helion OpenStack® Carrier Grade: Configuring NTP

This page provides detailed information on *configuring HP Helion OpenStack Carrier Grade nodes* for Network Time Protocol (NTP) and *instlling an NTP server on the seed cloud host*.

NTP is a networking protocol for clock synchronization between computer systems. The undercloud and overcloud systems are configured as NTP clients during the installation process.

HP Helion OpenStack Carrier Grade requires that all nodes point to the same NTP server. You can use an external NTP server or configure the seed cloud host as a server.

Notes:

- NTP clients should use only stratum 2 and higher servers (meaning stratum 1 or stratum 0).
- All the Helion servers use UTC as a time zone.

Install an NTP server on the seed

To configure an NTP server, follow these steps:

1. Log in to the HLM host.

```
sudo su -
```

2. Install the NTP package using the following command:

```
sudo apt-get install ntp
```

3. Add NTP servers to `/etc/ntp.conf`. The following example use servers from the NTP Pool Project:

```
server ntp.ubuntu.com
server 127.127.1.0
```

Note: The NTP stratum must be numerically lower than 10 (meaning stratum 9, stratum 8, etc.) in order to use as a source. If one is not available, you may be able to *fudge one*.

4. Configure system time zone using the `tzselect` command.

   a. Change to the /usr/bin/` directory.

b. Execute the `tzselect` command. The available time zones are listed.

c. Select from the listed time zones by entering a number at the promnpt.

The output should be placed in `/etc/profile` and executed on the command line.

```
source /etc/profile
```

5. Verify that your server is broadcasting using the `ntpq -p` command. You should see a message similar to the following:

```
ntpq -p
remote  refid   st  t   when    poll    reach   delay   offset  jitter
==============================================================================
*ops-ae1ops-ntp0    209.51.161.238  2   u   242 1024    377 0.509   0.043
  0.206
LOCAL(0)    .LOCL.  10  l   76h 64  0   0.000   0.000   0.000
```

You can now point clients to your NTP server

Configure all other nodes as NTP clients

1. SSH to the node you want to configure.
2. Add your NTP server IP to the clients `/etc/ntp.conf` file.
3. Configure system time zone using the `tzselect` command.

a. Change to the /usr/bin/` directory.

b. Execute the `tzselect` command. The available time zones are listed.

c. Select from the listed time zones by entering a number at the promnpt.

The output should be placed in `/etc/profile` and executed on the command line.

```
source /etc/profile
```

4. Restart the NTP service.

```
service ntp restart
```

5. Verify that you have a connection to the NTP server.

```
ntpq -pd

1 packets reassembled into response
remote  refid   st  t   when    poll    reach   delay   offset  jitter
==============================================================================
2 packets reassembled into response
+ntp0 209.51.161.238    2   u   82  1024    377 0.286   0.117   0.349
```

6. Verify that your server shows client connections.

```
ntpdc -c monlist

ntpdc -c monlist
remote address  port    local address   count   m   ver rstr    avgint
 lstint
===============================================================================
ntp0001.use 123 10.22.170.17    2365    4   4   1d0 1000    384
```

Fudging a stratum lower than 10

NTP uses a hierarchical, semi-layered system of time sources. Each level of this hierarchy is termed a *stratum* and is assigned a number starting with zero at the top. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy.

The numerically lower the stratum value, the higher priority that clock has.

HP Helion OpenStack uses stratum 10. Using a numerically high stratum ensures that this is only used if all external clocks fail. This will mitigate skew until external clocks return to service.

If your NTP stratum is numerically less than 10, set up your host as the time source by fudging a stratum 10.

1. Configure host as a time source.
2. Add the following to /etc/ntp.conf to force a stratum 10.

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
```

3. Restart the NTP service

```
service ntp restart
```

Using `fudge` to configure the local clock as stratum 10 makes NTP use the local clock when no timeservers are available. The system will only use the local clock if your system cannot access the NTP server.

Next Step

Deploying the Non-KVM Region

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Deploying the Non-KVM Region

The first phase of the HP Helion Openstack Carrier Grade installation involves creating a virtual machine for the Helion Lifecycle Management (HLM) and then deploying the HP Helion Openstack cloud.

HLM consists of the ongoing operations/maintenance as well as the initial deployment of the HP Helion OpenStack Carrier Grade system.

Prepare the system for deployment

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

1. 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. Make sure the `hlm_kvm_host` value is configured properly.
2. Check the hosts file `/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. Make sure the DCM network details are correct. Also, verify the CLM IP address in this file.

```
[hlm_kvm_host]
192.168.122.1
```

Deploy the HLM Virtual Machine

Use the following steps to deploy the HLM VM on the HLM Host using Ansible playbooks.

1. Make sure the Ansible playbook file is not in executable mode.

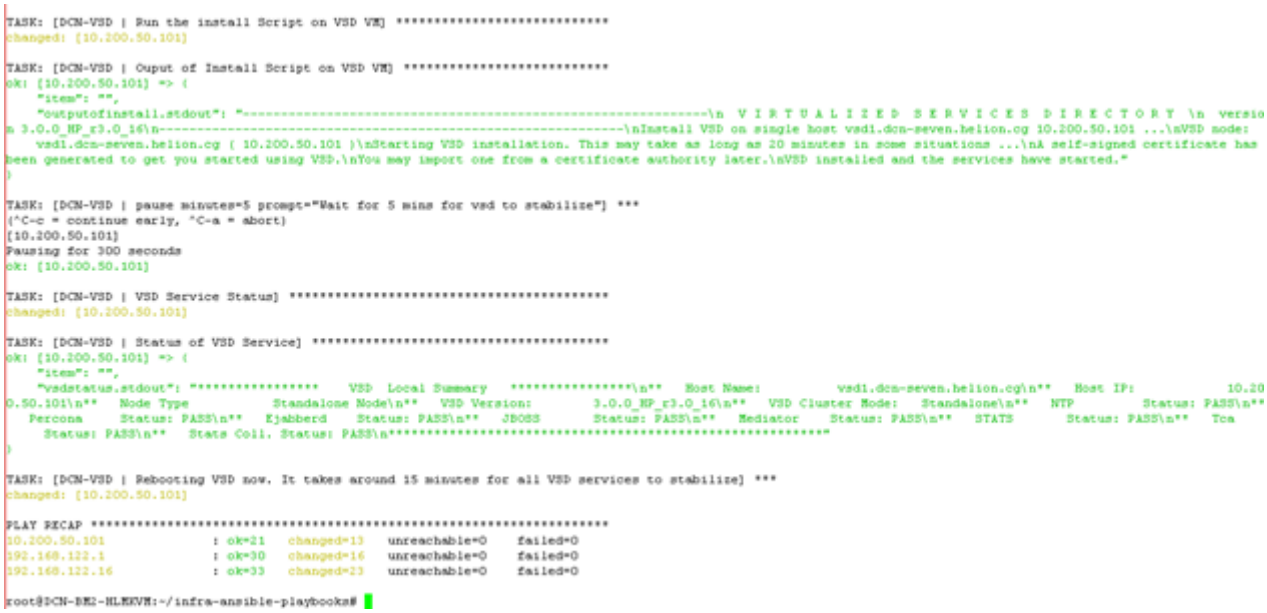
2. Execute the following command:

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

The command will do the following:

- Copy both installation files (tar balls) to the HLM host, decrypt, and extract the files.
- Execute the `updatepackages` command.
- Execute the `prepareenv` command.
- Execute the `Init cobbler` command.
- Execute the `Importiso` command.

You will see similar message when the playbook is run successful.



Configure a JSON file for installation

The HP Helion OpenStack deployment requires a JSON file. Use the following steps to install and edit the file.

1. Login to HLM VM.

```
ssh <HLM_VM_IP>
    HLM_VM_IP is the IP (hlm_clmstaticip) configured in the /root/infra-
ansible-playbooks/group_vars/all file of the HLM host
```

2. On the HLM VM, change to the home directory.

```
cd ~
```

3. Provision and configure your HP Helion OpenStack VM.

```
hnewcloud  <cloudname> <cloud_template>
```

Where:

- `<cloudname>` is the name of the cloud to create
- `<cloud_template>` is the name of the template to use.

The command creates the `<cloudname>` directory, which will contain a JSON template file `node-provision.json`. This template supplies input values to the `hprovision` script, later in the installation.

4. Edit `node-provision.json` file based on following guidelines:

Field	Baremetal
name	Name of the system you want to add
Pxe-mac-address	MAC address of the interface you want to PXE boot onto. This is not same as iLO MAC address,
Pxe-interface	The name of the interface on which PXE boot should occur. For example: `eth0`
pm_type	ipmilan
pm_ip	Power management IP (ilo ip)
pm_user	Power management user (ilo username)
pm_pass	Power management password (ilo password)
node_group	Enter the same value as `node-type` in the `nodes.json` file used during cloud deployment. For example: `CCN-001-001`.
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

To see a sample `node-provision.json` file, see *Create the HLM Virtual Machine*.

Configure PXE boot

After you edit the `node-provision.json` file, you must enable one-time PXE boot on cloud nodes to set the correct boot order. Execute the following on the HLM VM:

1. Use the following command to install the `python-hpilo` module on HLM VM:

   ```
   pip install python-hpilo
   ```

   `python-hpilo` is a python library and command-line tool for iLO.
2. Copy the `ilopxebootonce.py` from the `/root/cg-hlm/dev-tools/ilopxebootonce.py` to the directory where you have the `node-provision.json` file.
3. 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.

Create new cloud template and bring the cloud nodes up

1. Use the following script to start the provisioning of the HLM VM:

   hprovision `<cloudname>`

   Where:

   - `<cloudname>` is the name of the cloud to create

   This script will PXE boot the nodes specified in `node-provision.json` file. The script also tracks the PXE boot completion process and will create the `nodes.json` file in the directory.
2. Update the `node-provision.json` file used in the *previous step*.

a. Change to the <cloudname> directory:

```
cd ~/<cloudname>
```

b. Once the baremetal nodes are provisioned, make sure the nodes.json file is generated and that you can establish a password-less SSH connection to these nodes from HLM VM.

3. Modify the environment.json file to configure the VLANs and network addresses as appropriate for your environment.

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

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

Example:

```
"cidr": "192.168.101.0/24",
"start-address": "192.168.101.100"
```

NOTE: The Helion 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 node.

4. Modify the definition.json file:

   a. Set the number of compute systems to 2.

   ```
   "count": 2, //number of computes in the resource pool
   ```

   b. Update `ansible-vars` section with all the information based on your setup.

   c. Make sure you have two NTP entries at the end of this `definition.json` file as seen in the snapshot. If you have only one NTP server in your environment, specify the same NTP server twice.

5. Use the following steps to modify to the cinder/blocks directory for your cloud:

   - Change to the cinder/blocks directory:

     ```
     cd ~/<cloudname>/services/cinder/blocks
     ```

     Where <cloudname> is the name you assigned to the cloud.

   - Copy the cinder_conf_default.hp3parSample file to the cinder_conf_default file and edit the file to configure to 3PAR settings. For example:

     ```
     --3PAR details (connectivity is still being worked upon ETA 06/22/2015.
     hp3par_api_url=https://<hp3par_ip>:8080/api/v1
     hp3par_username=<hp3par_user>
     hp3par_password=<hp3par_user_password
     hp3par_cpg=bronze
     san_ip=<san_ip>
     san_login=<san_user>
     san_password=<san_password>
     hp3par_iscsi_ips=<iscsi_ip1>,<iscsi_ip2>,<iscsi_ip3>,<iscsi_ip4>
     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
     ```

6. Once you have correctly edited all the json Cloud Model files, run the HP Helion OpenStack Configuration Processor:

   ```
   hcfgproc -d definition.json
   ```

   The `hcfgproc` script gets installed in `/usr/local/bin` by the `prepare-env` script. The script generates a `clouds/` directory within the directory.
7. Review the CloudDiagram, `hosts.hf`, and `net/interfaces.d/eth.cfg` files to make sure the network settings are correct.
8. Initialize network interfaces on all the cloud nodes using the following command:

   ```
   hnetinit <cloudname>
   ```

   You can run this command from any directory.

   After this command completes, all cloud nodes and CLM network interfaces should be set correctly.
9. Use the following command to deploy the cloud:

   ```
   hdeploy <cloudname>
   ```

   Once cloud deployment is successfully complete, there will be 3 controller nodes in the non-KVM region.

Next Step

Deploying the KVM Region

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: Deploying the KVM Region

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

Bring Up Controller-0 in the KVM Region

1. Make sure other nodes to be used in KVM region are shutdown.
2. Use the `HP-HCG-Server-host-installer-15.05-b10.iso` to boot the controller node

   ```
   mount HP-HCG-Server-host-installer-15.05-b10.iso
   ```
3. Follow the install wizard. Select the Graphics mode for the controller only. Do not select `Controller +Compute`.
4. After the reboot, log in as user name `wrsroot` and password `wrsroot`. Make sure you change the password.
5. 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
   ```
6. Set the default gateway to the PXE network gateway

   ```
   route add default gw <CIDR_gateway_IP>
   ```
7. Copy the following files to the `/home/wrsroot/` directory of the controller-0:

   ```
   TS_15.05_PATCH_0001.patch  # HLM VM /root/cg-hlm/windriver-files
   region_config              # HLM VM ~/<cloud_name>/clouds/build40/001/stage/
   windriver-config
   ```

```
cakey.pem                    # HLM VM ~<cloud_name>/clouds/build40/001/stage/
windriver-config
```

```
license.lic                  # License file received/procured ny the user
```

```
helion_branding-v1.2.tgz     # HLM VM /root/cg-hlm/windriver-files
```

8. Move the `helion_branding-v1.2.tgz` to `/opt/branding` on the controller-0
9. Apply the required patches on controller-0:

```
sudo wrs-patch upload /home/wrsroot/TS_15.05_PATCH_0001.patch
sudo wrs-patch apply TS_15.05_PATCH_0001
sudo wrs-patch install-local
sudo reboot
```

10. Install the KVM region coud:

```
sudo config_region
```

Ignore the message which displays during `Config_region` process.

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

11. After `controller-0` is deployed, deploy 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> --mgmt_ip <mgmt_ip> --bm_mac <ilo_mac> --bm_ip <ilo_ip>
 --bm_type ilo4 --bm_username <ilo_user>  --bm_password <ilo_password>
```

12. While registering compute nodes, make sure you specify the `mgmt_ip`. This IP should from the KVM CLM range (refer to the `region_config` file) and must not overlap controller IPs. It is save to start after a block of 10 IPs.
13. Set the controller-1 and compute-0 to `One-time PXE boot from network`.
14. PXE boot all the registered nodes.
15. *Log in to the Horizon interface* and monitor the status of nodes being PXE booted. After succesful PXE boot, Operational State as Disabled and Availability State as Online in the **Admin > Inventory** page.

    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:  admin
```

    Change the password on first login.
16. For each compute node in the inventory, do the following

    a. Create Infra interface. See *HP Helion OpenStack Carrier Grade 1.1: Working with Host Interfaces*
    b. Create a Provider Network. See *HP Helion OpenStack Carrier Grade 1.1: Creating and Deleting Provider Networks*.
    c. Create VLAN Ranges on the provider network using the **Create Segmentation Range** option. See *HP Helion OpenStack Carrier Grade 1.1: Creating a Segmentation Range*.
    d. Create data interface. Due to latest networking changes, ensure you create data interface either of the following AE mode is tied to each interface:

```
eth2 and eth3 - Active/Standby
```

```
eth4 and eth5 - Balanced XOR / Layer 2
```

17. *Unlock the compute nodes*. Compute nodes will reboot. Keep polling the status on the inventory page to show **Available** and **Online**.
18. Access the Horizon dashboard using the CAN network IP (HTTPS). By default, Horizon is restricted to access the CAN network using the CLM network as the default gateway You can workaround this, use SSH to access each controller node and update the filters:

```
echo 0 > /proc/sys/net/ipv4/conf/default/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth0.<CAN_VLAN_ID>/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth0.<CLM_VLAN_ID>/rp_filter
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Next Step

Post-Installation Tasks

Return to Top

HP Helion OpenStack® Carrier Grade 1.1: HLM Post-Installation Tasks

After the HLM VM has been created, perform the following tasks before proceeding.

Enable logging for the hdeloy - ansible-playbook

Copy the `ansible.cfg` to the `~/<cloud-name>/clouds/<cloud-name>/001/stage/ansible/` directory before executing `hdeploy`.

Configure the LDP-CCN and LDP-CPN roles

To make sure that the LDP-CCN and LDP-CPN roles are created when LDAP integration is enabled.

Remove the double quotes in the `definition.json` file for the `ldap_enabled` variable.

```
"ldap_enabled": 1
```

If you have LDAP enabled in `definition.json`, you need to comment and add this command in the `ldap.yml` file.

1. On the HLM VM, edit the `clouds/dcnjunobuild33bed2new/001/stage/ansible/roles/LDP-CCN/tasks/ldap.yml` file.
2. Comment out the following line in the file:

```
# command: apt-get install python-ldap
```

3. Add the following line:

```
apt: name=python-ldap install_recommends=no state=latest force=yes
```

4. Save and close the file.

Return to Top