Hewlett Packard
Enterprise

Helion OpenStack Carrier Grade 4.0

SYSTEM ADMINISTRATION

4.0

Helion OpenStack Carrier Grade 4.0

System Administration

Contents

1

System Administration Introduction

Introduction to System Administration

System administration for the Helion OpenStack Carrier Grade 4.0 (HCG 4.0) involves system-level configuration and management of the physical nodes within the cloud.

System administration includes the following functions:

- configuration of the physical nodes
- node connection management
- network configuration
- fault and resource usage monitoring of the physical nodes
- backup and restore of the physical nodes

2

System Configuration Management

System Configuration Management Overview

Much of the system configuration data is specified as bootstrap-type configuration data defined during software installation, using the **config_controller** script. After installation, you can change this system configuration data, as well as additional system configuration data, using the web administration interface or the CLI.

There are a few exceptions to bootstrap system configuration data, specified at install time, that can NOT be changed afterwards; one should ensure these configurations are correct otherwise a system re-install is required. This configuration data includes: product type (Standard vs CPE), presence of a pxeboot network, management network subnet and subnet range, infrastructure network subnet and subnet range, and use of secure external connections.

System Configuration Management Using the CLI

You can use the CLI to make changes to the system configuration after installation.

For information about the types of configuration changes you can make, and guidelines for implementing them on an operational system, see System Configuration Management Overview

on page 3. During some configuration changes, system alarms are raised; for help viewing them from the CLI, see Viewing Active Alarms Using the Web Interface on page 216.

To make configuration changes using the CLI, you must log in as user **wrsroot** to the active controller and source the script **/etc/nova/openrc** to obtain Keystone administrative privileges. For details, see Linux User Accounts on page 169.

With the exception of the DNS Server Configuration, the configuration changes described in this section require that you lock and unlock the indicated hosts after the configuration change is made. For more information about locking and unlocking hosts, see Host Inventory on page 52.

Changing the DNS Server Configuration

You can change the DNS servers defined for HCG 4.0 at any time after installation.

During software installation, HCG 4.0 is configured with up to two DNS server IP addresses. You change these addresses using the Web administration interface or the CLI.

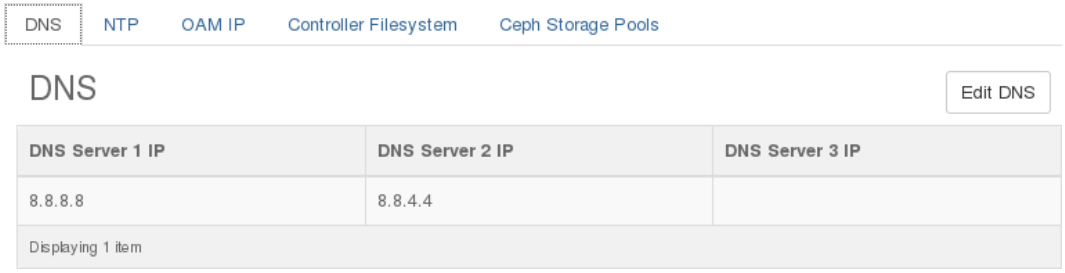
Procedure

1. In the HCG 4.0 Web administration interface, open the System Configuration page.

   The System Configuration page is available from **Admin** > **Platform** > **System Configuration** in the left-hand pane.

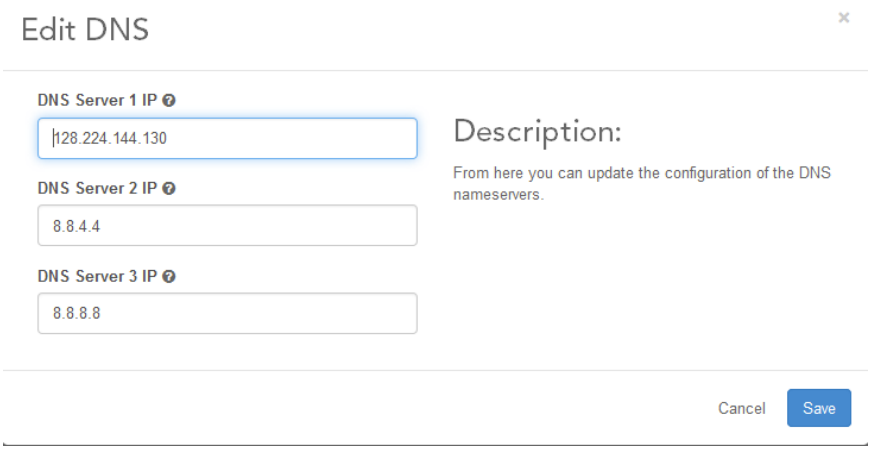
2. Select the DNS tab.

   The DNS page appears, showing the currently defined DNS servers and their IP addresses.



3. Click **Edit DNS**.

   The Edit DNS dialog box appears.



4. Replace the DNS Server IP addresses with different ones as required.

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.

Configuring the DNS Server Using the CLI

You can use the CLI to view and change the DNS server configuration.

To view the existing DNS server configuration, use the following command.

```
~(keystone_admin)$ system dns-show
    +--------------+--------------------------------------------+
| Property     | Value                                      |
+--------------+--------------------------------------------+
| uuid         | 7d4ae6d4-f43f-4735-8ee5-ce261f4f8aa7       |
| nameservers  | 128.224.144.130,147.11.57.128,147.11.57.133 |
| isystem_uuid | 106c2b53-175d-4271-af54-d43b02bb03fb       |
| created_at   | 2016-10-24T19:26:56.703008+00:00           |
| updated_at   | 2016-10-27T14:26:51.166448+00:00           |
+--------------+--------------------------------------------+
```

To change the DNS server IP addresses, use the following command syntax. The **nameservers** option takes a comma-delimited list of DNS server IP addresses.

```
~(keystone_admin)$ system dns-modify \
nameservers=IP_address_1[,IP_address_2][,IP_address_3] action=apply
```

For example:

```
~(keystone_admin)$ system dns-modify \
nameservers=8.8.8.8,8.8.4.4 action=apply
```

Changing the NTP Server Configuration

You can change the NTP server addresses defined for HCG 4.0 at any time after installation.

During software installation, HCG 4.0 is configured with up to three NTP server IP addresses. You change these addresses using the Web administration interface or the CLI.

Prerequisites

Before changing NTP server addresses, review the Fault Management page and ensure that any existing system alarms are cleared.

⚠ **CAUTION:** For the HCG 4.0 to use FQDN servers instead of IPv4 servers, at least one valid DNS server must be specified.

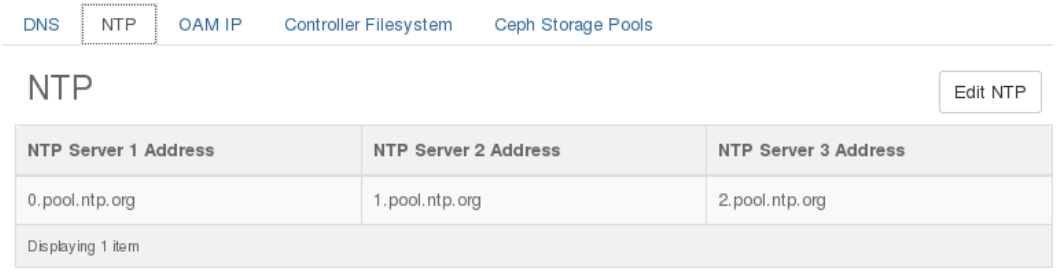
Procedure

1. In the HCG 4.0 Web administration interface, open the System Configuration page.

   The System Configuration page is available from **Admin** > **Platform** > **System Configuration** in the left-hand pane.

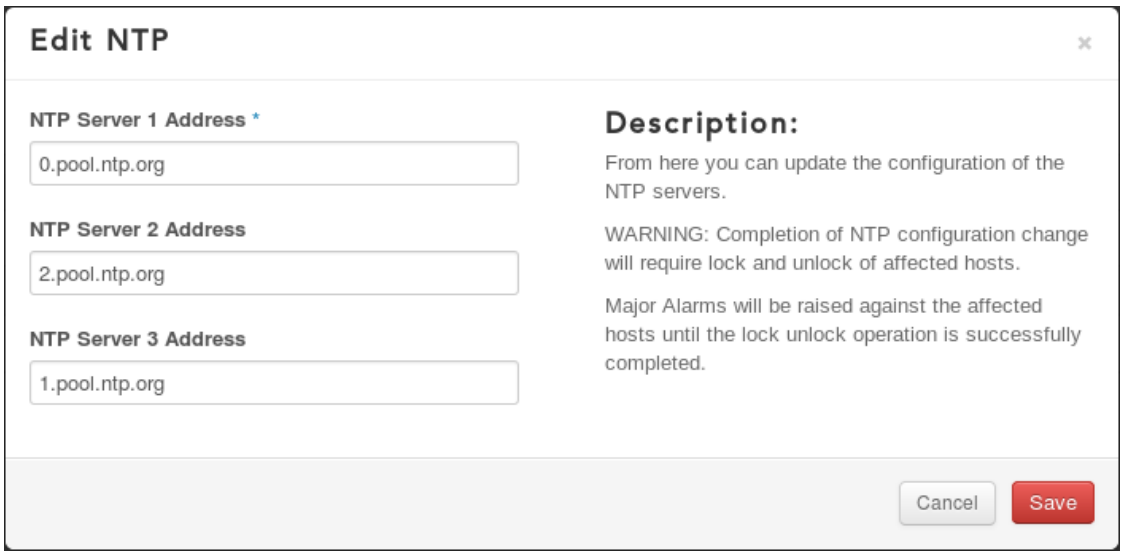
2. Select the NTP tab.

   The NTP page appears, showing the currently defined NTP servers and their IP addresses.



3. Click **Edit NTP**.

   The Edit NTP dialog box appears.



4. Replace the NTP Server IP addresses or names 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.

5. Click **Save**.

   This raises major alarms against the controllers and services. You can view the alarms on the Fault Management page.

6. Lock and unlock the controllers to clear the alarms.

   Open the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane, and then selec the **Hosts** tab. Hosts requiring attention are shown with the status **Config out-of-date**.

   To lock or unlock a host, click **Edit Host** for the host and then use the menu selections.

   a) Lock the standby controller.

      Wait for the lock operation to be completed.

   b) Unlock the standby controller.

      Wait for the host to become available. Its configuration is updated, and its error message is cleared.

   c) Perform a swact on the active controller.

      Click **Edit Host** > **Swact Host** > for the active controller.

      Web administration access is interrupted, and the HCG 4.0 login screen appears. Wait briefly for the Web service to stabilize, and then log in again.

   d) 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. Its configuration is updated, and its error message is cleared.

7. Ensure that the **250.001 Configuration out-of-date** alarms are cleared for both controllers.

Configuring the NTP Server Using the CLI

You can use the CLI to view or change the NTP Server Configuration.

To view the existing NTP server configuration, use the following command.

```
~(keystone_admin)$ system ntp-show
+--------------+--------------------------------------+
| Property     | Value                                |
+--------------+--------------------------------------+
| uuid         | 7d4ae6d4-f43f-4735-8ee5-ce261f4f8aa7 |
| ntpservers   | None                                 |
| isystem_uuid | 106c2b53-175d-4271-af54-d43b02bb03fb |
| created_at   | 2016-10-24T19:26:56.731230+00:00     |
| updated_at   | None                                 |
+--------------+--------------------------------------+
```

To change the NTP server IP addresses, use the following command syntax. The **ntpservers** option takes a comma-delimited list of NTP server names.

```
~(keystone_admin)$ system ntp-modify \
ntpservers=server_1[,server_2][,server_3] action=apply
```

For example:

```
~(keystone_admin)$ system ntp-modify \
ntpservers=0.north-america.pool.ntp.org,\
0.north-america.pool.ntp.org,0.north-america.pool.ntp.org \
action=apply
```

After changing the NTP server configuration, you must lock and unlock both controllers. This process requires a swact on the controllers.

Resynchronizing a Host to the NTP Server

If host synchronization is lost for any reason, you must lock and then unlock the host to restore the synchronization safely.

If a large time discrepancy (greater than 1000 seconds, or about 17 minutes) develops between the clock time on a host and the time as reported by an NTP server, the **ntpd** service on the host stops, and Alarm 200.006 (<hostname> 'ntpd' process has failed) is logged in the Alarm Log and the Customer Log. This can occur if the clock on the host is inadvertently set incorrectly, or cannot access the NTP server for the correct time at initialization and defaults to an incorrect time.

To recover, lock and then unlock the host. The time is automatically synchronized to the NTP server when the host is unlocked.

CAUTION: Do not attempt to recover by restarting the **ntpd** service. This can cause problems for other running services.

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.

During software installation, HCG 4.0 is configured with an OAM network subnet and related IP addresses. You can change these addresses using the Web administration interface or the CLI. You can use IPv4 or IPv6 addresses.

⚠ **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 compute-node hosts is interrupted until the hosts are locked and unlocked.

Prerequisites

Before changing the OAM IP configuration, review the Fault Management page and ensure that any existing system alarms are cleared.

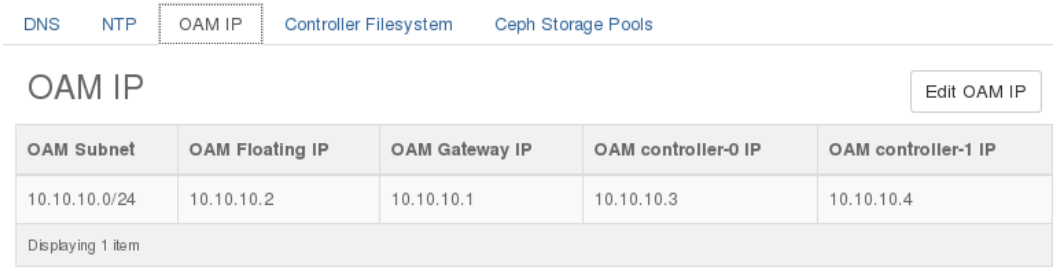
Procedure

1. In the HCG 4.0 Web administration interface, open the System Configuration page.

   The System Configuration page is available from **Admin** > **Platform** > **System Configuration** in the left-hand pane.

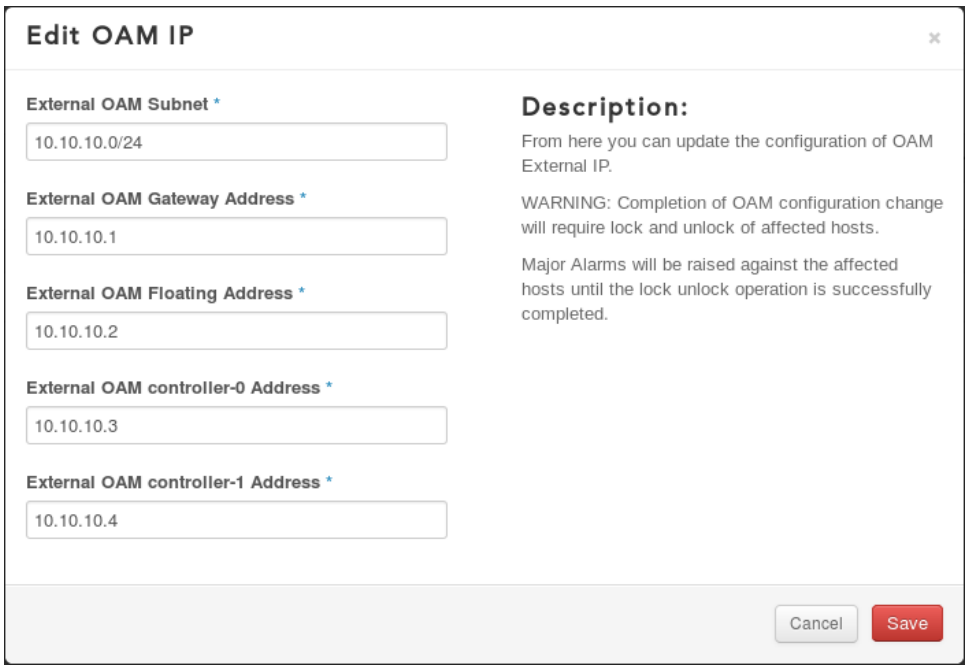
2. Select the OAM IP tab.

   The OAM IP page appears, showing the currently defined OAM network configuration.



3. Click **Edit OAM IP**.

   The Edit OAM IP dialog box appears.



4. Replace the IP addresses with different ones as required.

NOTE: If you change the IP address version (IPv4 or IPv6), ensure that the same version is used for the DNS servers (see Changing the DNS Server Configuration on page 4) and NTP servers (see Changing the NTP Server Configuration on page 6).

5. Click **Save**.

   This raises major alarms against the controllers and services. You can view the alarms on the Fault Management page.

6. Lock and unlock the controllers to clear the alarms.

   Open the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane, and then selec the **Hosts** tab. Hosts requiring attention are shown with the status **Config out-of-date**.

   To lock or unlock a host, click **Edit Host** for the host and then use the menu selections.

   a) Lock the standby controller.

      Wait for the lock operation to be completed.

   b) Unlock the standby controller.

      Wait for the host to become available. Its configuration is updated, and its error message is cleared.

   c) Perform a swact on the active controller.

      Click **Edit Host** > **Swact Host** > for the active controller.

      Web administration access is interrupted, and the HCG 4.0 login screen appears. Wait briefly for the Web service to stabilize, and then log in again.

   d) 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. Its configuration is updated, and its error message is cleared.

7. Lock and unlock each compute node.

CAUTION: Before locking a compute node, ensure that sufficient resources are available on other hosts to migrate any running instances.

8. Ensure that the **250.001 Configuration out-of-date** alarms are cleared for all hosts.

If any alarms are present, clear them by locking and unlocking the affected host. In most cases, the alarms are cleared within one minute. If other system configuration operations are pending for the host, allow more time for the alarms to be cleared.

Default Firewall Rules

HCG 4.0 applies these default firewall rules on the OAM network. The default rules are recommended for most applications.

Traffic is permitted for the following protocols and ports to allow access for platform or OpenStack services. By default, all other traffic is blocked.

NOTE: Depending on the system configuration, additional rules may apply.

- On systems configured for Swift object storage, port 7480 is added for access to the **ceph-radosgw-api** service.
- Custom rules may be added for other requirements. For more information, see Firewall Options on page 192.

Protocol	Port	Service Name
tcp	22	ssh
tcp	80	horizon (http only)
tcp	199	smux
tcp	443	horizon (https only)
tcp	4545	nfv-vim-api
tcp	5000	keystone-api
tcp	6080	nova-nonvc-proxy
tcp	6835	sysinv-api
tcp	8000	heat-cfn

Protocol	Port	Service Name
tcp	8003	heat-cloudwatch-api
tcp	8004	heat-api
tcp	8777	ceilometer-api
tcp	8776	cinder-api
tcp	8773	nova-ec2
tcp	8774	nova-api
tcp	9292	glance-api
tcp	9696	neutron-api
tcp	15491	patching-api
icmp		icmp
udp	123	ntp
udp	161	snmp
udp	2222	service manager
udp	2223	service manager

NOTE: UDP ports 2222 and 2223 are used by the service manager for state synchronization and heart beating between the controllers. All messages are authenticated with a SHA512 HMAC. Only packets originating from the peer controller are permitted; all other packets are dropped.

Firewall Rules File Format

HCG 4.0 supports custom OAM firewall rules compatible with the Linux **Netfilter** framework.

The custom rules are applied using **iptables-restore** or **ip6tables-restore**. They must be in a format supported by **iptables-save** or **ip6tables-save**.

NOTE: The file format must use Linux line endings. DOS line endings are not supported.

The following example illustrates how to add rules before and after the default rules.

```
*filter
-A INPUT-custom-pre -p tcp -m tcp --dport 9000 -m comment \
--comment "example pre entry" -j ACCEPT
-A INPUT-custom-post -p tcp -m tcp --dport 9001 -m comment \
```

```
--comment "example post entry" -j ACCEPT
COMMIT
```

For more information about the HCG 4.0 firewall, see Firewall Options on page 192. For general information about **Netfilter**, refer to the Internet or other public sources.

Changing the MTU of the OAM Interface

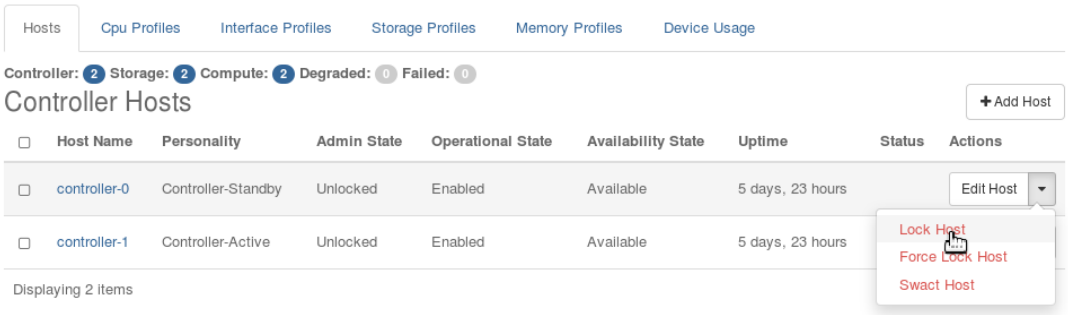
You can change the MTU value of the OAM interface from the Web administration interface.

If you prefer, you can use the CLI; see Changing the MTU of the OAM Interface Using the CLI on page 14.

Controller configuration changes require each controller to be locked. This requires a swact during the procedure.

Procedure

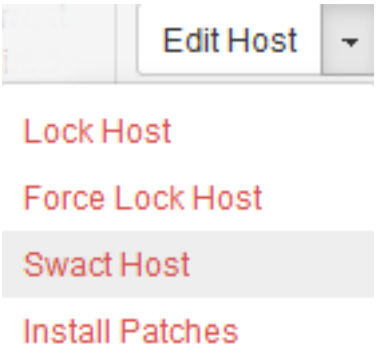
1. Lock the standby controller.
   a) From **Admin** > **Platform** > **Host Inventory**, select the **Hosts** tab.
   b) From the **Edit** menu for the standby controller, select **Lock Host**.



2. Edit the OAM interface to change the MTU value.
   a) Click the name of the standby controller, then select the **Interfaces** tab and click **Edit** for the OAM interface.
   b) In the Edit Interface dialog, edit the **MTU** field, and then click **Save**.
3. Unlock the standby controller.

   From the **Edit** menu for the standby controller, select **Unlock Host**.
4. Swact the hosts.

   From the **Edit** menu for the active controller, select **Swact Host**.



5. Lock the new standby controller.
6. Modify the MTU of the OAM interface on the new standby controller.
7. Unlock the standby controller.

Changing the MTU of the OAM Interface Using the CLI

You can change the MTU value of the OAM interface using the CLI.

If you prefer, you can use the Web administration interface; see Changing the MTU of the OAM Interface on page 13.

Controller configuration changes require each controller to be locked. This requires a swact.

Procedure

1. Lock the standby controller.

```
~(keystone_admin)$ system host-lock controller-1
```

2. Use the **system host-if-modify** command to specify the interface and the new MTU value on the standby controller.

   This example assumes the OAM interface uses **eth6**.

```
~(keystone_admin)$ system host-if-modify controller-1 eth6 --imtu 1600
```

3. Unlock the standby controller.

```
~(keystone_admin)$ system host-unlock controller-1
```

4. Swact the controllers.

```
~(keystone_admin)$ system host-swact controller-1
```

5. Lock the new standby controller.

```
~(keystone_admin)$ system host-lock controller-0
```

6. Modify the MTU of the corresponding interface on the standby controller.

```
~(keystone_admin)$ system host-if-modify controller-0 eth6 --imtu 1600
```

7. Unlock the standby controller.

```
~(keystone_admin)$ system host-unlock controller-0
```

Changing the MTU for a Data Interface

You can change the MTU value for a data interface from the Web administration interface or the CLI.

Prerequisites

All hosts attached to the provider network must be locked before you make changes to any of them.

Procedure

1. Lock all hosts attached to the provider network.
   a) From **Admin** > **Platform** > **Host Inventory**, select the **Hosts** tab.
   b) From the **Edit** menu for the standby controller, select **Lock Host**.
2. On all the hosts, edit the interface to change the MTU value.
   a) Click the name of the host, and then select the **Interfaces** tab and click **Edit** for the interface you want to change.
   b) In the Edit Interface dialog, edit the **MTU** field, and then click **Save**.
3. Unlock all the hosts.

   From the **Edit** menu for the host, select **Unlock Host**.

   The network MTU is updated with the new value.

Changing the MTU for a Data Interface Using the CLI

You can change the MTU value for a data interface from the Web administration interface or the CLI.

The MTU must be changed while all the compute hosts attached to the provider network are locked.

You can use CLI commands to lock and unlock hosts, and to modify the MTU on the hosts.

```
~(keystone_admin)$ system host-lock nodeName
~(keystone_admin)$ system host-if-modify nodeName ifname --imtu mtu_size
~(keystone_admin)$ system host-unlock nodeName
```

Where:

nodename

is the name of the host

ifname

is the name of the interface

mtu_size

is the new MTU value

For example:

```
~(keystone_admin)$ system host-if-modify compute-0 enp0s8 --imtu 1496
```

NOTE: You cannot set the MTU on a compute node interface to a value smaller than the largest MTU used on its provider networks.

Adding an Infrastructure Network

If an infrastructure network is not installed during initial configuration, you can add one later using the CLI.

Prerequisites

On a cluster with an infrastructure network, each host must have an infrastructure interface before it can be unlocked. Ensure that all hosts have the required hardware.

For a system with LVM-backed controller storage, the infrastructure network is optional. It can be used to offload the internal management network on clusters with many compute nodes.

You can add an infrastructure network after initial installation. For this operation, all nodes except the active controller must be locked. During the change, the nodes cannot be unlocked until the new configuration is applied to both controllers. In addition, before a node can be unlocked, an infrastructure interface must be configured on the host.

Procedure

1. Lock all hosts except the active controller.

   For each host, use the following command.

   ```
   ~(keystone_admin)$ system host-lock hostname
   ```

2. Specify the infrastructure subnet.

   ```
   ~(keystone_admin)$ system infra-add \
   [--start ip-address] [--end ip-address] [--mtu mtu] [--vlan_id vlan-id
   network subnet
   ```

   Where:

   Positional arguments:

   - *network subnet* - Network subnet

Optional arguments:

- --start *ip-address* - The start IP address in subnet
- --end *ip-address* - The end IP address in subnet
- --mtu *mtu* - The MTU for the network
- --vlan_id *ip-address* - The VLAN id for the subnet

For example:

```
~(keystone_admin)$ system infra-add 192.168.205.0/24

Active controller must be rebooted to apply manifests.
+---------------+--------------------------------------+
| Property      | Value                                |
+---------------+--------------------------------------+
| uuid          | 08a9f118-bf13-4e14-8c4b-c83a1072a894 |
| infra_subnet  | 192.168.205.0/24                     |
| infra_start   | 192.168.205.2                        |
| infra_end     | 192.168.205.254                      |
| infra_mtu     | 1500                                 |
| infra_vlan_id | None                                 |
| isystem_uuid  | 21d811ea-b32d-490d-81b2-d547722199a1 |
| created_at    | 2016-10-26T15:38:06.442031+00:00     |
| updated_at    | None                                 |
+---------------+--------------------------------------+
```

3. Add an infrastructure interface on the standby controller.

NOTE: You can also add an infrastructure network to a shared interface as a VLAN-tagged network. For more information, see *HCG 4.0 Planning: Shared (VLAN) Ethernet Interfaces*.

To add an infrastructure network to a dedicated interface, use the following command, specifying a name for the network and the port to use for the network connection. To identify the port to use for an infrastructure network, consult your configuration plan.

```
~(keystone_admin)$ system host-if-modify -nt infra \
-n interfacename hostname port
```

For example:

```
~(keystone_admin)$ system host-if-modify -nt infra \
-n infra0 controller-1 enp0s8
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| ifname           | infra0                               |
| networktype      | infra                                |
| iftype           | ethernet                             |
| ports            | [u'enp0s8']                          |
| providernetworks | None                                 |
| imac             | 08:00:27:7a:fa:a5                    |
| imtu             | 1500                                 |
| aemode           | active_standby                       |
| schedpolicy      | None                                 |
| txhashpolicy     | layer2                               |
| uuid             | d3efde57-c475-402e-acad-34f5029f3988 |
| ihost_uuid       | 62657285-cc9c-45a2-962e-ecb01647916f |
| vlan_id          | None                                 |
| uses             | []                                   |
| used_by          | []                                   |
| created_at       | 2014-12-31T20:13:16.326992+00:00     |
| updated_at       | None                                 |
+------------------+--------------------------------------+
```

4. Add an infrastructure interface on the active controller.

   For example:

```
~(keystone_admin)$ system host-if-modify -nt infra \
-n infra0 controller-0 enp0s8
+------------------+-------------------------------------+
| Property         | Value                               |
+------------------+-------------------------------------  -+
| ifname           | infra0                              |
| networktype      | infra                               |
| iftype           | ethernet                            |
| ports            | [u'enp0s8']                         |
| providernetworks | None                                |
| imac             | 08:00:27:51:58:6b                   |
| imtu             | 1500                                |
| aemode           | active_standby                      |
| schedpolicy      | None                                |
| txhashpolicy     | layer2                              |
| uuid             | 66c4543e-6bfd-4ede-9b8a-4d091cf290a9 |
| ihost_uuid       | 3c11607b-1550-4e99-a46f-2580c18683da |
| vlan_id          | None                                |
| uses             | []                                  |
| used_by          | []                                  |
| created_at       | 2014-12-31T20:29:51.759507+00:00    |
| updated_at       | None                                |
+------------------+-------------------------------------+
```

5. Reboot the standby controller.

```
~(keystone_admin)$ system host-reboot controller
```

   where *controller* is the current standby controller (**controller-1** or **controller-0**)

   This updates its configuration.

   Wait for the standby controller to reboot. To monitor its status, use the following command.

```
~(keystone_admin)$ watch -n 5 system host-list
```

   This displays a refreshed host list every five seconds. Monitor the output until the standby controller is shown as locked and online. To stop monitoring, enter **CTRL-C**.

⚠ **CAUTION:** To prevent potential service conflicts due to inconsistent controller network configurations, do not unlock the standby controller until the active controller is also rebooted.

6. Reboot the active controller.

   For example:

```
~(keystone_admin)$ sudo reboot
The system is going down for reboot NOW!
```

   Wait for the controller to reboot.

7. Log in to the active controller and become the Keystone **admin** user.

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

8. Unlock the standby controller.

```
~(keystone_admin)$ system host-unlock controller-1
+-----------------+-------------------------------------+
```

```
| Property         | Value                                |
+------------------+--------------------------------------+
| action           | none                                 |
| administrative   | locked                               |
| availability     | online                               |
| bm_ip            |                                      |
| bm_mac           |                                      |
| bm_type          | None                                 |
| bm_username      |                                      |
| capabilities     | {}                                   |
| created_at       | 2014-12-24T16:44:08.749540+00:00     |
| cstatus          |                                      |
| hostname         | controller-1                         |
| iconfig_applied  | 76aa6a81-620a-4ba2-85c3-113d1c42f5ec |
| iconfig_fini     | 76aa6a81-620a-4ba2-85c3-113d1c42f5ec |
| iconfig_target   | 76aa6a81-620a-4ba2-85c3-113d1c42f5ec |
| id               | 5                                    |
| invprovision     | unprovisioned                        |
| location         | {u'locn': u'Rack 1 Pos 2'}           |
| mgmt_ip          | 192.168.204.4                        |
| mgmt_mac         | 08:00:27:ba:e8:52                    |
| operational      | disabled                             |
| personality      | controller                           |
| reserved         | False                                |
| serialid         | None                                 |
| task             | Unlocking                            |
| updated_at       | 2015-01-02T17:12:56.464592+00:00     |
| uptime           | 1955                                 |
| uuid             | 62657285-cc9c-45a2-962e-ecb01647916f |
+------------------+--------------------------------------+
```

9. Add infrastructure interfaces to each compute node.

For each node, use the following command.

```
~(keystone_admin)$ system host-if-modify -nt infra \
-n networkname hostname port
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| ifname           | infra0                               |
| networktype      | infra                                |
| iftype           | ethernet                             |
| ports            | [u'enp0s10']                         |
| providernetworks | None                                 |
| imac             | 08:00:27:20:d2:d1                    |
| imtu             | 1500                                 |
| aemode           | active_standby                       |
| schedpolicy      | None                                 |
| txhashpolicy     | layer2                               |
| uuid             | d664ad66-58fa-4378-b906-ae417d58dbf0 |
| ihost_uuid       | 43b462ac-05fc-43dd-82de-160c7ab0923f |
| vlan_id          | None                                 |
| uses             | []                                   |
| used_by          | []                                   |
| created_at       | 2015-01-02T17:33:37.138694+00:00     |
| updated_at       | None                                 |
+------------------+--------------------------------------+
```

You can now unlock the compute nodes. This clears any **Configuration out-of-date** errors.

3

Provider Network Management

Provider Networks

Provider networks are used to attach data interfaces.

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.

Displaying Provider Network Information

You can view provider network details from the Web administration interface or the CLI. You can also view provider network topologies from the Web administration interface.

Using the Web administration interface, you can obtain information about provider networks in two places:

- The **Provider Network Topology** view. This is a graphical representation of all provider networks on the system and their connections to compute hosts. You can select individual provider networks to view details. You can also review active alarms for provider network connections. For more information, see The Provider Network Topology View on page 23.

NOTE: You cannot make changes from this view.

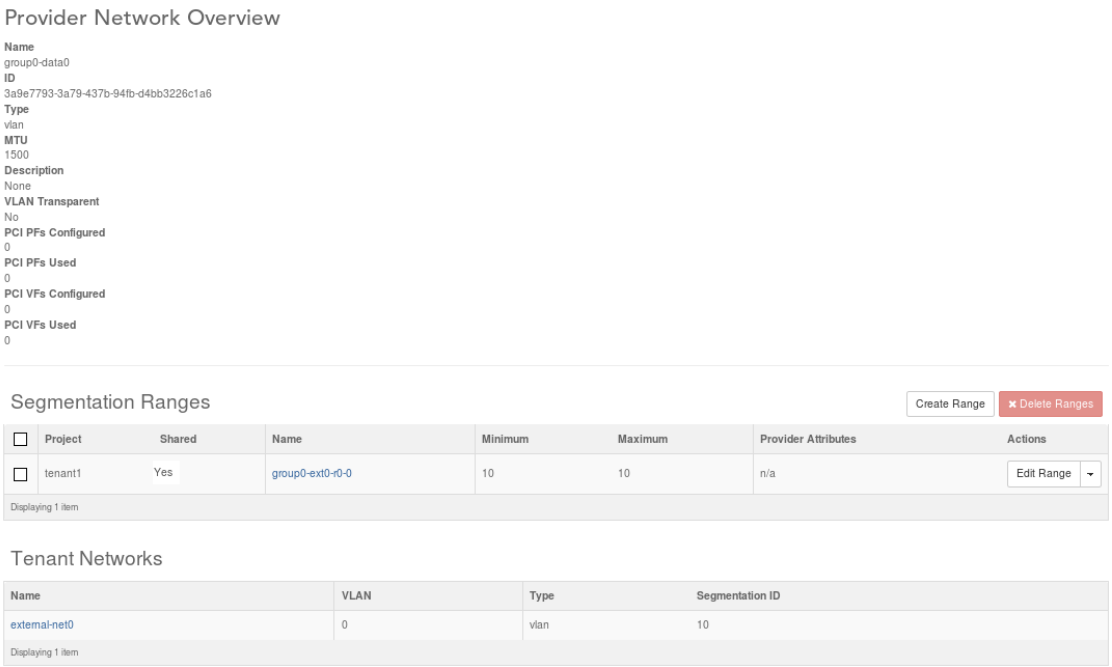
- The Provider Networks page. This is a list of all provider networks on the system and their settings and segmentation ranges. You can select an individual provider network to view details, and you can create and edit provider networks and segmentation ranges.

Both places use the **Provider Network Details** tab to present details. If you prefer, you can view the details using the CLI; for more information, see Displaying Provider Network Information Using the CLI on page 22.

Procedure

1. From the left pane menu, select **Admin** > **Platform** > **Provider Networks**.
2. Click the name of the provider network to open the Provider Network Overview page.

   Details for the provider network are displayed, including any associated segmentation ranges and tenant networks.



Displaying Provider Network Information Using the CLI

You can display information about provider networks from the CLI.

To view information for a provider network from the CLI, use the following command:

```
~(keystone_admin)$ neutron providernet-show providernet
```

where *providernet* is the name or UUID of the provider network.

For example:

```
~(keystone_admin)$ neutron providernet-show group0-data0
```

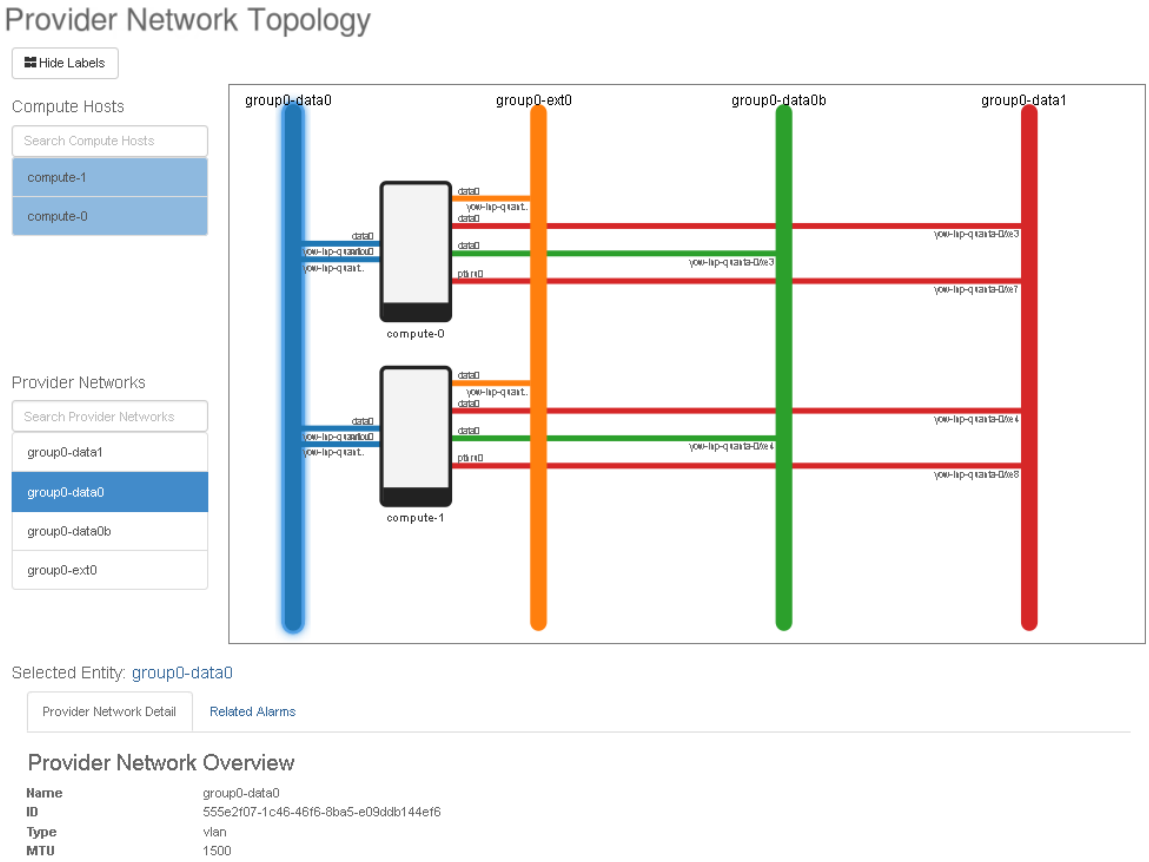
You can use the following command to retrieve the names of the provider networks:

```
~(keystone_admin)$ neutron providernet-list
```

The Provider Network Topology View

The Provider Network Topology view shows provider networks and compute host data interface connections for the system using a color-coded graphical display. Active alarm information is also shown in real time. You can select individual hosts or networks to highlight their connections and obtain more details.

To display this view, select **Admin** > **Platform** > **Provider Network Topology**.



Selection and Navigation

The Provider Network Topology view shows all compute hosts and provider networks graphically in a framed topology window, and lists them by name in the **Compute Hosts** and **Provider Networks** lists to the left of the window. You can select an entity using the window or the lists. The selected entity is highlighted in both places.

If the topology of the system is too large to fit in the window, you can drag inside the window to see other areas. You can also bring an entity into view by selecting it from the lists. The view is panned automatically to show the entity.

Additional Details for Entities

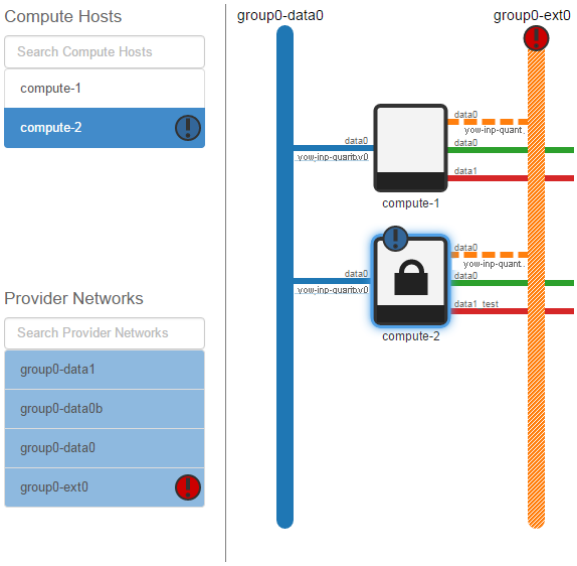
When you select an entity, associated entities are highlighted in the **Compute Hosts** list or the **Provider Networks** list. For example, if you select the **group0-data0** provider network, all hosts attached to it are highlighted in the **Compute Hosts** list.

Additional information for the selected entity is available in tabbed pages below the topology window.

- For a compute host, the additional information includes the **Overview**, **Interfaces**, and **LLDP** tabs from the Host Inventory Detail, as well as a **Related Alarms** tab that lists any active alarms associated with the host.
- For a provider network, the additional information includes the **Provider Network Detail** tab from the Provider Network Overview, and a **Related Alarms** tab that lists any active alarms associated with the provider network.

Alarm Reporting

Active alarms for entities are displayed in real time in the topology window, using icons superimposed on the entities. The alarms are color-coded for severity using the same colors as the Global Alarm Banner. Details for the alarms are listed in the **Related Alarms** tab for the entity.



Labels for Network Connections

Network connections in the topology window may be labeled with the data interface name (displayed above the connection line) and LLDP neighbor information (displayed below the connection line). You can show or hide the labels using a button above the lists (**Show Labels** or **Hide Labels**).

Configuring Provider Networks

You can use the HCG 4.0 CLI or Web administration interface to set up provider networks over physical networks.

A *provider network* is a layer-2 virtual network associated with a physical network. Provider networks are used to provide connectivity for tenant networks.

You can choose from three types of provider network:

- A flat network mapped directly to the physical network.
- A VLAN network, which can support multiple tenant networks using designated ranges of VLAN IDs for communication between hosts on the same Layer 2 network.
- A VXLAN network, which can support multiple tenant networks using designated ranges of VNIs for communication between hosts on different Layer 2 segments separated by one or more L3 routers.

For more about provider networks and tenant networks, see the *HCG 4.0 Planning: Network Requirements*.

To create an association with a physical network, the provider network must be mapped to an Ethernet interface on a compute node. At least one such interface must be set up before the compute node can be unlocked. For more information, see Network Interface Provisioning on page 75.

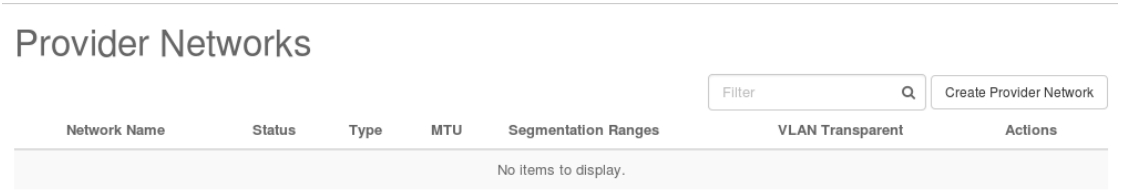
Procedure

1. Open the HCG 4.0 Web administration interface.

   Using a browser, navigate to the OAM floating IP address, and log in as **admin**.

2. In the left-hand pane, select **Admin** > **Platform** > **Provider Networks**.

   The Provider Networks list is displayed.



3. Create a provider network.

   Click **Create Provider Network**.

   In the Create Provider Network window, complete the fields as required.

   Name

   The name of the provider network.

Description

A free-text field for reference.

Type

The type of provider network to be created.

flat

mapped directly to the physical network

vlan

supports multiple tenant networks using VLAN IDs.

vxlan

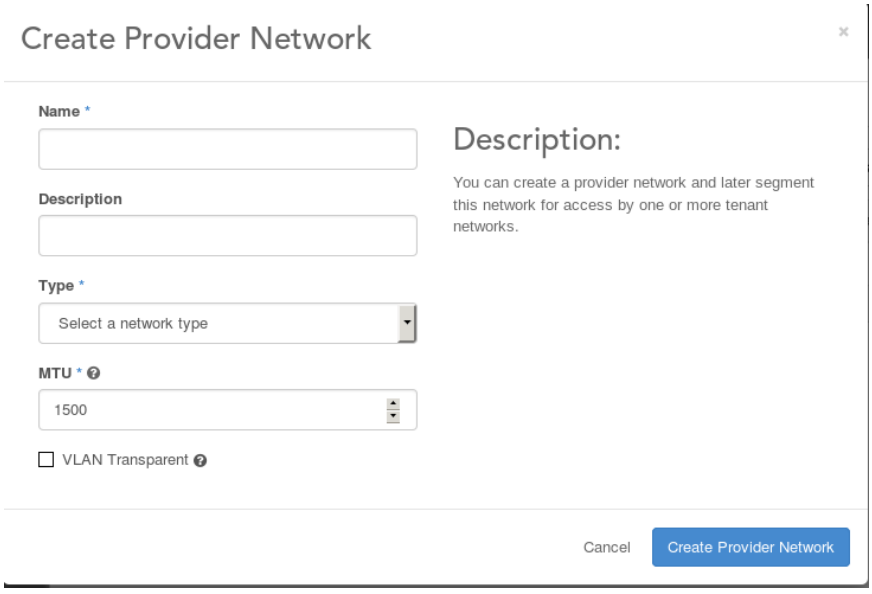
supports multiple tenant networks using VXLAN VNIs.

MTU

The maximum transmission unit for the Ethernet segment used to access the network.

VLAN Transparent

Allow VLAN tagged packets to be encapsulated within a VXLAN segment without removing or modifying the guest VLAN tag.



4. Commit the changes.

   Click **Create Provider Network**.

   The new provider network is added to the Provider Networks list.

Postrequisites

After creating a provider network of the VLAN or VXLAN type, you can assign one or more *segmentation ranges* consisting of a set of consecutive VLAN IDs (for VLANs) or VNIs (for VXLANs). Segmentation ranges are required in order to set up tenant networks.

Segmentation ranges are not required in order to attach interfaces and unlock compute nodes.

For general information about segmentation ranges, see the Provider Networks on page 21.

Configuring Provider Networks Using the CLI

You can set up provider networks over physical networks using the **controller-0** command-line interface. The provider networks provide connectivity for tenant networks.

You must configure at least one provider network in order to assign data interfaces to compute nodes and unlock the hosts.

Prerequisites

Controller-0 must be installed and configured.

To create a provider network using the CLI, use the following command:

```
~(keystone_admin)$ neutron providernet-create name \
--type=type --description=description mtu mtu_size \
--vlan-transparent={True,False}
```

where

name

is a name for the provider network

type

is the type of provider network (**flat**, **vlan**, or **vxlan**)

description

is a brief description for reference purposes

mtu_size

is the maximum transmission unit size

For example, to add a VLAN provider network named providernet-a:

```
~(keystone_admin)$ neutron providernet-create providernet-a --type=vlan
Created a new providernet:
+------------------+--------------------------------------+
| Field            | Value                                |
+------------------+--------------------------------------+
| description      |                                      |
| id               | a5938194-a296-4d92-af5f-c3a064b56f7f |
| mtu              | 1500                                 |
| name             | providernet-a                        |
| ranges           |                                      |
| status           | DOWN                                 |
| type             | vlan                                 |
| vlan_transparent | False                                |
+------------------+--------------------------------------+
```

You can obtain information about provider networks and segmentation ranges using the following commands.

```
~(keystone_admin)$ neutron net-list-on-providernet providernet
```

```
~(keystone_admin)$ neutron providernet-range-show providernet-range
```

Creating Segmentation Ranges

The **admin** user must create segmentation ranges on existing provider networks of the **vlan** type in order to support tenant networks.

Prerequisites

This task assumes that provider networks have already been created to unlock the compute nodes and make the system operational. For more information, see Configuring Provider Networks on page 25.

Segmentation ranges are sets of contiguous identifiers defined on a provider network. Each ID is used to implement a tenant network.

Depending on how a segmentation range is configured, its ID can be available to all tenants (shared), or designated for use by a particular tenant. When a tenant or admin creates a new tenant network, it is assigned an ID automatically from the available ranges on available provider networks.

For a provider network of type VLAN, the identifiers are called VLAN IDs.

Procedure

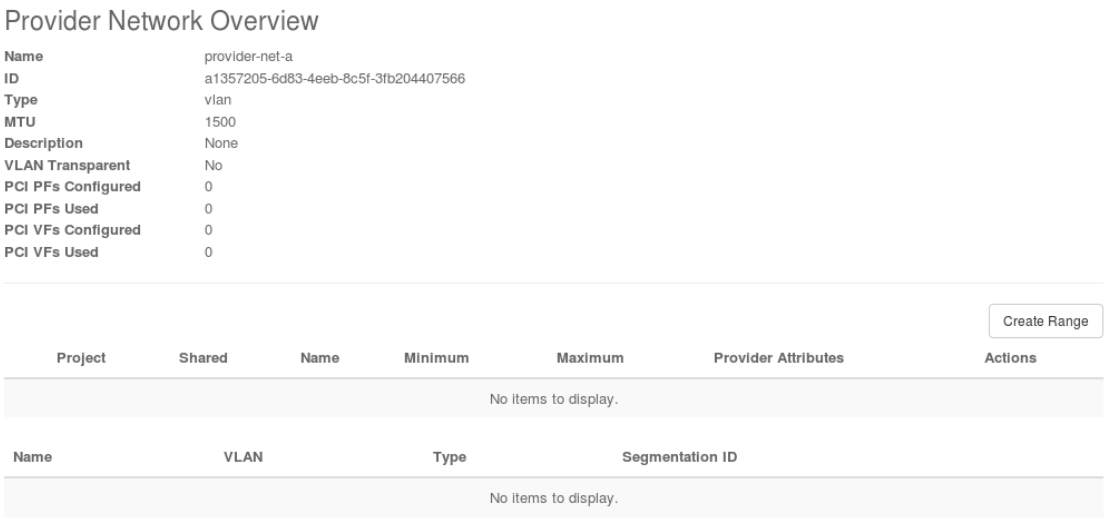
1. List the provider networks currently defined on the system.

   Select **Admin** > **Platform** > **Provider Networks**.

   The Provider Networks page appears.

2. Click the name of the provider network where you want to create a segmentation range.

   The Provider Network Overview page appears.



3. Add a segmentation range and assign it to a tenant.

   On the Provider Network Overview page, click **Create Range** to open the Create Segmentation Range page. Complete the form as required.

   Name

   The name of the segmentation range.

   Description

   A free-text field for reference.

   Shared

   If selected, shares the range for use by all tenants.

   Project

   The tenant associated with the segmentation range.

   Minimum

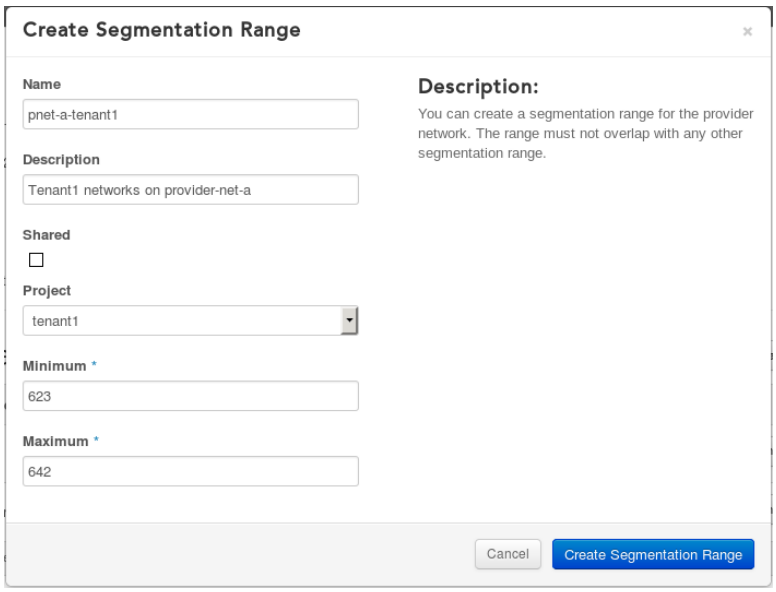
   The lowest value of a range of IDs.

   Maximum

   The highest value of a range of IDs.

⚠ **CAUTION:** The range must not overlap other segmentation ranges on the same provider network.

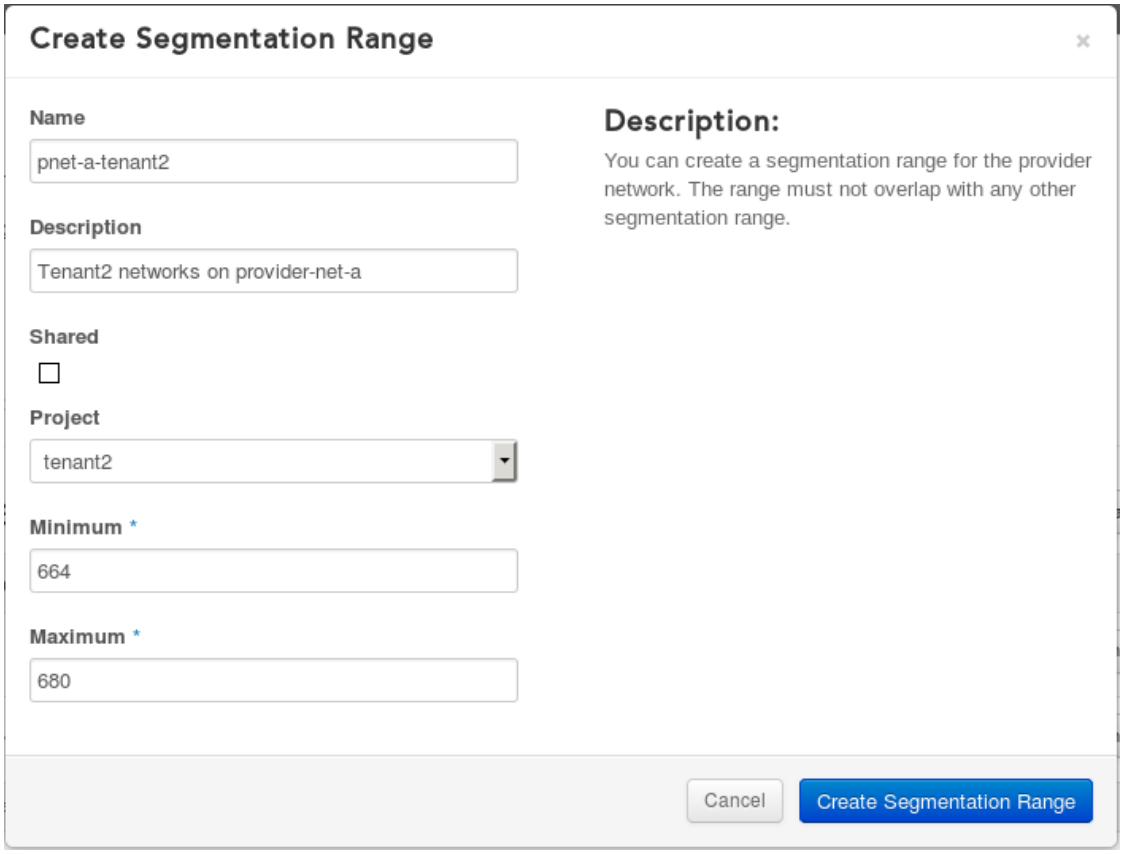
To add a segmentation range on **provider-net-a** for use by **tenant1**, fill in the form as illustrated below.



4. Click **Create Segmentation Range** to commit the changes.

5. Add a segmentation range on **provider-net-a** for use by **tenant2**.

   On the Provider Network Overview page, click **Create Range** to open the Create Segmentation Range page. Fill in the form as illustrated below:



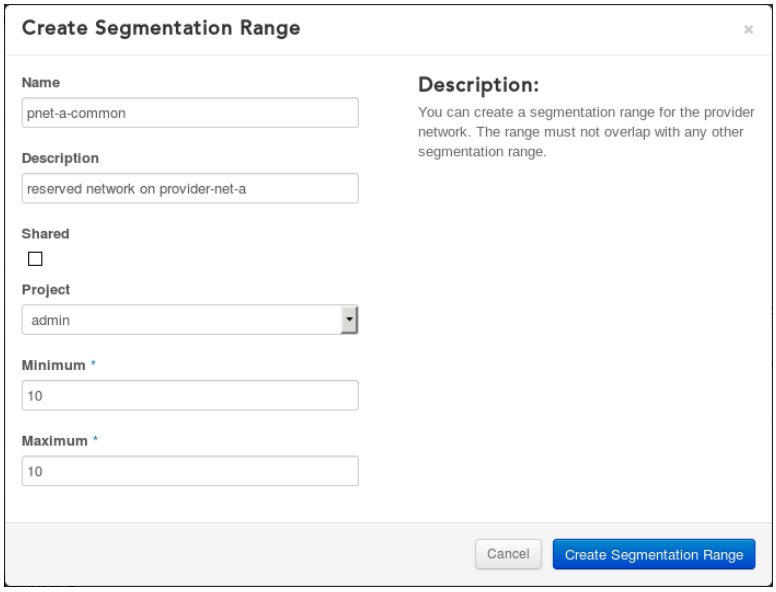
   Click **Create Segmentation Range** to commit the changes.

This creates a segmentation range on **provider-net-a** for use by **tenant2**. The range includes VLAN IDs 664–680. For reference, this range is assigned the name **pnet-a-tenant2**.

6. Add a segmentation range on **provider-net-a** for use by the **admin** tenant.

   This step assigns a segmentation range with a single VLAN ID (10) for use only by the **admin** tenant. Later in this exercise, the **admin** tenant uses this VLAN ID for the **external-net** tenant network.

   On the Provider Network Overview page, click **Create Range** to display the Create Segmentation Range page. Fill in the form as illustrated below:



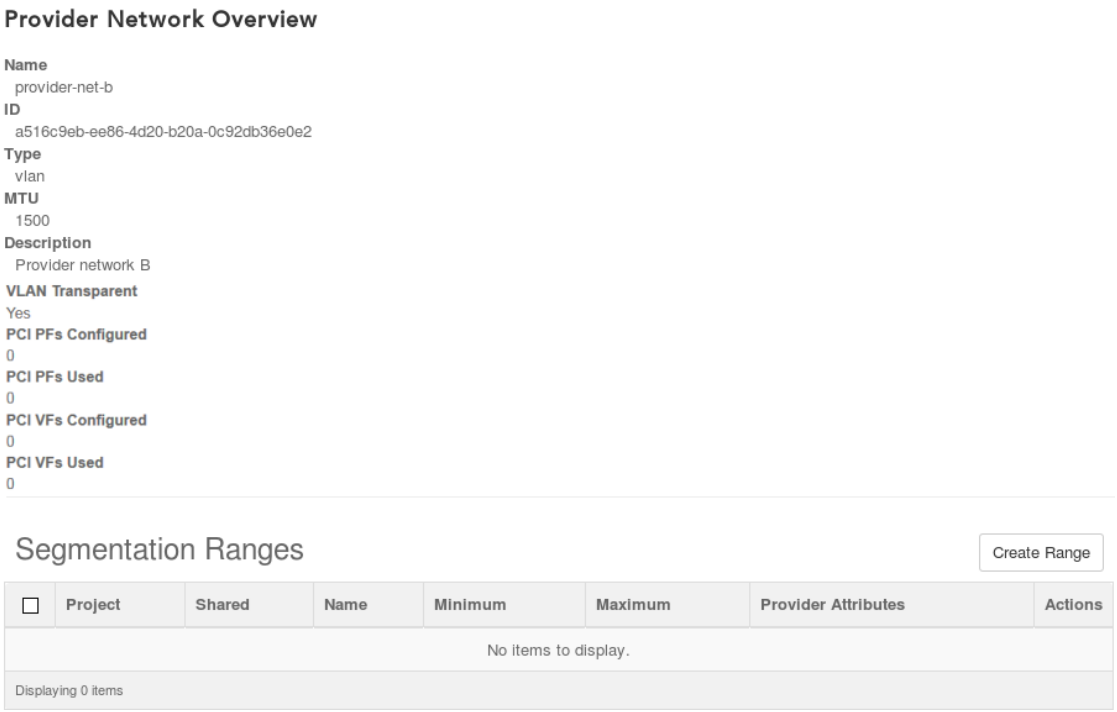
   Click **Create Segmentation Range** to commit the changes.

   This creates a segmentation range on **provider-net-a** for use by **admin**. The range includes a single VLAN ID (10). For reference, this range is assigned the name **pnet-a-common**.

7. Edit **provider-net-b** to add a segmentation range.

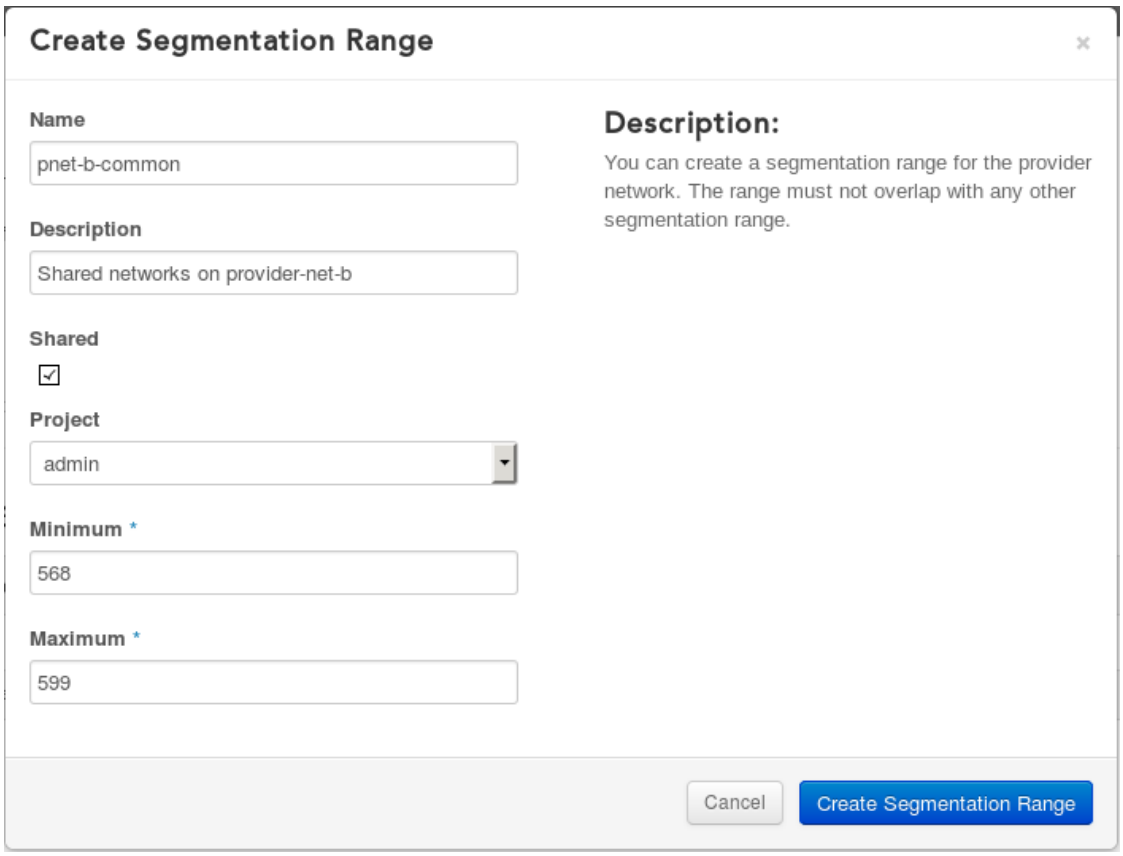
   On the Provider Networks page, click **provider-net-b**.

   The Provider Network Overview page appears.



8. Add a segmentation range on **provider-net-b** for use by all tenants.

   On the Provider Network Overview page, click **Create Range** to open the Create Segmentation Range page. Fill in the form as illustrated below:



Click **Create Segmentation Range** to commit the changes.

This creates a *shared* segmentation range on **provider-net-b**. Shared segmentation ranges contain VLAN IDs that can be used by any tenant. This one includes VLAN IDs 568–599. For reference, this range is assigned the name **pnet-b-common**.

Creating Segmentation Ranges Using the CLI

You can use the CLI to add segmentation ranges to provider networks.

Prerequisites

This task assumes that provider networks have already been created in order to unlock the compute nodes and make the system operational. For more information about creating provider networks, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Configuring Provider Networks on page 25*.

Procedure

Use the **neutron providernet-range-create** command to create segmentation ranges.

This example creates segmentation ranges on provider network **provider-net-a**.

```
~(keystone_admin)$ neutron providernet-range-create provider-net-a \
--name pnet-a-common --description "External network access" --range 10-10
~(keystone_admin)$ neutron providernet-range-create provider-net-a \
--name pnet-a-tenant1 --tenant-id ${tenant1_UUID} --description "Shared internal
network" \
--range 623-642
~(keystone_admin)$ neutron providernet-range-create provider-net-a \
```

```
--name pnet-a-tenant2 --tenant-id ${tenant2_UUID} --description "Shared internal
network" \
--range 664-680
```

Using VXLANs

You can use Virtual eXtensible Local Area Networks (VXLANs) to connect VM instances across non-contiguous Layer 2 segments (that is, Layer 2 segments connected by one or more Layer 3 routers).

A VXLAN is a Layer 2 overlay network scheme on a Layer 3 network infrastructure. Packets originating from VMs and destined for other VMs are encapsulated with IP, UDP, and VXLAN headers and sent as Layer 3 packets. The IP addresses of the source and destination compute nodes are included in the headers.

You can configure VXLANs on HCG 4.0 using the following workflow.

Procedure

1. Set up a provider network of the VXLAN type.

   For details, see Setting Up a VXLAN Provider Network on page 34.

2. Configure the endpoint IP addresses of the compute nodes.
   - To configure static IP addresses for individual interfaces, see Adding a Static IP Address to a Data Interface on page 38.
   - To assign IP addresses from predefined address pools, see Using IP Address Pools for Data Interfaces on page 42.

3. Establish routes between the hosts.

   For details, see Adding and Maintaining Routes for a VXLAN Network on page 44

Postrequisites

You must also ensure that the networking environment meets certain minimum requirements. For more information, see *Tenant Networks*.

Setting Up a VXLAN Provider Network

You can use the CLI or the web administration interface to set up a VXLAN provider network and add segmentation ranges.

VXLAN provider networks are an alternative to VLAN provider networks when VM L2 connectivity is required across separate Layer 2 network segments separated by one or more Layer 3 routers.

The steps in this section describe how to set up a VXLAN provider network and add segmentation ranges using the web administration interface. For information about using CLI commands, see Setting Up a VXLAN Provider Network Using the CLI on page 36.

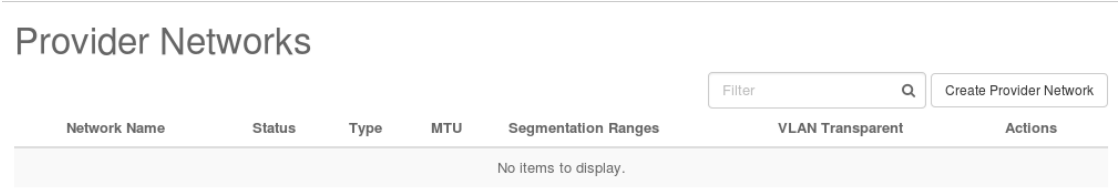
Procedure

1. Open the HCG 4.0 Web administration interface.

   Using a browser, navigate to the OAM floating IP address, and log in as **admin**.

2. In the left-hand pane, select **Admin** > **Platform** > **Provider Networks**.

   The Provider Networks list is displayed.



3. Create a provider network.

   Click **Create Provider Network**.

   In the Create Provider Network window, complete the fields as required.

   Name

   The name of the provider network.

   Description

   A free-text field for reference.

   Type

   The type of provider network to be created.

   flat

   mapped directly to the physical network

   vlan

   supports multiple tenant networks using VLAN IDs.

   vxlan

   supports multiple tenant networks using VXLAN VNIs.

   MTU

   The maximum transmission unit for the Ethernet segment used to access the network.

   VLAN Transparent

   Allow VLAN tagged packets to be encapsulated within a VXLAN segment without removing or modifying the guest VLAN tag.

   For the **Type**, select **VXLAN**.

   For the MTU, set a maximum transmission unit that allows for the overhead required by VXLAN encapsulation. For more information, see *The Ethernet MTU*.

4. Commit the changes.

   Click **Create Provider Network**.

The new provider network is added to the Provider Networks list.

5. Add one or more segmentation ranges.

   Segmentation ranges are sets of contiguous identifiers defined on a provider network. Each ID is used to implement a tenant network.

   On the Provider Network Overview page, click **Create Range** to open the Create Segmentation Range page. Complete the form as required.

   Name

   The name of the segmentation range.

   Description

   A free-text field for reference.

   Shared

   If selected, shares the range for use by all tenants.

   Project

   The tenant associated with the segmentation range.

   Minimum

   The lowest value of a range of IDs.

   Maximum

   The highest value of a range of IDs.

⚠ **CAUTION:** The range must not overlap other segmentation ranges on the same provider network.

6. Click **Create Segmentation Range** to commit the changes.

Setting Up a VXLAN Provider Network Using the CLI

You can use the command line interface to set up a VXLAN provider network and add segmentation ranges.

VXLAN provider networks are an alternative to VLAN provider networks when VM L2 connectivity is required across separate Layer 2 network segments separated by one or more Layer 3 routers.

The steps in this section describe how to set up a VXLAN provider network and add segmentation ranges using the command line interface. For information about using the web administration interface, see Setting Up a VXLAN Provider Network on page 34.

To create a provider network using the CLI, use the following command:

```
~(keystone_admin)$ neutron providernet-create name \
--type=type --description=description mtu mtu_size \
--vlan-transparent={True,False}
```

where

name

is a name for the provider network

type

is the type of provider network (**flat**, **vlan**, or **vxlan**)

description

is a brief description for reference purposes

mtu_size

is the maximum transmission unit size

For example, to add a VXLAN provider network named providernet-a:

```
~(keystone_admin)$ neutron providernet-create providernet-a --type=vxlan
Created a new providernet:
+------------------+--------------------------------------+
| Field            | Value                                |
+------------------+--------------------------------------+
| description      |                                      |
| id               | a5938194-a296-4d92-af5f-c3a064b56f7f |
| mtu              | 1500                                 |
| name             | providernet-a                        |
| ranges           |                                      |
| status           | DOWN                                 |
| type             | vxlan                                |
| vlan_transparent | False                                |
+------------------+--------------------------------------+
```

To add a segmentation range using the CLI, use the following command:

```
~(keystone_admin)$ neutron providernet-range-create provider_network \
--name=range_name --tenant_id=tenant \
--description=description --range min-max \
--group multicast_address --port=udp_port \
--ttl=time_to_live
```

where

provider_network

is the name of the associated provider network

name

is a name for the segmentation range

tenant

is the name or UUID of the tenant associated with the range

description

is a brief description for reference purposes

min

is the lowest value in the range

max

is the highest value in the range

vlan-transparent

Allow VLAN tagged packets to be encapsulated within a VXLAN segment without removing or modifying the guest VLAN tag.

The following additional values are used for segmentation ranges on VxLAN provider networks:

multicast_address

The IPv4 or IPv6 address for participation in a multicast group used to discover MAC addresses for destination VMs. You can use a different multicast group for each segmentation range to help organize and partition network traffic.

udp_port

The destination UDP port for packets sent on the VXLAN. You can select either the IANA standard 4789 to use this range with the OpenStack Neutron service, or the legacy standard 8472 for use with some commercial switch equipment.

time_to_live

The time-to-live, measured in hops, for packets sent on the VXLAN. The value is decremented at each hop; when it reaches zero, the packet expires. You can use this to limit the scope of the VXLAN. For example, to limit the packet to no more than three router hops, use a time-to-live value of 4.

For more about these parameters, refer to the steps for using the web administration interface.

You can obtain information about provider networks and segmentation ranges using the following commands.

```
~(keystone_admin)$ neutron net-list-on-providernet providernet

~(keystone_admin)$ neutron providernet-range-show providernet-range
```

Adding a Static IP Address to a Data Interface

You can add static IP addresses to a data interface using the web administration interface or the command line.

For VXLAN connectivity between VMs, you must add appropriate endpoint IP addresses to the compute node interfaces. You can add individual static addresses, or you can assign addresses from a pool associated with the data interface. For more about using address pools, see Using IP Address Pools for Data Interfaces on page 42.

To add a static IP address using the web administration interface, refer to the following steps. To use the command-line interface, see Managing Data Interface Static IP Addresses Using the CLI on page 40

Prerequisites

To make interface changes, you must lock the compute host first.

Procedure

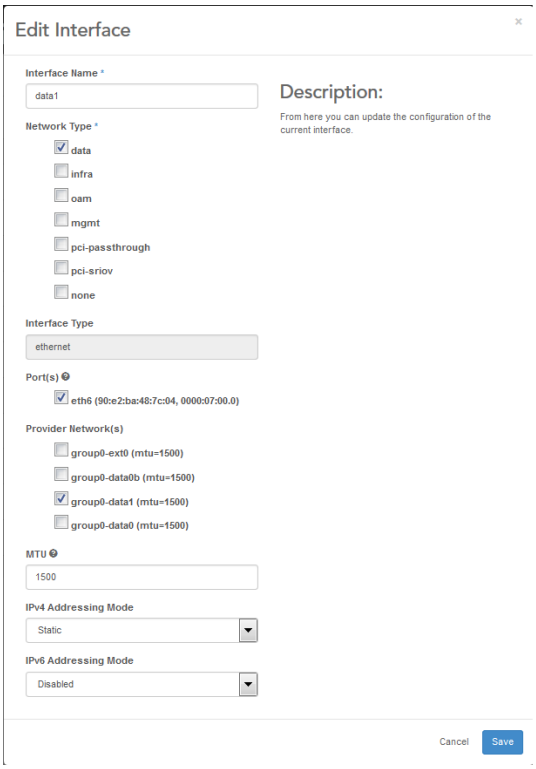
1. Lock the compute host.
2. Set the interface to support an IPv4 or IPv6 address, or both.

a) Select **Admin** > **Platform** > **Host Inventory** to open the Host Inventory page.

b) Select the **Host** tab, and then double-click the compute host to open the Host Detail page.

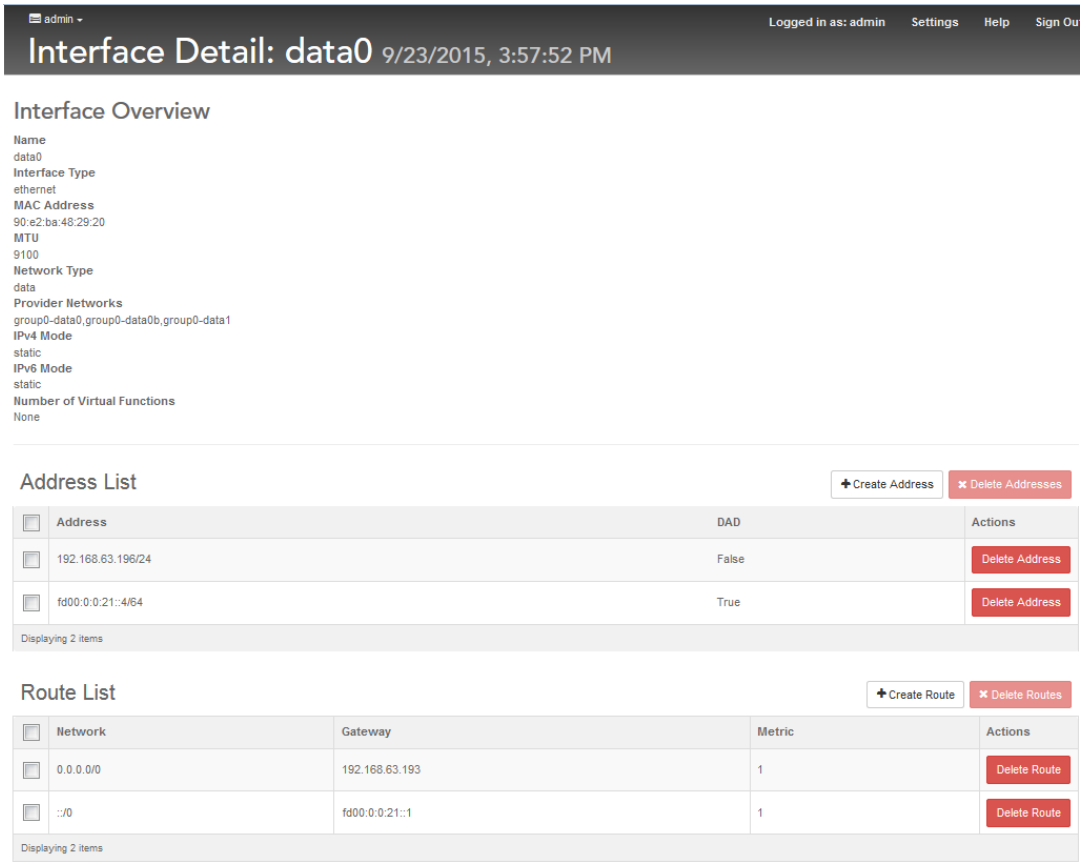
c) Click **Edit Interface** for the data interface you want to edit.

d) In the Edit Interface dialog box, set the **IPv4 Addressing Mode** or the **IPv6 Addressing Mode** to **Static**.

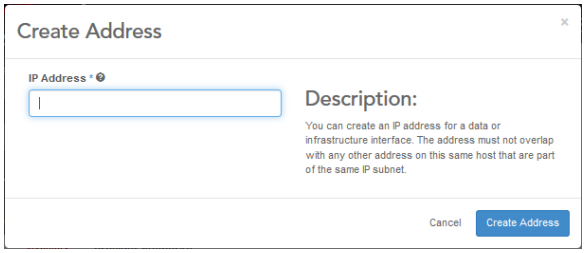


3. Add an IPv4 or IPv6 address to the interface.

a) On the Inventory Detail page, click the **Name** of the interface to open the Interface Detail page.



b) Click **Create Address** to open the Create Address dialog box.



c) Enter the IPv4 or IPv6 address and netmask (for example, 192.168.1.3/24), and then click **Create Address**.

The new address is added to the **Address List**.

4. Unlock the compute node and wait for it to become available.

Managing Data Interface Static IP Addresses Using the CLI

If you prefer, you can create and manage static addresses for data interfaces using the CLI.

For more infomation about using static addresses for data interfaces, see Adding a Static IP Address to a Data Interface on page 38.

Prerequisites

To make interface changes, you must lock the compute node first.

Procedure

1. Lock the compute node.
2. Set the interface to support an IPv4 or IPv6 address, or both.

```
~(keystone_admin)$ system host-if-modify node ifname --ipv4-mode=ipv4mode --ipv6-
mode=ipv6mode
```

where

node

is the name or UUID of the compute node

ifname

is the name of the interface

ipv4mode

is either **disabled** or **static**

ipv6mode

is either **disabled** or **static**

3. Add an IPv4 or IPv6 address to the interface.

```
~(keystone_admin)$ system host-addr-add node ifname ip_address prefix
```

where

node

is the name or UUID of the compute node

ifname

is the name of the interface

ip_address

is an IPv4 or IPv6 address

prefix

is the netmask length for the address

To delete an address, use the following commands:

```
~(keystone_admin)$ system host-addr-list hostname/ID
```

This displays the UUIDs of existing addresses, as shown in this example below.

```
~(keystone_admin)$ system host-addr-list compute-0

+--------------------------------------+--------
+--------------------------------------+--------+
| uuid                                 | ifname |
address                            | prefix |
+--------------------------------------+--------
```

```
+--------------------------------------+--------+
| 290629f6-41e5-48d9-8b4c-cca1f459d2d2 | ae0    |
2605:6400:2:fed5:22:e7c7:2700:e5c3 | 112    |
| 5de0e0bf-21fc-4532-b33b-bf07eaedf82e | ae0    |
2605:6400:2:fed5:22:e7c7:27b9:e5c3 | 122    |
| e78923d7-3ccf-4332-a28e-04a56be7b616 | ae0    |
192.168.61.70                        | 27     |
+--------------------------------------+--------
+--------------------------------------+--------+
```

```
~(keystone_admin)$ system host-addr-delete uuid
```

where **uuid** is the UUID of the address.

4. Unlock the compute node and wait for it to become available.

Using IP Address Pools for Data Interfaces

You can create pools of IP addresses for use with data interfaces.

As an alternative to manually adding static IP addresses to data interfaces for use with VXLANs, you can define pools of IP addresses and associate them with one or more data interfaces. Each pool consists of one or more contiguous ranges of IPv4 or IPv6 addresses. When a data interface is associated with a pool, its IP address is allocated from the pool. The allocation may be either random or sequential, depending on the settings for the pool.

You can use the web administration interface or the CLI to create and manage address pools. For information about using the CLI, see Managing IP Address Pools Using the CLI on page 43.

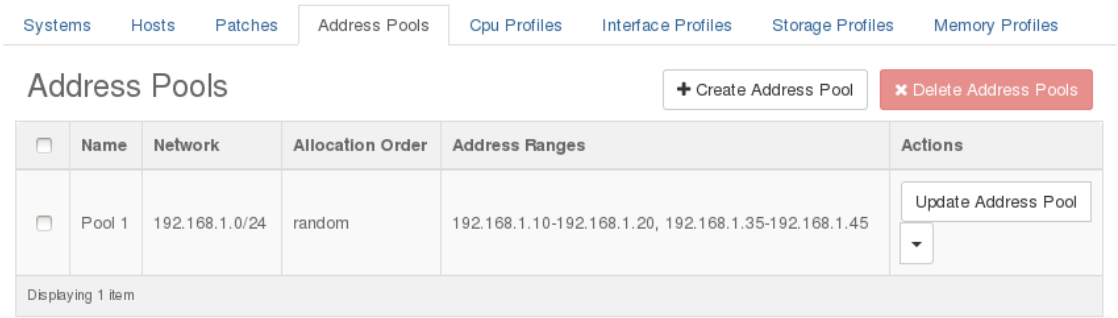
Prerequisites

To make interface changes, you must lock the compute node first.

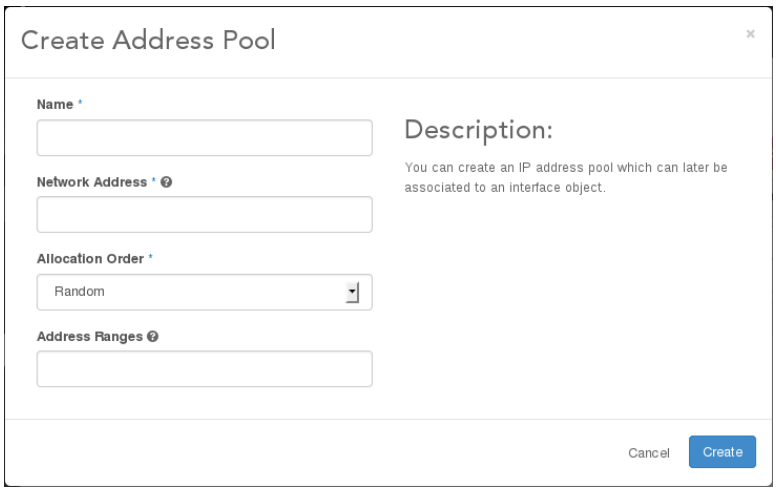
Procedure

1. Lock the compute node.
2. In the HCG 4.0 Web administration interface, open the System Configuration page.

   The System Configuration page is available from **Admin** > **Platform** > **System Configuration** in the left-hand pane.
3. Select the **Address Pools** tab.



   You can use the controls on the Address Pools page to create, update, or delete address pools.
4. To create an address pool, click **Create Address Pool** and complete the dialog box.



Name

A name used for selecting the pool during data interface setup.

Network Address

The subnet for the range (for example, **192.168.1.0/24**).

Allocation Order

The order for assigning addresses. You can select **Sequential** or **Random** from the drop-down list.

Address Range

One or more ranges, where the start and end IP address of each range is separated by a dash, and the ranges are separated by commas (for example, **192.168.1.10-192.168.1.20, 192.168.1.35-192.168.1.45**). If no range is specified, the full range is used.

Postrequisites

You can select an address pool by name when setting up the **IPv4 Addressing Mode** or **IPv6 Addressing Mode** for a data interface. For more information, see Interface Settings on page 78.

Managing IP Address Pools Using the CLI

You can create and manage address pools using CLI commands.

For more information about address pools, see Using IP Address Pools for Data Interfaces on page 42.

Prerequisites

To make interface changes, you must lock the compute node first.

Creating an Address Pool

To create an address pool, use a command of the following form:

```
~(keystone_admin)$ system addrpool-add name network prefix \
[-- order assign_order] [--ranges addr_ranges]
```

where:

name

is a name used to select the pool during data interface setup

network

is the subnet and mask for the range (for example, **192.168.1.0**)

prefix

is the subnet mask, expressed in network prefix length notation (for example, **24**)

assign_order

is the order in which to assign addresses from the pool (**random** or **sequential**). The default is **random**.

addr_ranges

is a set of IP address ranges to use for assignment, where the start and end IP address of each range is separated by a dash, and the ranges are separated by commas (for example, **192.168.1.10-192.168.1.20, 192.168.1.35-192.168.1.45**). If no range is specified, the full range is used.

Listing Address Pools

To list existing address pools, use a command of the following form:

```
~(keystone_admin)$ system addrpool-show uuid
```

where *uuid* is the universally unique identifier for the pool.

Modifying an Address Pool

To modify an address pool, use a command of the following form:

```
~(keystone_admin)$ system addrpool-modify uuid [--name name] \
[-- order assign_order] [--ranges addr_ranges]
```

Deleting an Address Pool

To delete an address pool, use a command of the following form:

```
~(keystone_admin)$ system addrpool-delete uuid
```

Postrequisites

To use address pools with data interfaces, see Using IP Address Pools for Data Interfaces on page 42.

Adding and Maintaining Routes for a VXLAN Network

You can add or delete routing table entries for hosts on a VXLAN network using the CLI.

Prerequisites

The compute node must be locked.

To add routes, use the following command.

```
~(keystone_admin)$ system host-route-add node ifname network prefix gateway metric
```

where

node

is the name or UUID of the compute node

ifname

is the name of the interface

network

is an IPv4 or IPv6 network address

prefix

is the netmask length for the network address

gateway

is the default gateway

metric

is the cost of the route (the number of hops)

To delete routes, use the following command.

```
~(keystone_admin)$ system host-route-delete uuid ifname network prefix gateway metric
```

where **uuid** is the UUID of the route to be deleted.

To list existing routes, including their UUIDs, use the following command.

```
~(keystone_admin)$ system host-route-list compute-0
```

Overview of Provider Network Connectivity Tests

These tests check the connectivity between compute nodes over each segment of each provider network.

This enables you to verify that a provider network is configured correctly before launching VMs on the network.

Audits run both periodically, and when triggered by provider network or host events, in order to test the connectivity over each network segment. They can also be manually requested using the CLI.

The tests for each network type are as follows:

- Flat: Ping between compute nodes on the network.
- VLAN: Ping between compute nodes over each VLAN segment assigned to the provider network.
- VXLAN: Ping for each segmentation range assigned to the provider network.

For each individual test, one ping is sent with a size of 64 bytes, and another is sent with the MTU of the provider network. Each of those pings is sent from each node to 2 elected masters, and the results are reported to neutron-server.

If a failure occurs on an audit run, an alarm is raised with details of the provider network connectivity failure.

Provider Network Connectivity Test CLI Commands

CLI commands are available for listing and scheduling provider network connectivity tests.

neutron providernet-connectivity-test-list

This command lists the connectivity information for the provider networks. The following parameters are available:

- **--audit-uuid**
- **--providernet-name**
- **--providernet-id**
- **--host-name**
- **--host-id**
- **--segmentation-id**

```
[root@controller-0 wrsroot(keystone_admin)]# neutron providernet-connectivity-test-list

+--------------------------------------+------------------+------+
| providernet_id                       | providernet_name | type |
+--------------------------------------+------------------+------+
| ed20d5e5-d193-48ea-9dae-c5cb5b2ab056 | physnet1         | vlan |
| ecc16429-4580-4bfa-bfbd-b8d096543300 | physnet0         | vlan |
| ed20d5e5-d193-48ea-9dae-c5cb5b2ab056 | physnet1         | vlan |
| ecc16429-4580-4bfa-bfbd-b8d096543300 | physnet0         | vlan |
+--------------------------------------+------------------+------+

-----------+------------------+--------+
 host_name | segmentation_ids | status |
-----------+------------------+--------+
 compute-1 | 500-599          | PASS   |
 compute-0 | 10, 400-499      | PASS   |
 compute-0 | 500-599          | PASS   |
 compute-0 | 500-599          | PASS   |
 compute-1 | 10, 400-499      | PASS   |
 ----------+------------------+--------+
```

neutron providernet-connectivity-test-schedule

This command schedules a new connectivity test to be run. The following parameters are available:

- **--host**
- **--providernet**
- **--segmentation-id**

```
[root@controller-0 wrsroot(keystone_admin)]# neutron providernet-connectivity-test-
schedule

Created a new providernet_connectivity_test:
+---------------+--------------------------------------+
| Field         | Value                                |
+---------------+--------------------------------------+
| audit_uuid    | 4d22c747-6dba-4548-947e-b63a5160121e |
+---------------+--------------------------------------+
```

4

Node Hardware Management

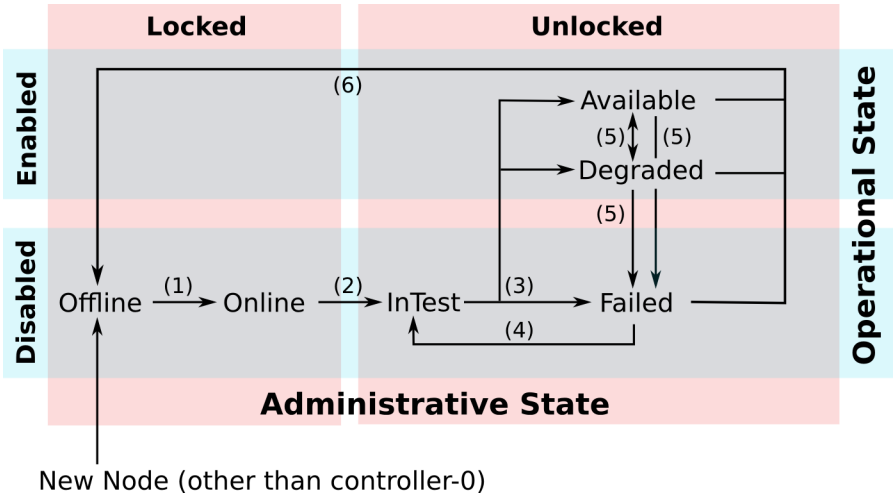
The Life Cycle of a Host

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 HCG 4.0 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.

Figure 1: The Life Cycle of a Host



In this figure:

- The administrative states, locked and unlocked, are presented in two columns.
- The operational states, disabled and enabled, are presented in two rows.
- The availability states are presented as elements inside the administrative/operational matrix.

The description that follows uses the availability states only, because for each state the corresponding administrative and operational states can be read directly from the figure.

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:

(1) *Offline* to *Online*

This transition takes place once the administrator configures the host name and personality of the host. During the transition, the HCG 4.0 software is installed and the host reboots. The transition concludes when the controller establishes maintenance and inventory connectivity with the new host.

(2) *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.

(3) *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.

(4) *Failed* to *InTest*

This is a value-added maintenance transition that the HA framework executes automatically to recover failed hosts.

(5) *Available* to/from *Degraded*, *Available* to *Failed*, and *Degraded* to *Failed*

These are transitions that can occur at any time due to changes on the operational state and faults on unlocked hosts.

(6) *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 migration of the active instances to another available compute node.

Host Status and Alarms During System Configuration Changes

For all types of configuration changes, alarms and status messages appear while the system is in transition. You can use the information provided by these messages to help guide the transition successfully.

Configuration changes require multiple hosts to be reconfigured, during which the settings across the cluster are not consistent. This causes alarms to be raised for the system.

- Changes to the DNS server configuration cause transitory alarms. These alarms are cleared automatically when the configuration change is applied.
- Changes to the External OAM network IP addresses or NTP server addresses, and in particular to the controller storage allotments, cause persistent alarms. These alarms must be cleared manually, by locking and unlocking the affected hosts or performing other administrative actions.

Alarms appear on the Fault Management page, and related status messages appear on the Hosts tab on the Host Inventory page. A variety of alarms can be reported on the Fault Management page, depending on the configuration change.

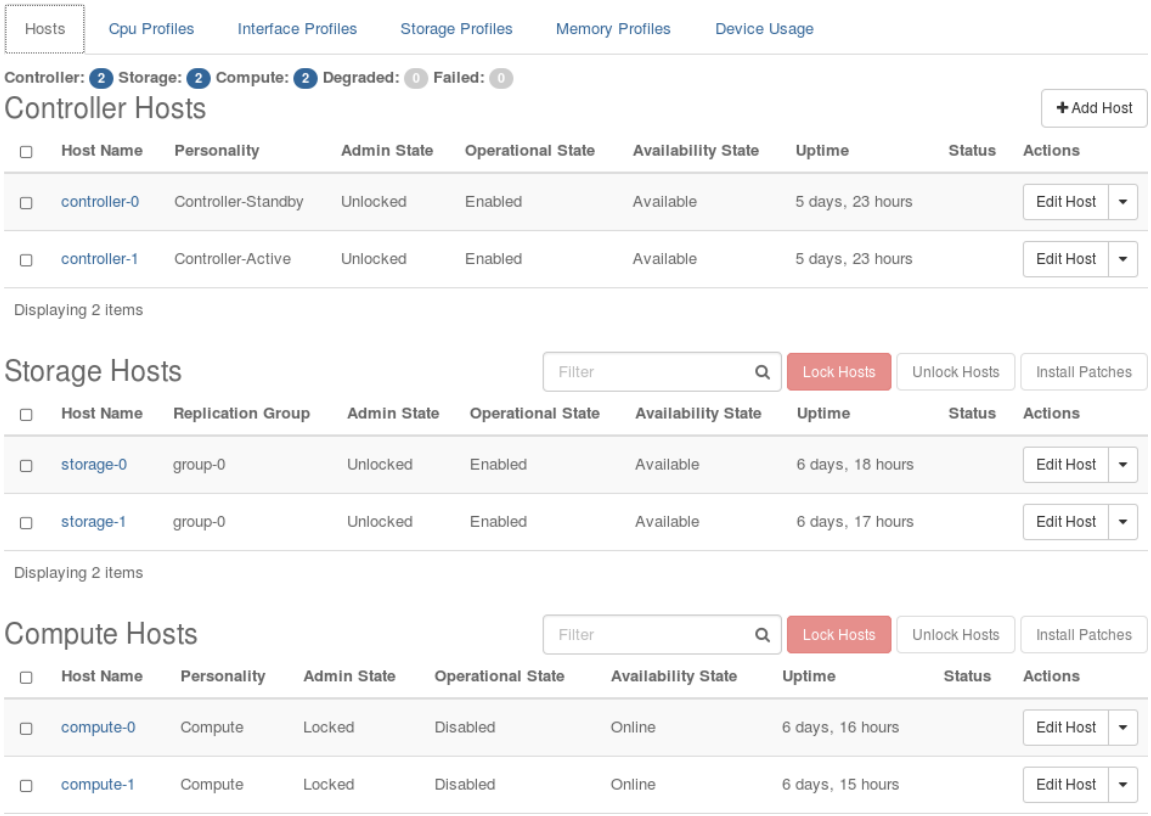
⚠ **CAUTION:** To help identify alarms raised during a configuration change, ensure that any existing system alarms are cleared before you begin.

On the Hosts tab of the Host Inventory page, the status **Config out-of-date** is shown for hosts affected by the change. Each host with this status must be locked and then unlocked to update its configuration and clear the alarm.

Host Inventory

The **Hosts** tab on the Host Inventory page provides an overview of the current state of all hosts in the HCG 4.0 cluster. From this tab, you can obtain detailed information about the hosts, and execute maintenance operations.

A sample **Hosts** tab is illustrated below:



Host Name

The name assigned to the host. This is an active link pointing to the detailed inventory page for the host. For more information, see Inventory Detail on page 58.

Personality

The personality of the host (controller, compute, or storage).

Replication Group

For a storage host, the group to which the host belongs. Data is replicated on each host in the group. For more information, see Storage Clusters (Replication Groups) on page 137.

Admin State

The administrative state of the host:

Locked

The host is administratively prohibited from performing services. This is the initial state for hosts auto-discovered in the cluster.

A controller node in this state is not functioning in HA mode, and it is not running any active controller services.

Compute and storage nodes in this state do not provide any service. In particular, a locked compute node is not running any virtual machine instances, and no new ones will be scheduled to run on it.

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.

A compute node in this state, and not in the failed state, is eligible for regular scheduling and maintenance operations on virtual machines.

A storage node in this state, and not in the failed state, provides storage services.

Operational State

The operational state of the host:

Disabled

Indicates that the host is not providing the expected services. This can 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 the 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 HCG 4.0, 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. For more information, see Fault Management on page 211.

Failed

A major fault has occurred and the host is no longer providing any services. The HCG 4.0 maintenance system automatically tries to recover hosts in this state.

In the case of a compute node, any virtual machines that were running before are immediately evacuated to another enabled compute node with sufficient available resources.

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.

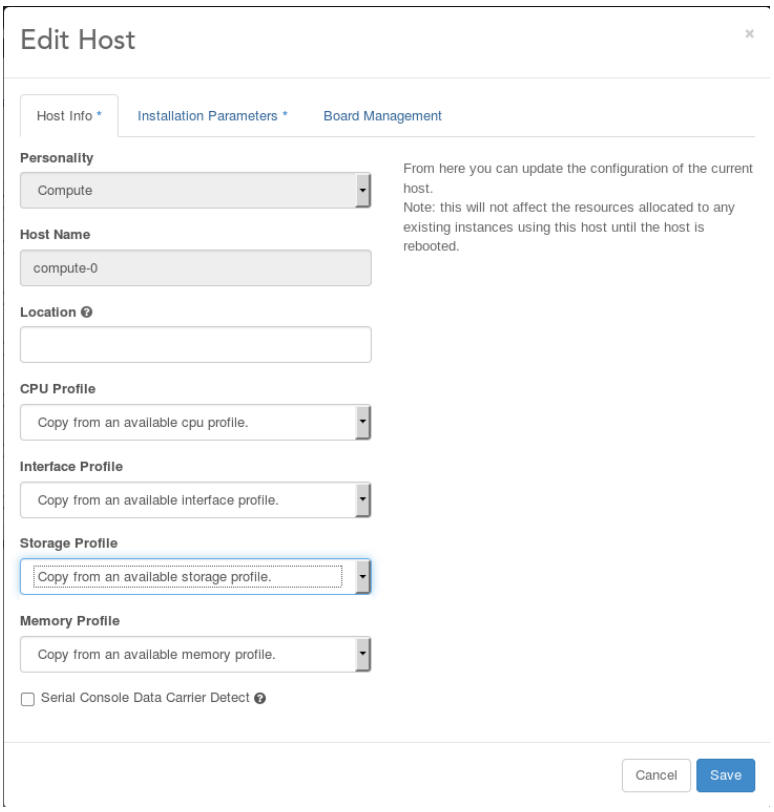
Status

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.

Actions

The actions column presents an **Edit Host** button and a drop-down menu.

The **Edit Host** button displays the Edit Host window as illustrated below for a compute node:



This is the same window you use to assign the host's personality when installing the HCG 4.0 software on the host.

- The **Host Info** tab provides access for modifying the host name (compute and storage nodes only) and applying profiles. For more about profiles, see *HCG 4.0 Installation: Hardware Profiles*.
- The **Installation Parameters** tab provides access to installation settings. Changes take effect if the host is re-installed. For more information, see the *HCG 4.0 Installation* document that pertains to your HCG 4.0 configuration.
- The **Board Management** tab provides access to the management board configuration, if available on the host. For more information, see *HCG 4.0 Planning: Board Management Network Planning*.

Next to the **Edit Host** button is a drop-down menu used for maintenance operations. The available operations depend on the host type and state, and on whether the host is configured for board management.

Lock Host

Attempts to bring an unlocked 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 migrated to alternative compute nodes. Migration of the virtual machine instances is initiated automatically by HCG 4.0 as soon as the state transition is requested. For more about migration behavior, see VM Storage Settings for Migration, Resize, or Evacuation on page 159.

You can lock a host from the controller's command line, as follows:

```
~(keystone_admin)$  system host-lock hostname
```

Forced Lock Host

Forces an unlocked host to be out of service.

⚠

CAUTION: A force lock operation on a compute host causes an immediate service outage on all hosted virtual machines (VM failures). Before using a force lock on a compute host, perform the following steps:

1. Try to lock the host normally using **Lock Host**.
2. If the **Lock Host** attempt fails, manually migrate all VMs running on the host, and then try using **Lock Host** again.

Use a force lock only if the above steps fail to lock the host.

You can also apply a force lock from the controller's command line as follows:

```
~(keystone_admin)$  system host-lock --force hostname
```

When you apply a force lock, the system displays a warning message appropriate to the personality of the host.

Swact Host

This operation is available on controller nodes only. It initiates 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.

You can swact a host from the controller's command line as follows:

```
~(keystone_admin)$  system host-swact --force hostname
```

Unlock Host

Brings a locked host into service. The first step is to reset the target host to ensure that it starts from a well-known 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.

You can unlock a host from the controller's command line as follows:

```
~(keystone_admin)$  system host-unlock hostname
```

Reboot Host

Gracefully shuts down a locked host, ensuring that all system processes are properly shut off first. The host then reboots automatically.

You can reboot a host from the controller's command line as follows:

```
~(keystone_admin)$  system host-reboot hostname
```

Reinstall Host

Forces a full re-installation of the HCG 4.0 software on a locked host. The host's hard drive is erased, and the installation process is started afresh.

NOTE: Performing a host reinstall successfully is dependent on your BIOS boot order. Observe the following tips:

- Prior to installation, configure the BIOS to allow booting from disk and the network.
- During the host re-installation, it is recommended that you have a console serial cable attached to the host to observe the boot progress.
- The BIOS boot order should be:
  1. The boot partition.
     Typically, this is the disk associated with **/dev/sda** and is as defined in **/proc/cmdline** when the load is booted.
  2. The NIC on the boot interface (such as management or PXE network).
- Set the BIOS boot options to ensure a failsafe boot, if available; for example, rotating through available boot interfaces, watchdog timer on boot, retry boot interfaces, and so forth.

If the BIOS boot still fails to progress, you may need to force a boot using the network interfaces through the BIOS boot option.

Power Off Host

Gracefully powers off the host, ensuring that all system processes are properly shut off first. 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 power off a host from the controller's command line as follows:

```
~(keystone_admin)$  system host-power-off hostname
```

Power On Host

Powers on the host. 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-off state.

You can power on a host from the controller's command line as follows:

```
~(keystone_admin)$  system host-power-on hostname
```

Reset Host

Performs an out-of-band reset, stopping and restarting the host without ensuring that all system processes are shut off first. 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.

Use this selection only if **Reboot Host** fails.

You can reset a host from the controller's command line as follows:

```
~(keystone_admin)$  system host-reset hostname
```

Delete Host

Removes the host from the inventory database, and erases its hard drive.

You can delete a host from the controller's command line as follows:

```
~(keystone_admin)$  system host-delete hostname
```

Install Patches

Initiates any pending patching operations. Once successfully executed, the host returns back to the locked state. See *HCG 4.0 Software Management: Managing Software Patches* for details.

This option is only available if there are patching operations pending for the host.

Inventory Detail

From the Inventory Detail page you can see and edit detailed information about a host, and use it to define hardware profiles that can be used across the cluster.

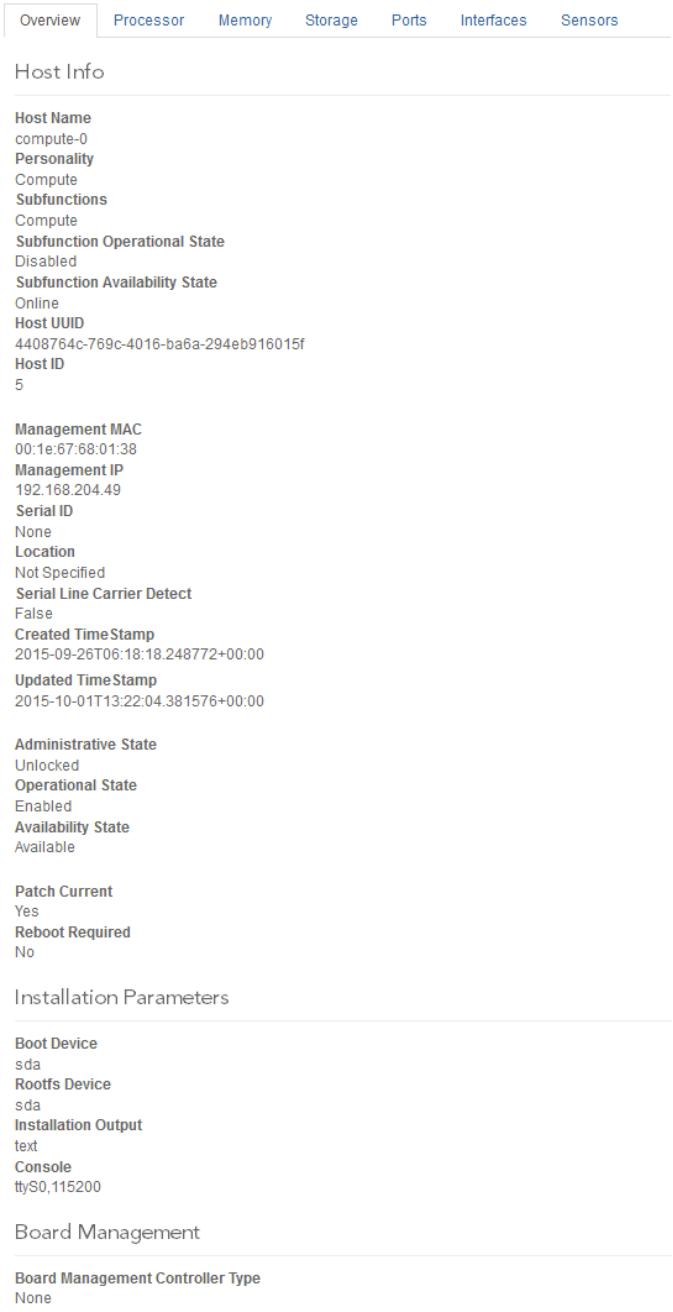
To access the Inventory Detail page for a host, select **Admin** > **Platform** > **Host Inventory**, and then on the Hosts tab, click the name of the host.

The inventory detail for a host consists of multiple tabs, each addressing a different aspect of the host. They include:

- Overview Tab on page 59
- Processor Tab on page 60
- Memory Tab on page 62
- Storage Tab on page 63
- Ports Tab on page 67
- Interfaces Tab on page 68
- Sensors Tab on page 70
- Devices Tab on page 73

Overview Tab

The **Overview** tab on the Inventory Detail page summarizes core details about a host object.



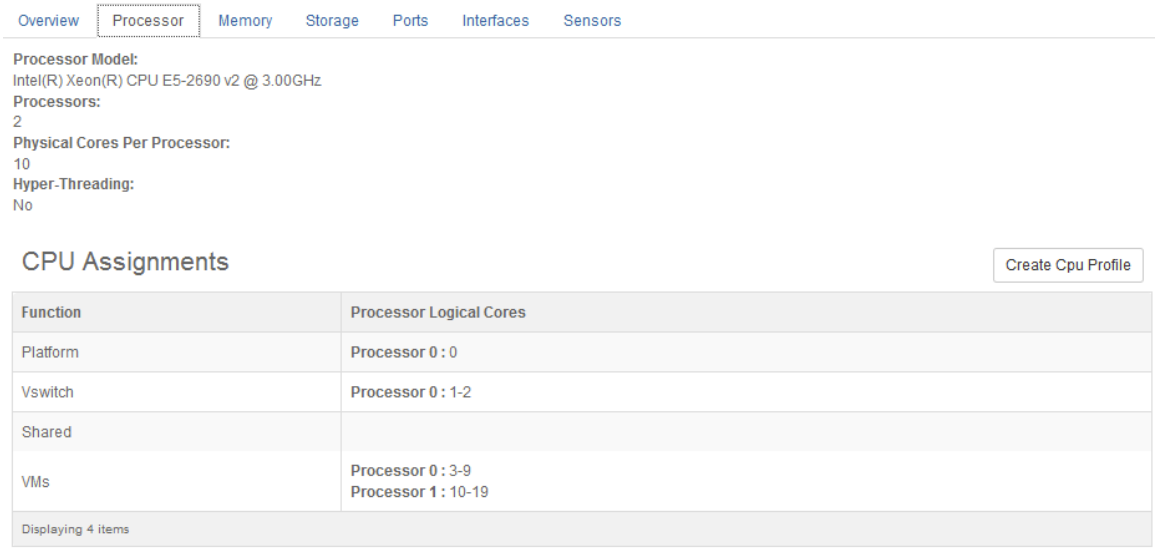
The following items are included in the summary:

- 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-update <hostname> serialid=xxx** to update it.

- location, as entered by the operator using the Edit Host window (see Host Inventory on page 52)
- 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

Processor Tab

The **Processor** tab on the Inventory Detail page presents processor details for a host.



The **Processor** tab includes the following items:

- processor model, number of processors, number of cores per processor, and Hyper-Threading status (enabled or disabled)
- the CPU assignments. For more details, see *HCG 4.0 Installation: CPU Profiles*.

Two buttons are also available as follows:

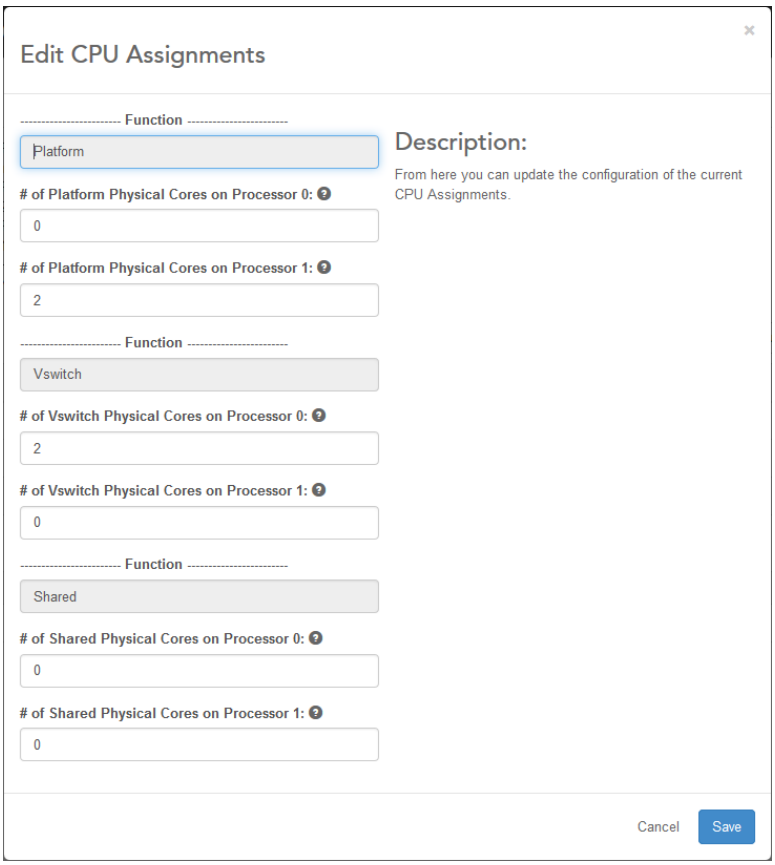
Create CPU Profile

Clicking this button displays the Create CPU Profile window. For more information, see *HCG 4.0 Installation: Hardware Profiles*.

Edit CPU Assignments

This button is available only when the host is in the locked state.

Clicking this button displays the Edit CPU Assignments window. On a compute node, you can use this window to assign cores to specific functions, as illustrated below. Unassigned cores are available for allocation to virtual machine threads. Changes do not take effect until the host is unlocked.



NOTE: On a controller or storage node, only the Platform function is shown, and all available cores are automatically assigned as platform cores.

Platform

You can reserve one or more cores in each NUMA node for platform use. One core on each host is required to run the operating system and associated services.

The ability to assign platform cores to specific NUMA nodes offers increased flexibility for high-performance configurations. For example, you can dedicate certain NUMA nodes for vSwitch or VM use, or affine VMs that require high-performance IRQ servicing with NUMA nodes that service the requests.

Vswitch

AVS (vSwitch) 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 when all AVS cores, the physical ports, and the virtual machines that use them are running on the same processor. You can affine VMs to NUMA nodes with AVS cores; for more information, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Affining a VM to a NUMA Node with a vSwitch Core*. Alternatively, 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 1 to the AVS threads.

NOTE: When allocating vSwitch cores, consider optimizing the processing of packets to and from physical ports used for data interfaces. For more information, see *HCG 4.0 Cloud Administration: Ensuring Optimal vSwitch Processing of Physical Ports*.

Shared

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 *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Pinning a vCPU to a Shared Physical CPU*

To see how many cores a processor contains, hover over the Information icon.

Related Links

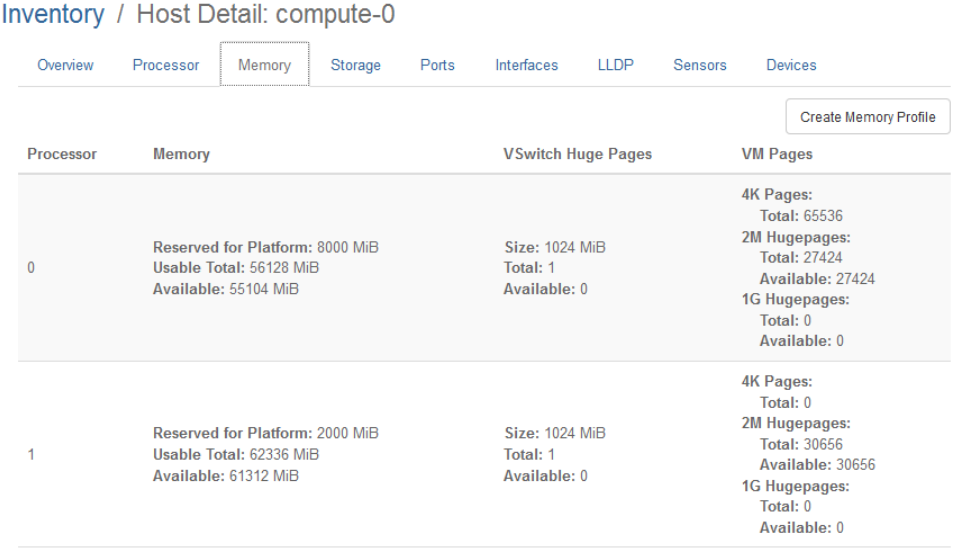
Viewing NUMA Node Resources on a Host on page 209
You can use the CLI to display the NUMA node resources for a host.

Designating Shared Physical CPUs on a Compute Host on page 110
You can designate one shared physical CPU per physical processor on a compute host to run low-load or non-real-time tasks for multiple VMs, freeing other cores on the host for dedicated high-load tasks.

Changing the Hyper-threading Status on page 112
The hyper-threading status is controlled by the BIOS settings of the host.

Memory Tab

The **Memory** tab on the Inventory Detail page displays host memory details.



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 of memory reserved for the platform (system software), and the usable total available for use by virtual machines. The usable total includes memory reserved for vSwitch huge pages.

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 Pages

This column is relevant on compute nodes only.

The size of the pages, and the total and available page figures. If changes to the huge page allocations are requested for a locked host, they are shown as **Pending**.

Related Links

Host Memory Provisioning on page 113
For each NUMA node on a host, you can adjust the amount of memory reserved for platform use, and the size and number of memory pages allocated for use by VMs.

Allocating Host Memory for VM Pages or Platform Use on page 114
You can edit the platform and VM page memory allocations for a NUMA node from the Web administration interface using the **Memory** tab on the Host Inventory pane.

Allocating Host Memory Using the CLI on page 116
You can edit the platform and huge page memory allocations for a NUMA node from the CLI.

Storage Tab

The **Storage** tab on the Inventory Detail page presents storage details for a host.

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.

Disks

UUID	Device	Type	Size (MiB)	RPM	Serial ID	Model
74946264-ff50-4d1d-acef-2b8bf8a65b8a	/dev/sda	HDD	476940	7200	S2V0T8LA	ST9500423AS

Displaying 1 item

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 (HDD or SSD).

Size

The capacity of the device in MiB.

RPM

The rotational speed of the device.

Serial ID

The device's serial ID number.

Model

The manufacturer's model for the device.

Cinder Device

This list is present for controller hosts on a system with controller storage. It lists the provisioning details for Cinder storage.


Cinder Device

UUID	Function	Disk UUID
ac1e5596-ad49-4fdd-8394-29902caac01e	cinder	bcf02b00-6f89-457e-a8cf-a1c8ae4843d2

Displaying 1 item

UUID

The unique identifier for the device.

Function

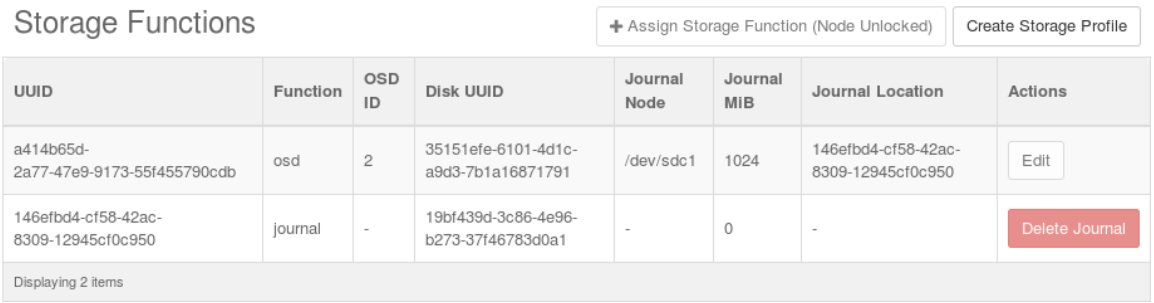
The service that the device supports (**cinder**).

Disk UUID

The unique identifier for the disk associated with the device.

Storage Functions

This list is presented for storage hosts. It shows a list of logical storage functions (OSDs and Ceph journal functions) defined on available disks.


Storage Functions

+ Assign Storage Function (Node Unlocked) | Create Storage Profile

UUID	Function	OSD ID	Disk UUID	Journal Node	Journal MiB	Journal Location	Actions
a414b65d-2a77-47e9-9173-55f455790cdb	osd	2	35151efe-6101-4d1c-a9d3-7b1a16871791	/dev/sdc1	1024	146efbd4-cf58-42ac-8309-12945cf0c950	Edit
146efbd4-cf58-42ac-8309-12945cf0c950	journal	-	19bf439d-3c86-4e96-b273-37f46783d0a1	-	0	-	Delete Journal

Displaying 2 items

For each volume, the following information is included:

UUID

The unique identifier for the storage volume.

Function

The type of function (**osd** for object storage, or **journal** for Ceph journal storage).

OSD ID

For an OSD function, the identity of the associated Ceph object storage daemon.

Disk UUID

The unique identifier for the disk associated with the storage volume.

Journal Node

For an OSD function, the device where the associated Ceph journal is maintained.

Journal MiB

For an OSD function, the size of the associated Ceph journal.

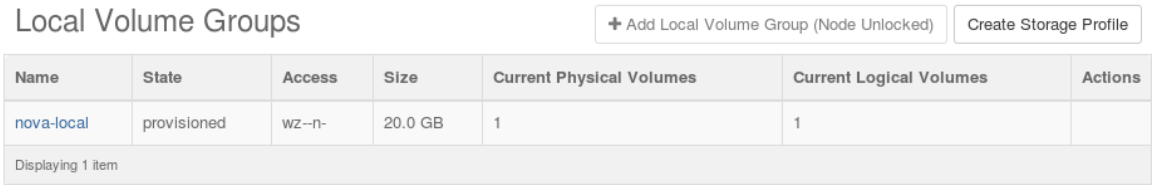
Journal Location

For an OSD function, the unique identifier for the associated journal function, if applicable.

For information about creating storage volumes, see Provisioning Storage on a Storage Host on page 138. For information about creating and applying storage profiles, see *HCG 4.0 Installation: Hardware Profiles*.

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 on page 133.



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 (**w**riteable, **r**eadonly, resi**z**eable, e**x**ported, **p**artial, or **c**lustered).

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 on a Compute Host on page 134.

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.

Related Links

Managing Physical Volumes on a Compute Host on page 134
You can add, delete, and review physical volumes on a compute host.

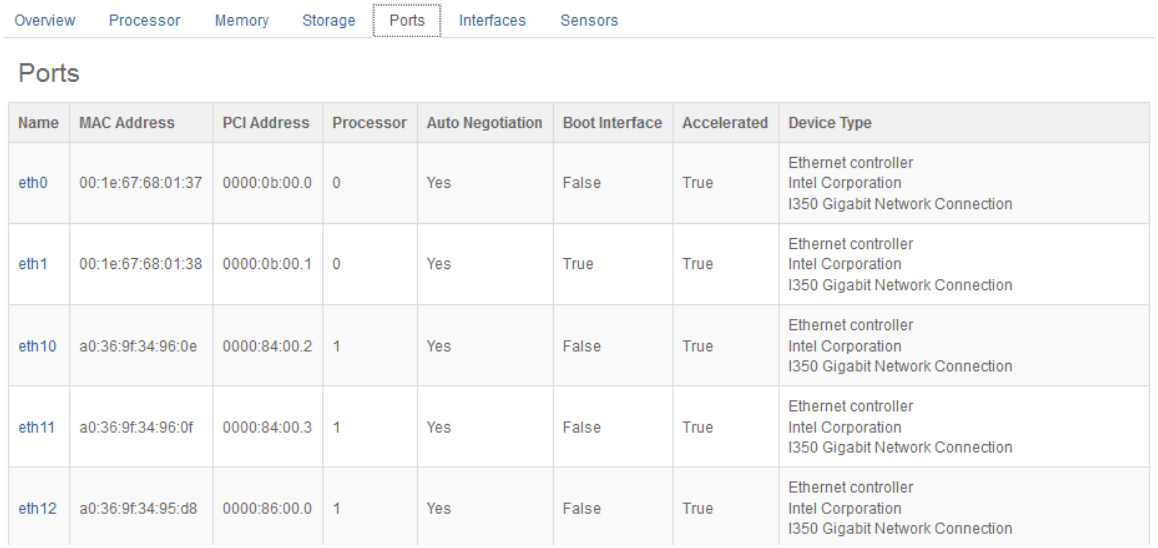
Local Volume Groups on page 132
Local volume groups are used to designate one or more physical volumes on a compute host as collective storage space.

Managing Local Volume Groups on page 133
You can add, delete, and review local volume groups on a compute host.

Managing Local Volume Groups Using the CLI on page 134
You can use CLI commands to manage local volume groups.

Ports Tab

The **Ports** tab on the Inventory Detail page presents information about the physical ports on a host.



Currently none of the port attributes is configurable; they are all read directly from the hardware. 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 I/O 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.

Accelerated

The acceleration status. If the port is supported by AVS using DPDK poll-mode drivers, acceleration is used. Otherwise, the port operates in non-accelerated mode with AVS leveraging the kernel drivers.

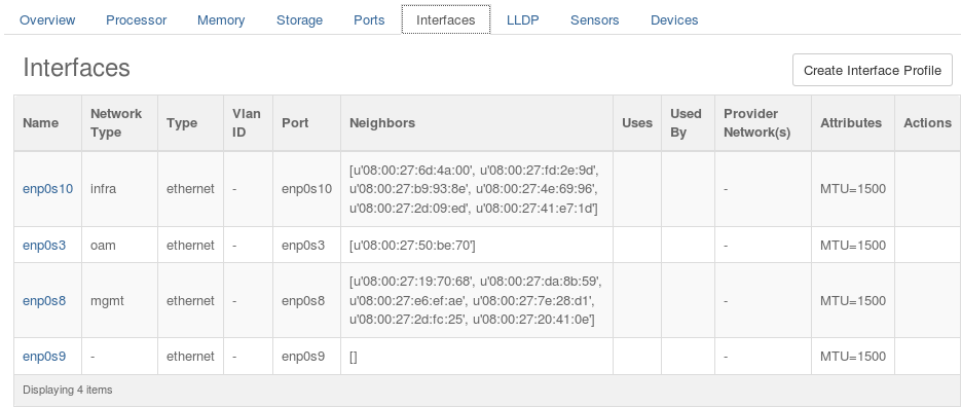
Device Type

Hardware information about the port type, manufacturer, and model.

Interfaces Tab

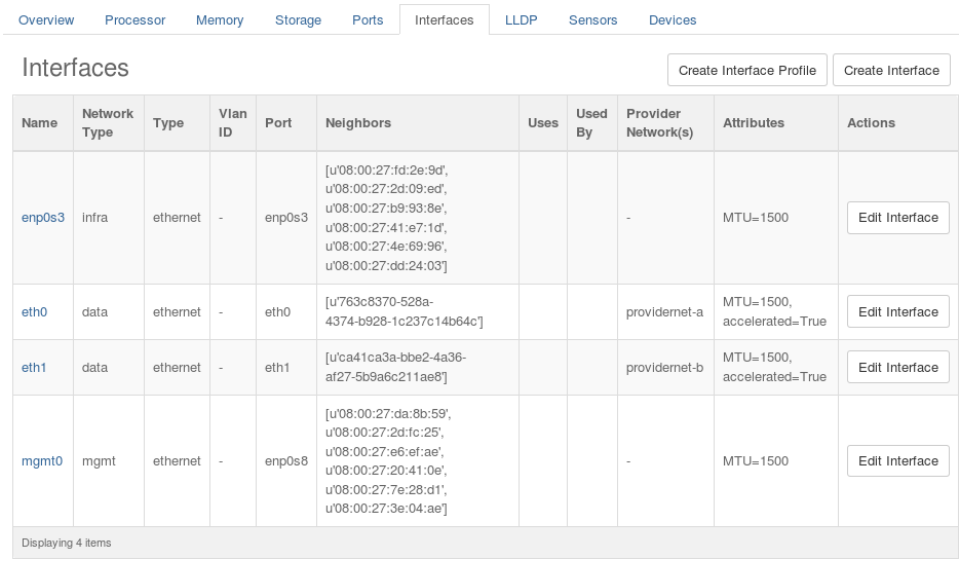
The **Interfaces** tab on the Inventory Detail page presents details about the logical L2 network interfaces on a node.

The following example is for an unlocked controller node:



In this example, the node has three allocated interfaces. The interfaces **enp0s3**, connecting to the OAM network, and **enp0s8** connecting to the internal management network, reflect the allocation given when the node was provisioned.

On a configured compute node, the **Interfaces** tab presents additional logical interfaces. The following example is for a locked node:



In this example, the node has four allocated interfaces: **enp0s3** connecting to the infrastructure network, **mgmt0** connecting to the internal management network, and **eth0** and **eth1** connecting to the provider networks **providernet-a** and **providernet-b**, respectively. The interface **mgmt0** is auto-provisioned as part of the automated software installation process on the compute node. It can be modified but not deleted.

NOTE: For data interfaces, you can optimize vSwitch processing of packets to and from physical ports by using only ports that are connected to processors with vSwitch cores. For more information, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Ensuring Optimal vSwitch Processing of Physical Ports*.

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 *HCG 4.0 Planning: 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 *HCG 4.0 Planning: 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

Details including the current MTU size for the interface and whether the interface is DPDK-accelerated.

Actions

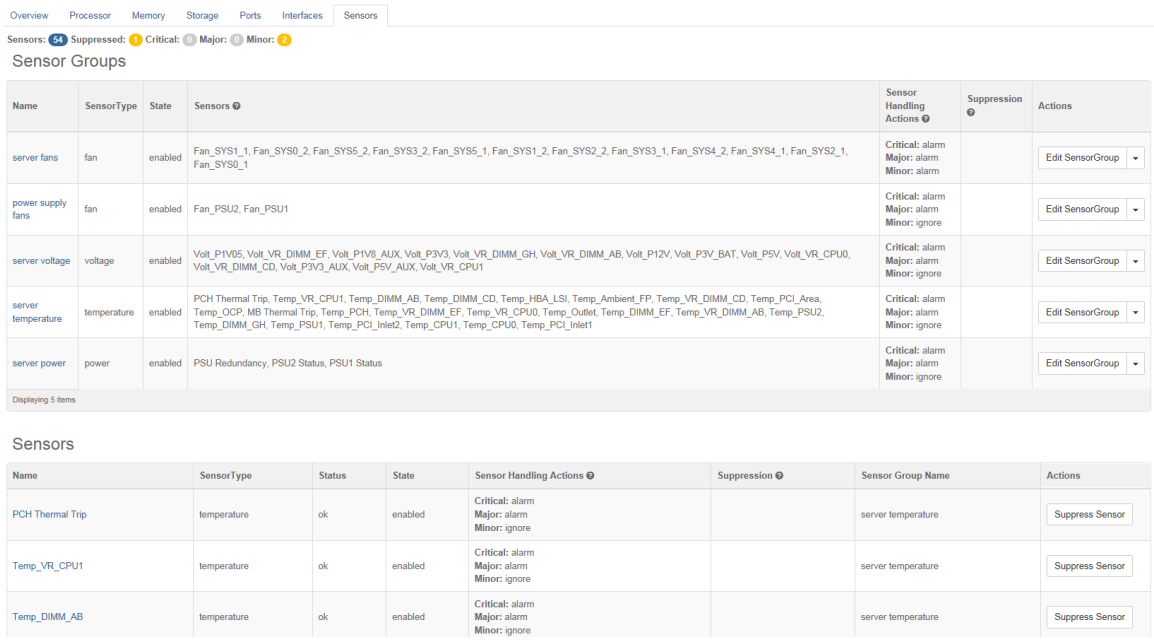
On a locked node, you can modify a logical interface, and execute management operations on it. This is implemented using the **Edit Interface** and **More** buttons. These buttons are not available when the node is unlocked.

Sensors Tab

The **Sensors** tab on the Inventory Detail page presents details for sensors used to monitor host hardware health.

If an optional board management control (BMC) module is present on the host and configured for the host in the HCG 4.0 inventory, and sensor support is implemented for the BMC type in HCG 4.0, this tab lists the available sensors and shows their status. It also lists *sensor groups* that have been defined for the sensors.

NOTE: Currrently, sensor support is implemented for Quanta BMCs. For more about BMC modules, see *HCG 4.0 Planning: Board Management Network Planning*.



Sensor Status

Each of the individual sensors in the Sensors list can report the following status conditions:

- OK
- Minor
- Major
- Critical

The status of each sensor is audited periodically to refresh the system monitoring data. You can configure the refresh period, or *audit interval*, for sensor groups.

Actions

You can configure different actions for each status level using sensor groups. The configured action applies to all sensors in the sensor group. The following actions are supported:

alarm

This generates a HCG 4.0 alarm with a severity level corresponding to the sensor status level. For more about HCG 4.0 alarms, see Fault Management on page 211.

For the status levels Major and Critical, it also sets the Availability State of the host to Degraded. For more about availability states, see Host Inventory on page 52.

ignore

The status is reported in the Sensor list, but no action is taken.

power cycle

This action applies to critical faults only.

If this action is selected for a group that has a sensor reporting a critical fault, then the Hardware Monitor Service sends a **power cycle** notification to the Maintenance Service for action handling. While the fault remains, the Maintenance Service powers-down the host,

then waits for a five minute cool down period, and then powers it up. When it comes online, it waits for another five minute recovery period. If a critical fault still exists, then the cycle is repeated, up to three times. If the fault goes away, the host recovers in its current admin state. (An extra reboot may be required if this fault is detected while the host is unlocked.) If after three tries the fault still remains, then the server is powered down and left that way, requiring manual action to recover. If the server was locked, its state shows as **locked-disabled-power-off** and requires a **power-on** action followed by an **unlock** action to enable the server. If the server was unlocked, its state shows as **unlocked-disabled-power-off** and requires a **lock** and then a **power-on** to manually power the server back on. When the server's availability status shows "online", it can be **unlocked** to enable again.

reset

This action applies to critical faults only.

If this action is selected for a group that has a sensor reporting a critical fault, then the Hardware Monitor Service sends a reset notification to the Maintenance Service for action handling. If the server is locked, then the Maintenance Service forces a reset of the server. If the server is unlocked, then the Maintenance Service fails the server and runs the full enable FSM in an attempt to recover it to the **ENABLED** state. In both cases, there is a 10 minute wait period before another reset/enable is issued if the Hardware Monitor Service continues to report the fault. This hold-off period gives the host time to boot and re-enable. If the fault persists, so does this behavior. If the fault goes away, then the host recovers in its current admin state.

log

When the log action is selected for any severity level, the Hardware Monitor Service generates a severity-specific customer log instead of an alarm. Configuration change logs are also generated for action, audit interval, and sensor suppression state changes.

You can suppress the configured action for individual sensors or groups of sensors. Suppressed sensors are still audited, and their status is reported in the Sensors list. For more information, see Suppressing Sensor Actions on page 120.

Sensor Groups

Sensors that perform the same type of monitoring are collected into Sensor Groups. You can configure audit intervals and alarm actions for each group. The configured values apply to all sensors in the group. For more information, see Adjusting Sensor Actions and Audit Intervals on page 119.

The available Sensor Groups and their membership are predefined in HCG 4.0.

server fans

Sensors that monitor the speed and health of CPU cooling fans.

power supply fans

Sensors that monitor the speed and health of power supply cooling fans.

server voltage

Sensors that monitor DC voltage levels supplied to components.

server temperature

Sensors that monitor component or ambient temperatures.

server power

Sensors that monitor the operational status of power supplies.

Related Links

Adjusting Sensor Actions and Audit Intervals on page 119
You can configure audit intervals and actions for groups of sensors.

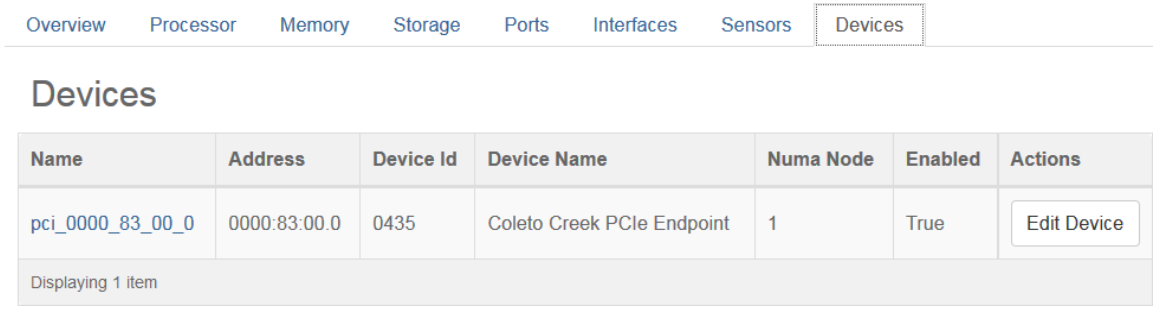
Suppressing Sensor Actions on page 120
You can suppress the configured **Action** for individual sensors or groups of sensors

CLI Commands for Managing Sensors on page 121
You can use the command-line interface to list sensor information and change sensor settings.

Devices Tab

The **Devices** tab on the Inventory Detail page presents details for non-NIC PCI devices that can be made available for use by VMs.

All non-NIC PCI devices that can be exposed to a guest are listed. They are automatically detected by the system, and cannot be manually added or deleted.



NOTE: PCI passthrough and SR-IOV Ethernet interfaces are listed separately. For more information, see Displaying Provider Network Information on page 21.

The following information is presented:

Name

The name of the device, as identified by the system inventory.

Address

The PCI address of the device.

Device Id

The ID of the device, assigned by the vendor.

Device Name

The name of the device, as identified by the host's Linux kernel.

Numa Node

The NUMA node of the device.

Enabled

Whether exposure to VMs is enabled for the device.

To view usage information for individual devices, see Viewing Resource Usage for a Device on page 207. To specify whether a device is exposed to VMs, see Exposing a Device for Use by VMs on page 112.

For a list of devices supported by HCG 4.0, refer to the Release Notes.

CLI Commands for Managing Devices

The following commands are available for managing PCI devices on a host:

- **system host-device-list**

  Lists the devices for a host.

- **system host-device-show**

  Lists the device at a specific PCI address on a host.

- **system host-device-modify**

  Provides for exposing a device to VMs.

For example:

```
~(keystone_admin)$ system host-device-list compute-0
~(keystone_admin)$ system host-device-show compute-0 0000:09:00.0
~(keystone_admin)$ system host-device-modify --name="Encryption1" --enable=True
compute-0
```

Related Links

Viewing Resource Usage for a Device on page 207
You can view PCI device usage from the web administration interface or the CLI.

Exposing a Device for Use by VMs on page 112
You can expose PCI passthrough or SR-IOV devices so that they are accessible for use by VMs.

Viewing Resource Usage for a Device Using the CLI

You can view PCI device usage from the the CLI.

View device information using the following CLI commands:

```
~(keystone_admin)$ nova device-list

+---------------------------------+-----------+-----------+...
| Device Name                     | Device Id | Vendor Id |...
+---------------------------------+-----------+-----------+...
+ Coleto Creek PCIe Co-processor + 0443      + 8086      +...
+---------------------------------+-----------+-----------+...

...--------------------+-------------+--------------------+--------------+
... pci_pfs_configured | pci_pfs_used | pci_vfs_configured | pci_vfs_used |
...--------------------+-------------+--------------------+--------------+
... 0                  + 0           + 64                 + 1            +
...--------------------+-------------+--------------------+--------------+


~(keystone_admin)$ nova device-show 0443
+---------------------------------+-----------+-----------+-----------+...
| Device Name                     | Device Id | Vendor Id | Host      |...
+---------------------------------+-----------+-----------+-----------+...
| Coleto Creek PCIe Co-processor | 0443      | 8086      | compute-0 |...
| Coleto Creek PCIe Co-processor | 0443      | 8086      | compute-1 |...
+---------------------------------+-----------+-----------+-----------+...

...--------------------+-------------+--------------------+--------------+
```

```
... pci_pfs_configured | pci_pfs_used | pci_vfs_configured | pci_vfs_used |
...--------------------+--------------+--------------------+--------------+
... 0                  | 0            | 32                 | 0            |
... 0                  | 0            | 32                 | 1            |
...--------------------+--------------+--------------------+--------------+
```

where

Device Name

is the name of the device, as listed in the system inventory

Device Id

is the ID of the device

Vendor Id

is the vendor ID of the device

Host

is the node hosting the device

pci_pfs_configured

is the number of PCI passthrough devices

pci_pfs_used

is the number of PCI passthrough devices allocated to instances

pci_vfs_configured

is the number of SR-IOV devices

pci_vfs_used

is the number of SR-IOV interfaces allocated to instances

Network Interface Provisioning

Before you can unlock and use the compute or storage nodes, you must configure the interfaces to attach them to networks.

Some interfaces require manual provisioning before the nodes can be unlocked.

- For the second controller node, you must attach an interface to the OAM network, and to the infrastructure network if used, before you can unlock the node.
- For a storage node, you must attach an interface to the infrastructure network before you can unlock the node.
- For a compute node, you must attach interfaces to provider networks before you can unlock the node. The provider networks must be set up beforehand; for more information, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Configuring Provider Networks on page 25* . If the compute cluster uses an infrastructure network, you must attach an interface to the infrastructure network before you can unlock the node. In addition, if the infrastructure uses static addressing, you must assign an IP address to the interface using the **system host-addr-add** command.

HCG 4.0 supports three types of interfaces:

Ethernet interfaces

These are created automatically for each port on the host. You must configure Ethernet interfaces by specifying the network type.

aggregated Ethernet interfaces

For link protection, you can create an aggregated Ethernet interface with two or more ports, and configure it with the network type.

VLAN interfaces

To support multiple interfaces on the same physical Ethernet or aggregated Ethernet interface, you can create VLAN interfaces and configure them with the network type.

The procedure for attaching an interface depends on the interface type.

- To attach an Ethernet interface, see Configuring Ethernet Interfaces on page 85.
- To attach an aggregated Ethernet interface, see Configuring Aggregated Ethernet Interfaces on page 89.
- To attach a VLAN interface, see Configuring VLAN Interfaces on page 94.

NOTE: To attach a data network to an existing management or infrastructure network interface, see Editing Interface Settings on page 81.

As an alternative, you can use the CLI to attach interfaces. See Network Interface Provisioning Using the CLI on page 76.

Logical interfaces of network types **oam** and **mgmt** cannot be deleted. They can only be modified to use different physical ports when required.

For more information on interfaces, see *HCG 4.0 Planning: Ethernet Interfaces*.

NOTE: On compute and storage nodes, the Ethernet interface for the internal management network is attached automatically, to support installation using PXE booting. On controller nodes, the interface for the internal management network is attached according to the settings specified during the controller configuration script. For more information, see *HCG 4.0 Installation: The Controller Configuration Script*.

Network Interface Provisioning Using the CLI

You can use CLI commands to create and attach network interfaces.

For more information about interface provisioning, or help using the Web administration interface, see Network Interface Provisioning on page 75.

To list attached interfaces, use the **system host-if-list** command.

```
~(keystone_admin)$ system host-if-list controller-0
...+--------+------...+----------+---------+-------------+------------+-------------
+...
...| name   | netwo...| type     | vlan id | ports       | uses i/f   | used by i/f
|...
...+--------+------...+----------+---------+-------------+------------+-------------
+...
...| infra0 | infra...| vlan     | 22      | []          | [u'mgmt0'] | []
|...
...| oam0   | oam  ...| ethernet | None    | [u'enp0s3'] | []         | []
```

```
|...
...| mgmt0  | mgmt ...| ethernet | None    | [u'enp0s8'] | []         | [u'infra0']
|...
...+--------+------...+----------+---------+-------------+------------+-------------
+...
```

To see all available interfaces, add the **-a** flag.

```
~(keystone_admin)$ system host-if-list -a controller-0
...+--------+------...+----------+---------+--------------+------------+-------------
+...
...| name   | netwo...| type     | vlan id | ports        | uses i/f   | used by i/f
|...
...+--------+------...+----------+---------+--------------+------------+-------------
+...
...| eth3   | None ...| ethernet | None    | [u'enp0s10'] | []         | []
|...
...| infra0 | infra...| vlan     | 22      | []           | [u'mgmt0'] | []
|...
...| eth2   | None ...| ethernet | None    | [u'enp0s9']  | []         | []
|...
...| oam0   | oam  ...| ethernet | None    | [u'enp0s3']  | []         | []
|...
...| mgmt0  | mgmt ...| ethernet | None    | [u'enp0s8']  | []         | [u'infra0']
|...
...+--------+------...+----------+---------+--------------+------------+-------------
+...
```

To assign an IP address to an interface, use the **system host-addr-add** command. This is required for the management and infrastructure networks if static IP address assignment is in use.

```
~(keystone_admin)$ system host-addr-add node ifname ip_address prefix
```

where

node

is the name or UUID of the compute node

ifname

is the name of the interface

ip_address

is an IPv4 or IPv6 address

prefix

is the netmask length for the address

Combined Data and Management or Infrastructure Interfaces

You can add a data interface to a management or infrastructure interface using a command of the following form:

```
~(keystone_admin)$ system host-if-modify –nt “mgmt,data” –p group0-data0 compute-0
mgmt0
```

This example adds a data network to the **mgmt0** interface on **compute-0**, for the provider network **group0-data0**.

Interface Settings

The settings for creating or editing an interface on a node depend on the type of network to which the interface is connected (for example, **infra** or **data**), as well as the type of interface (for example, **aggregated ethernet** or **vlan**).

These settings are available on the **Edit Interface** and **Create Interface** dialog boxes for a host, accessible from the **Interfaces** tab of the Host Inventory page.

For more about creating and editing interfaces, see Network Interface Provisioning on page 75.

Interface Name

A name used to identify the interface.

Network Type

The type of network to which the interface is attached.

NOTE: This selection supports multiple network types on the same *logical* interface. HCG 4.0 also supports multiple network types on the same *physical* interface, using VLAN interfaces.

You can select multiple checkboxes, but the only valid multiple selection is **data** in addition to either **mgmt** or **infra** on the interface connected to the management or infrastructure network.

Depending on the interface, the checkbox options can include:

none

Clears the Network Type setting.

infra

Attaches the interface to an infrastructure network.

When a compute or storage node is added to HCG 4.0, an interface must be attached to the infrastructure network before the node can be unlocked.

You can edit the infrastructure interface to add a **data** network and provider network. This allows both infrastructure and data traffic to be carried on the interface.

oam

Attaches the interface to the OAM network.

The OAM network is used by controller nodes for administrator remote access. It is not applicable to compute or storage nodes.

mgmt

Attaches the interface to the internal management network.

When a compute or storage node is added to HCG 4.0, the interface used for PXE boot is assigned automatically to the internal management network. In the settings for this interface, **mgmt** is already selected. For other interfaces, this selection is not used.

You can edit the management interface to add a **data** network and provider network. This allows both management and data traffic to be carried on the interface.

pci-passthrough

Provides for a direct connection to physical interface hardware and the attached provider network from a virtual machine. A single VM can directly access the physical interface. For more information, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Configuring PCI Passthrough Ethernet Interfaces*.

data

Attaches the interface to a provider network.

You can add a data interface to a management or infrastructure interface by editing the interface and selecting **data** in addition to **mgmt** or **infra**.

pci-sriov

Provides for a direct connection to a virtual unit of physical interface hardware, and the attached provider network, from a virtual machine. Multiple VMs can directly access and share the same physical interface. For more information, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Configuring SR-IOV Ethernet Interfaces*.

Interface Type

(Shown only when the **Network Type** is set to **mgmt**, **oam**, **data**, or **infra**) The type of interface (Ethernet, aggregated Ethernet, or VLAN).

Aggregated Ethernet - Mode

(Shown only when the **Interface Type** is set to **aggregated ethernet**) The operational mode for link aggregation.

Aggregated Ethernet - Tx Policy

(Shown only when the **Aggregated Ethernet - Mode** is set to **balanced** or **802.3ad**) The transmit policy for link aggregation.

Vlan ID

(Shown only when the **Interface Type** is set to **vlan**) A unique VLAN identifier for the network.

Port(s)

The physical port or ports used for the interface.

Provider Networks

(Shown only when the Network Type is set to **data**, **pci-passthrough**, or **pci-sriov**) The available provider networks. To attach the interface to a provider network, select the provider network.

NOTE: You cannot attach to a VLAN provider network using a VLAN data interface.

MTU

The maximum transmission unit for the interface. For more information, see *HCG 4.0 Planning: The Ethernet MTU*.

NOTE: You cannot change the MTU for an infrastructure interface. The value from the network resource is always used.

IPv4 Addressing Mode

(Shown only when the **Network Type** is set to **data**) The method for assigning an IP address to the interface for use with VXLAN networks. For more information about VXLAN networks, see *Helion OpenStack Carrier Grade 4.0 System Administration: Using VXLANs on page 34*.

Disabled

Do not assign an IPv4 address.

Static

Use a static IPv4 address.

Pool

Use an address from a pool of IPv4 addresses that has been defined and associated with the data interface.

IPv4 Address Pool

(Shown only when the **IPv4 Addressing Mode** is set to **pool**) The pool from which to assign an IPv4 address.

IPv6 Addressing Mode

(Shown only when the **Network Type** is set to **data**) The method for assigning an IP address to the interface for use with VXLAN networks. For more information about VXLAN networks, see *Helion OpenStack Carrier Grade 4.0 System Administration: Using VXLANs on page 34*.

Disabled

Do not assign an IPv6 address.

Static

Use a static IPv6 address.

Pool

Use an address from a pool of IPv6 addresses that has been defined and associated with the data interface.

Automatic Assignment

Use an automatically assigned IPv6 address.

Link Local

Use a link local IPv6 address.

IPv6 Address Pool

(Shown only when the **IPv6 Addressing Mode** is set to **pool**) The pool from which to assign an IPv6 address.

Virtual Functions

(Shown only when the Network Type is set to **pci-sriov**) The number of virtual interfaces to use. For more information, see *Helion OpenStack Carrier Grade 4.0Cloud Administration: Configuring SR-IOV Ethernet Interfaces*.

Maximum Virtual Functions

(Shown only when the Network Type is set to **pci-sriov**)

the maximum number of virtual interfaces available.

For more information about adding provider networks, see *Helion OpenStack Carrier Grade 4.0 System Administration: Configuring Provider Networks on page 25*.

For more information about link aggregation, see *Link Aggregation Settings on page 92*.

For more information about IP address pools, see *Helion OpenStack Carrier Grade 4.0 System Administration: Using IP Address Pools for Data Interfaces on page 42*.

Editing Interface Settings

You can change the settings for a host interface.

The ability to change the interface settings is especially useful for updating the management interface. When a compute node is first created, its internal management interface is automatically set up using the default **Interface Type** (**ethernet**). If you are using LAG on the internal management network, you must update this manually to **aggregated ethernet**.

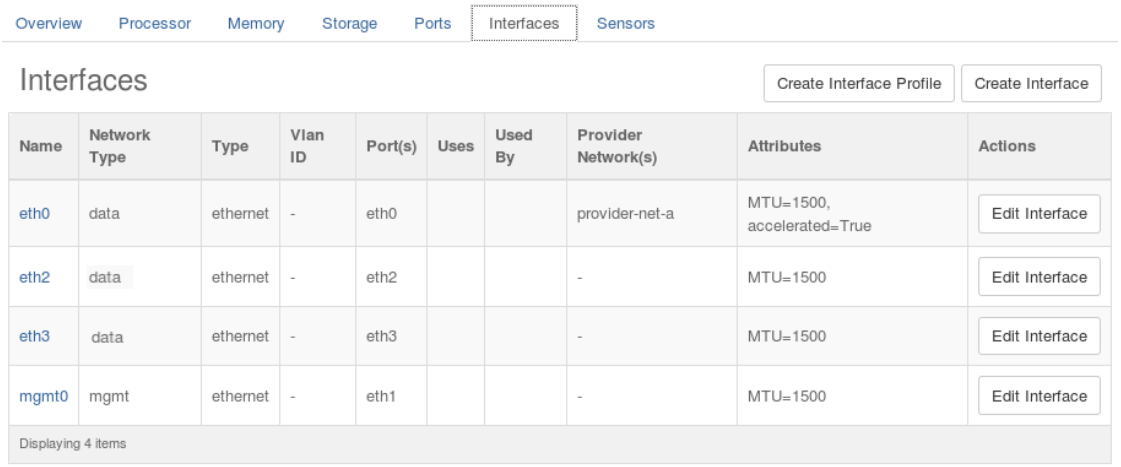
You can also edit an internal management or infrastructure interface to attach to a data network by selecting **data** as an additional Network Type for the interface, or using the CLI. For CLI instructions, see Network Interface Provisioning Using the CLI on page 76.

To add or edit IP addresses on a data interface, see *Helion OpenStack Carrier Grade 4.0 System Administration: Adding a Static IP Address to a Data Interface on page 38*.

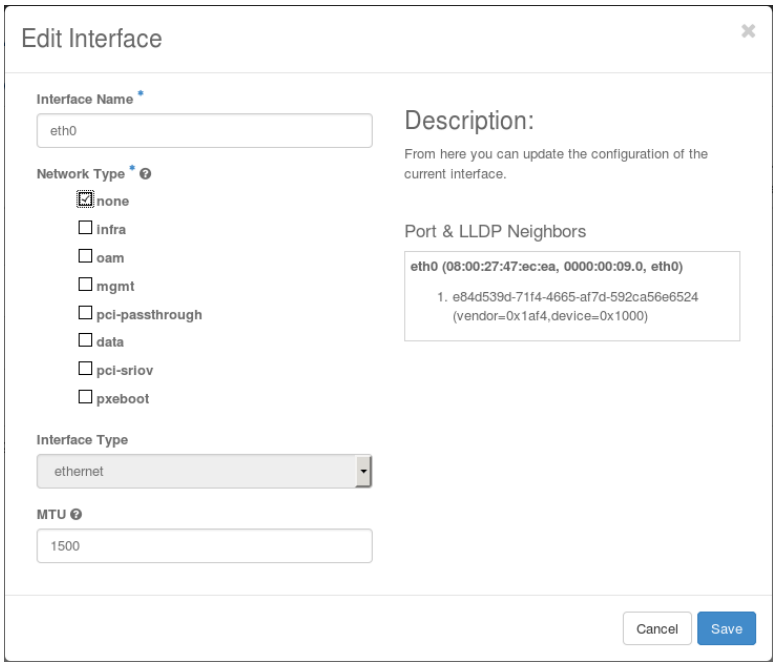
Procedure

1. Lock the host to make changes.
   a) On the **Admin** menu of the Web administration interface, in the **System** section, select **Inventory**.
   b) Select the **Hosts** tab.
   c) In the **Actions** column, open the drop-down list for the host, and then select **Lock Host**.
   d) Wait for the host to be reported as **Locked**.
2. Open the **Inventory Detail** page for the locked host.

   In the **Host Name** column, click the name of the host.
3. Select the **Interfaces** tab to display the existing interfaces.



4. Click **Edit Interface** for the interface you want to change.



5. Make the required changes, and then click **Save**.

The settings shown depend on the interface type. For information about the available settings, see Interface Settings on page 78.

6. Unlock the host.

Related Links

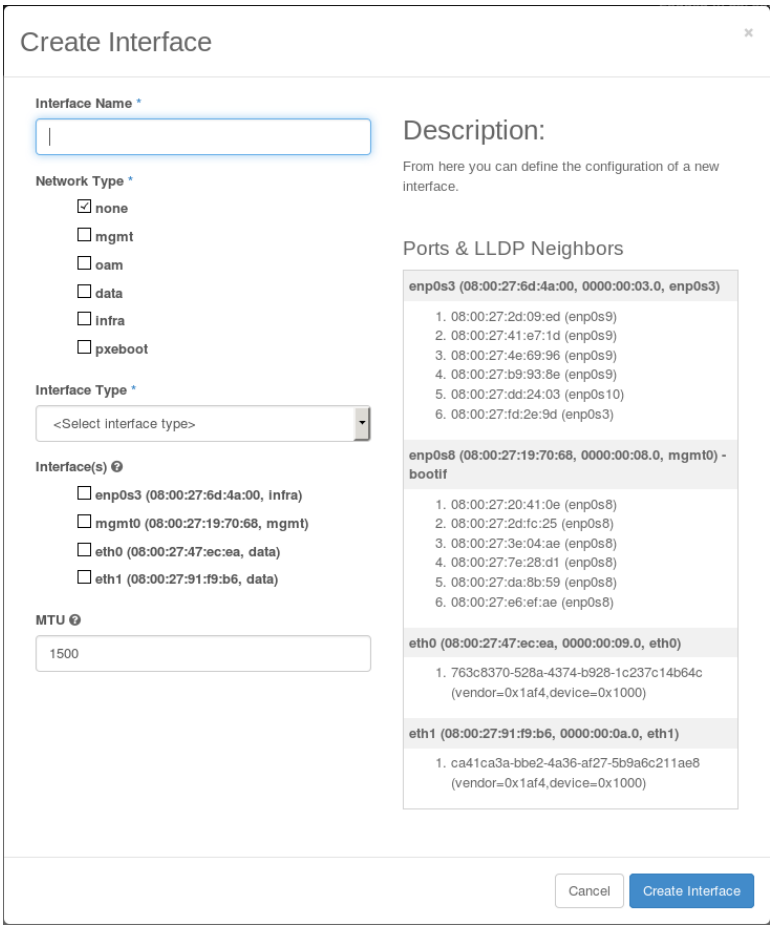
Ports Tab on page 67
The **Ports** tab on the Inventory Detail page presents information about the physical ports on a host.

Interfaces Tab on page 68
The **Interfaces** tab on the Inventory Detail page presents details about the logical L2 network interfaces on a node.

Creating Interfaces

You can create new logical interfaces using the **Create Interface** button on the **Interfaces** tab.

This button is available only on nodes in the locked state. When the button is clicked, the Create Interface dialog box is displayed, as illustrated below.



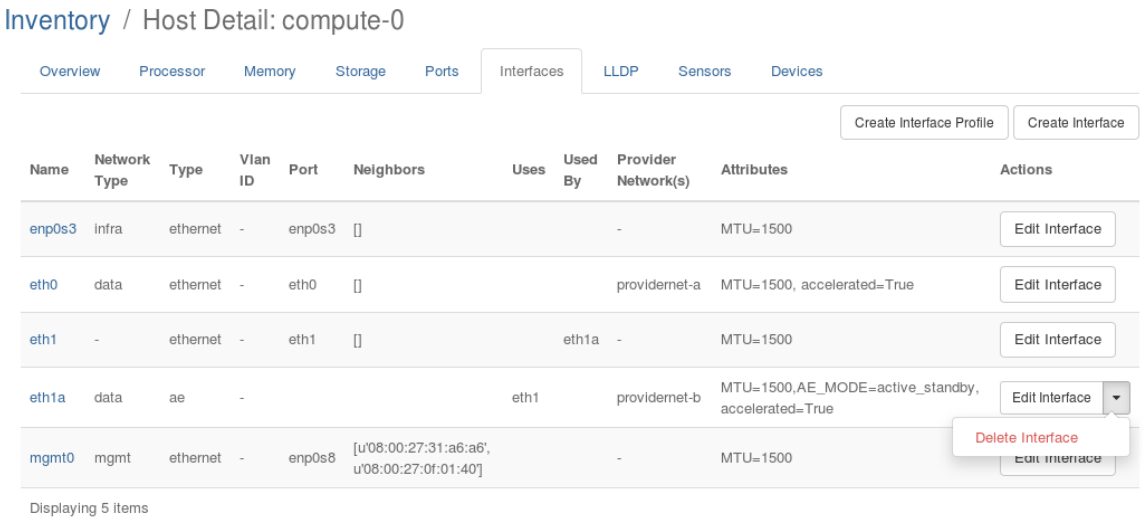
Different fields are displayed depending on the interface type selected. For more information, see Interface Settings on page 78.

Deleting Interfaces

You can delete an interface using the Web administration interface or the CLI.

NOTE: You cannot delete an interface of type **Ethernet**. You can only designate it as unused by setting its network type to **none**.

From the Web administration interface, you can delete an interface from the **Interface** tab of the Host Inventory page.



From the CLI, you can use the **system host-if-delete** command.

```
~(keystone_admin)system host-if-delete host interface
```

where

host

is the hostname or ID of the host

interface

is the name or UUID of the interface

For example, to delete an aggregated Ethernet interface named **eth1a** on **compute-0**:

```
~(keystone_admin)$ system host-if-delete compute-0 eth1a
Deleted interface: host compute-0 if eth1a
```

Marking an Ethernet Interface as Unused

You cannot delete an Ethernet interface. You can mark an Ethernet interface as unused by setting the interface type to **none** from the Web administration interface, or from the CLI using the **system host-if-modify** command.

For example, to designate the **eth1** Ethernet interface on **compute-0** as unused:

```
~(keystone_admin)$ system host-if-modify -nt none compute-0 eth1
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| ifname           | eth1                                 |
| networktype      | None                                 |
| iftype           | ethernet                             |
| ports            | [u'eth1']                            |
| providernetworks | None                                 |
| imac             | 08:00:27:91:f9:b6                    |
| imtu             | 1500                                 |
| aemode           | None                                 |
| schedpolicy      | None                                 |
| txhashpolicy     | None                                 |
| uuid             | 87dd1d4b-1e38-4f6c-a692-4c4199a3ef0e |
| ihost_uuid       | 3b659824-eac3-4446-af73-f4a519e8ab30 |
| vlan_id          | None                                 |
| uses             | []                                   |
| used_by          | []                                   |
| created_at       | 2016-09-22T18:24:08.092296+00:00     |
| updated_at       | 2016-09-22T18:36:46.333354+00:00     |
| sriov_numvfs     | 0                                    |
| ipv4_mode        | None                                 |
| ipv6_mode        | None                                 |
| accelerated      | [u'True']                            |
+------------------+--------------------------------------+
```

Configuring Ethernet Interfaces

You can attach an Ethernet interface to a network by editing the interface.

When a compute or storage node is added to HCG 4.0 and initialized, Ethernet interfaces are created automatically for each physical port detected. To support installation using PXE booting, one interface is attached automatically to the internal management network. You must attach additional interfaces manually before you can unlock the node. For more about this requirement, see Network Interface Provisioning on page 75.

For a network that uses Ethernet interfaces, you can edit an existing Ethernet interface on the node to attach it, as described in this topic. You can also do this from the CLI; for more information, see Network Interface Provisioning Using the CLI on page 76.

For a network that uses aggregated Ethernet or VLAN interfaces, you must create an interface in order to attach it; see Configuring Aggregated Ethernet Interfaces on page 89 or Configuring VLAN Interfaces on page 94.

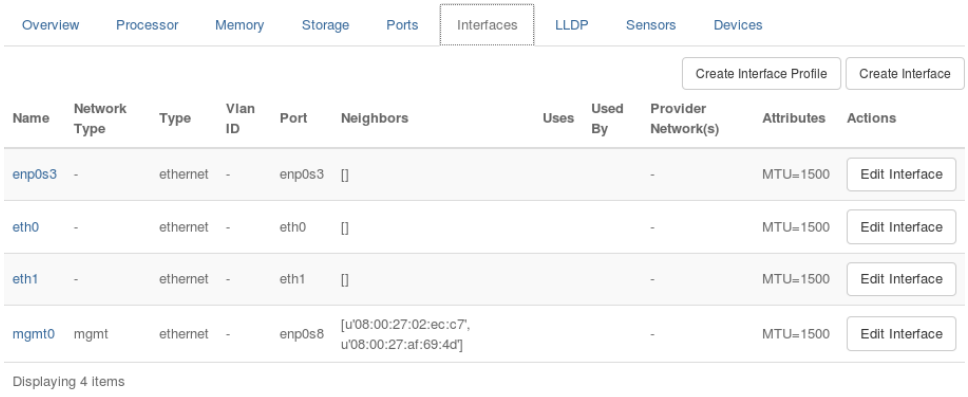
Procedure

1. Open the **Inventory Detail** page for the host.

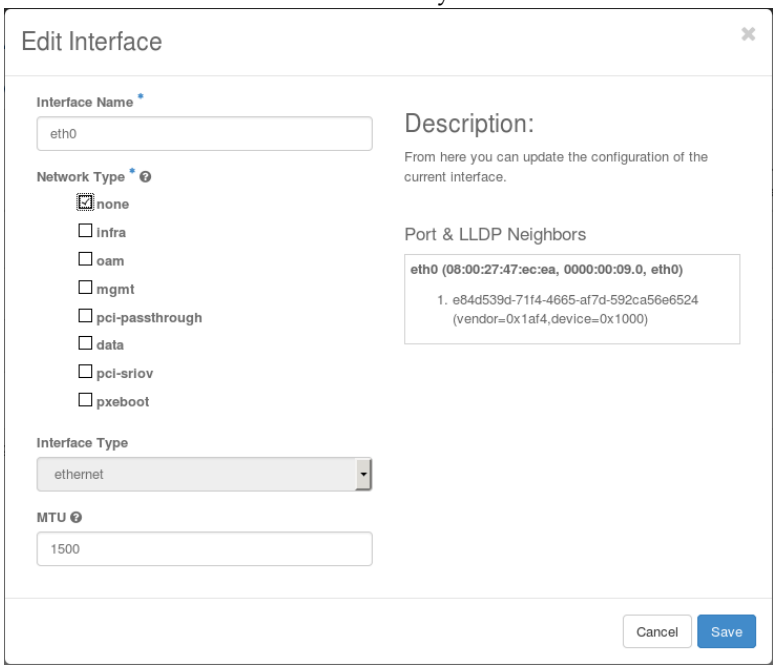
a) Open the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane.

b) Select the **Hosts** tab, and then in the **Host Name** column, click the name of the host.

2. Select the **Interfaces** tab.



3. Click **Edit Interface** for the interface you want to attach to a network.



For an Ethernet interface, the **Port** is already selected.

4. Select the type of network for the interface.

For details, see Interface Settings on page 78.

5. Complete the required information for the type of interface.

For more information, see Interface Settings on page 78.

6. Click **Save** to save your changes and close the dialog box.

NOTE:

If an interface is not supported by AVS using DPDK poll-mode drivers, it will operate in non-accelerated mode leveraging kernel drivers.

The interface is attached to the network.

Configuring Ethernet Interfaces Using the CLI

You can use the CLI to attach Ethernet interfaces to networks.

Ethernet interfaces are created automatically. To attach one to a network, use a command of the following form:

```
~(keystone_admin)$ system host-if-modify -n ifname -m mtu \
-nt networktype hostname ethname [-p providernetworklist] \
[--ipv4-mode=ip4_mode [ipv4-pool addr_pool]] [--ipv6-mode=ip6_mode [ipv6-pool
addr_pool]]
```

where

ifname

is a name for the interface

mtu

is the MTU for the interface

networktype

is the type of network to attach to

hostname

is the name or UUID of the host

ethname

is the name or UUID of the Ethernet interface to use

providernetworklist

is a list of provider networks, delimited by quotes and separated by spaces; for example, "provider-net-a provider-net-b". To specify a single provider network, omit the quotes. This parameter is required only if the *networktype* is set to **data**.

ip4_mode

is the mode for assigning IPv4 addresses to a data interface (**static** or **pool**), for use with VXLANs

ip6_mode

is the mode for assigning IPv6 addresses to a data interface (**static** or **pool**), for use with VXLANs

addr_pool

is the name of an IPv4 or IPv6 address pool, for use with the **pool** mode of IP address assignment for data interfaces used with VXLANs

For valid values, see Interface Settings on page 78.

For example, to attach an interface named **enp0s3** to the OAM network, using Ethernet interface **enp0s3** on **controller-1**:

```
~(keystone_admin)$ system host-if-modify -n enp0s3 \
-nt oam controller-1 enp0s3
+------------------+----------------------------------------+
| Property         | Value                                  |
+------------------+----------------------------------------+
| ifname           | enp0s3                                 |
| networktype      | oam                                    |
| iftype           | ethernet                               |
| ports            | [u'enp0s3']                            |
| providernetworks | None                                   |
| imac             | 08:00:27:58:0c:e5                      |
| imtu             | 1500                                   |
| aemode           | None                                   |
| schedpolicy      | None                                   |
| txhashpolicy     | None                                   |
| uuid             | 14300770-13bf-48fd-b9af-756ec7d8adc1   |
| ihost_uuid       | e1c47086-3230-4b92-91d0-208c55130a52   |
| vlan_id          | None                                   |
| uses             | []                                     |
| used_by          | []                                     |
| created_at       | 2015-12-10T14:24:25.967362+00:00       |
| updated_at       | 2015-12-10T17:01:08.761323+00:00       |
| sriov_numvfs     | 0                                      |
| accelerated      | [u'True']                              |
+------------------+----------------------------------------+
```

To attach an interface named **enp0s9** to a VLAN provider network named **providernet-a**, using Ethernet interface **enp0s9** on **compute-0**:

```
~(keystone_admin)$ system host-if-modify -n enp0s9 \
-nt data compute-0 enp0s9 -p providernet-a
+------------------+----------------------------------------+
| Property         | Value                                  |
+------------------+----------------------------------------+
| ifname           | enp0s9                                 |
| networktype      | data                                   |
| iftype           | ethernet                               |
| ports            | [u'enp0s9']                            |
| providernetworks | providernet-a                          |
| imac             | 08:00:27:66:38:c6                      |
| imtu             | 1500                                   |
| aemode           | None                                   |
| schedpolicy      | None                                   |
| txhashpolicy     | None                                   |
| uuid             | 4ff97cc5-8e59-4763-9a85-c4be3996ddbe   |
| ihost_uuid       | 327b2136-ffb6-4cd5-8fed-d2ec545302aa   |
| vlan_id          | None                                   |
| uses             | []                                     |
| used_by          | []                                     |
| created_at       | 2015-12-23T13:04:49.768322+00:00       |
| updated_at       | 2015-12-23T16:16:19.540661+00:00       |
| sriov_numvfs     | 0                                      |
| ipv4_mode        | disabled                               |
| ipv6_mode        | disabled                               |
| accelerated      | [u'True']                              |
+------------------+----------------------------------------+
```

Configuring Aggregated Ethernet Interfaces

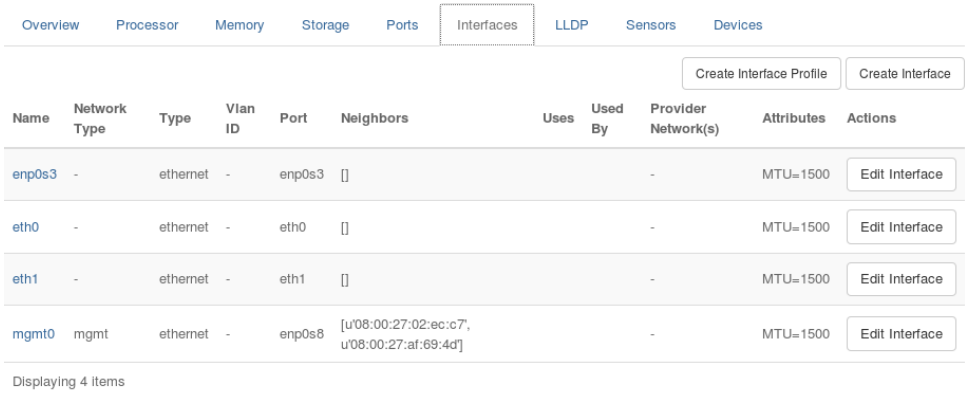
You can add and remove interfaces from a LAG group on a host using the Web administration interface or the CLI.

For CLI instructions, see Network Interface Provisioning Using the CLI on page 76.

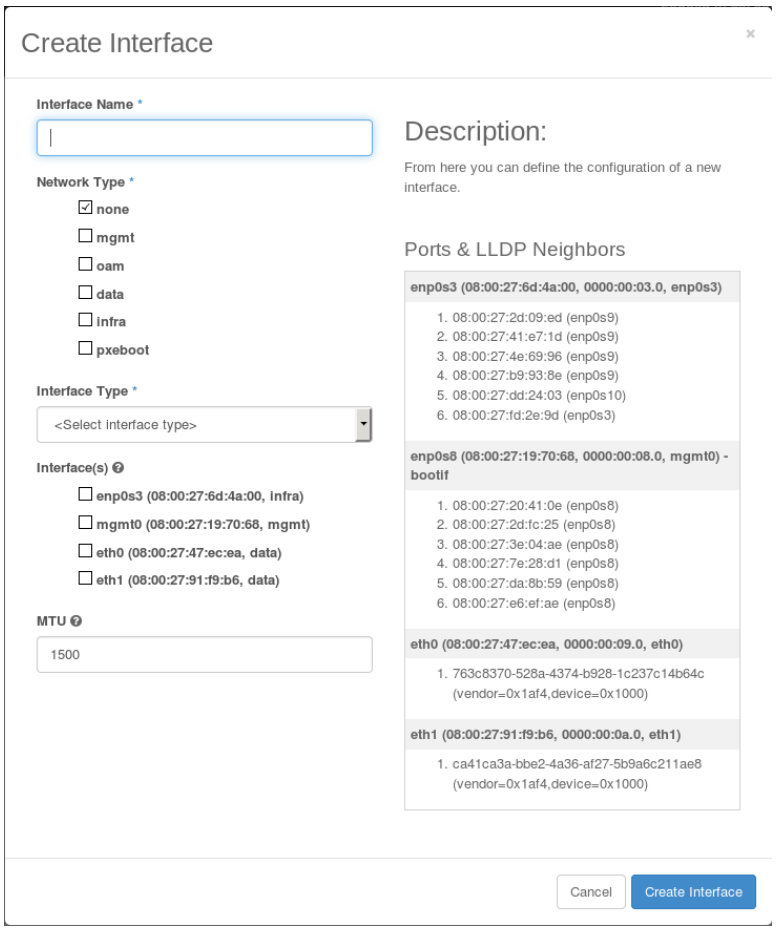
HCG 4.0 supports up to four ports in a LAG group.

Procedure

1. Open the **Inventory Detail** page for the host.
   a) Open the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane.
   b) Select the **Hosts** tab, and then in the **Host Name** column, click the name of the host.
2. Select the **Interfaces** tab.



3. Click **Create Interface**.



4. Select the type of network for the interface.

   For details, see Interface Settings on page 78.

5. If required, open the **Interface Type** drop-down menu, and select **aggregated ethernet**.

   The **Interface Type** control appears when the **Network Type** is set to **mgmt**, **oam**, **data**, or **infra**.

6. Set the **Aggregated Ethernet - Mode**. For more information, see Link Aggregation Settings on page 92.

7. From the **Interfaces** list, select the Ethernet interfaces used to attach this interface to the network.

8. Complete any other settings required for the Network Type. For more information, see Interface Settings on page 78.

9. To save your changes and close the dialog box, click **Create Interface**.

The interface is created and attached to the network.

Configuring Aggregated Ethernet Interfaces Using the CLI

You can use the CLI to attach aggregated Ethernet interfaces to networks.

HCG 4.0 supports up to four ports in a LAG group.

To create an aggregated Ethernet interface and attach it to a network, use a command of the following form:

```
~(keystone_admin)$ system host-if-add hostname -m mtu \
-a aemode -x policy ifname \
 ae "providernetworklist" ethname1 ethname2
```

where

ifname

is a name for the interface

mtu

is the MTU for the interface

aemode

is the link aggregation mode

policy

is the balanced tx distribution hash policy

hostname

is the name or UUID of the host

providernetworklist

is a list of provider networks to attach to, separated by spaces

NOTE: For networks other than data networks, the value **none** is required.

ethname1, ethname2

are the names or UUIDs of the member interfaces

For example, to attach an aggregated Ethernet interface named **ae0** to provider networks **provider-net-a** and **provider-net-b**, using member interfaces **enp0s9** and **enp0s10** on **compute-0**:

```
~(keystone_admin)$ system host-if-add compute-0 -a balanced \
-x layer2 ae0 ae "provider-net-a provider-net-b" enp0s9 enp0s10
```

For more about link aggregation modes and policies, see Link Aggregation Settings on page 92.

Changing a Management Interface to Aggregated

When compute and storage nodes are provisioned, the Ethernet interface used for PXE boot is automatically assigned to the internal management network.

To configure a management LAG interface you first need to remove the internal management network type from the existing management Ethernet interface and then add a new AE interface,

specifying the **mgmt** network type, **ae** interface type, **802.3 AE** mode, transmit hash policy and the slave interfaces.

Prerequisites

The node must be locked to edit an interface.

From the command line, you must first delete and then recreate the management interface.

```
~(keystone_admin)$ system host-if-modify -nt none node interface
```

where:

node

is the name of the node from which to delete an interface

interface

is the Ethernet interface to delete

You must then create the new interface.

```
~(keystone_admin)$ system host-if-add -nt mgmt -a 802.3ad -x layer2 node interface ae
none ports
```

where

node

is the name of the node

interface

is the name to be assigned to the interface

ports

are the Ethernet ports to assign

For example:

```
~(keystone_admin)$ system host-if-add -nt mgmt -a 802.3ad -x layer2 compute-0 bond0 ae
none enp0s8 enp0s9
```

Link Aggregation Settings

HCG 4.0 supports several link aggregation (LAG) operational modes.

If you select link aggregation (also known as Aggregate Ethernet) when configuring the management, infrastructure, or OAM networks, you can choose from the following operational modes. For more information, refer to the Linux kernel Ethernet Bonding Driver documentation available online.

NOTE: Ensure that the LAG mode on the corresponding Top-of-Rack (ToR) switch ports is configured to match your selection.

Table 1 **Supported Link Aggregation Operational Modes**

Mode	Description	Supported Interface Types
Active-backup (default value)	Provides fault tolerance. Only one slave interface at a time is available. The backup slave interface becomes active only when the active slave interface fails.	OAM, infrastructure, and data interfaces (compute nodes)
Balanced XOR	Provides aggregated bandwidth and fault tolerance. The same slave interface is used for each destination MAC address. This mode uses the default transmit policy, where the target slave interface is determined by calculating the source MAC address XOR'd with the destination MAC address, modulo 2. You can modify the transmit policy using the **xmit-hash-policy** option. For details, see Table 2 on page 93.	OAM, infrastructure, and data interfaces (compute nodes)
802.3ad	Provides aggregated bandwidth and fault tolerance. Implements dynamic link aggregation as per the IEEE 802.3ad (LACP) specification. You can modify the transmit policy using the xmit-hash-policy option. For details, see Table 2 on page 93. In order to support PXE booting over an aggregated management interface, the far-end switch ports must be configured in passive LACP mode. This is required because the BIOS on the host does not support LACP and cannot establish a LAG group, and therefore can use only one of the aggregated interfaces during PXE boot. If the far-end switch is configured to use active LACP, it can establish a LAG group and use either interface, potentially resulting in a communication failure during the boot process.	Management, infrastructure, and data interfaces (compute nodes)

Table 2 **xmit-hash-policy Options**

Option	Description	Supported Interface Types
Layer 2 (default value)	Hashes on source and destination MAC addresses.	OAM, internal management, infrastructure, and data interfaces (compute nodes)
Layer 2 + 3	Hashes on source and destination MAC addresses, and on source and destination IP addresses.	OAM, internal management, and infrastructure

Option	Description	Supported Interface Types
Layer 3 + 4	Hashes on source and destination IP addresses, and on source and destination ports.	OAM, internal management, and infrastructure

Configuring VLAN Interfaces

You can attach an interface to multiple networks using VLAN tagging.

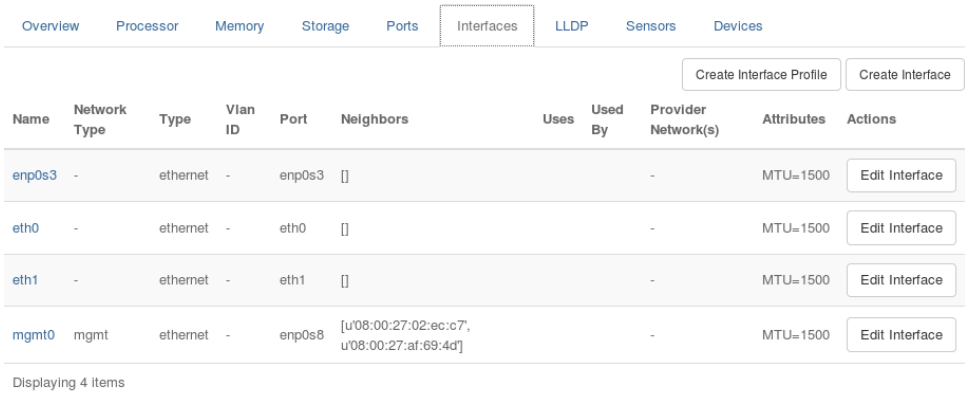
If the cluster is configured with VLAN-tagged networks, you can share an Ethernet interface by attaching it to one or more VLAN-tagged networks. You can do this using the Web administration interface or the CLI. For CLI instructions, see Network Interface Provisioning Using the CLI on page 76.

NOTE: When attaching to a data network using a VLAN interface, you can select a flat or VXLAN provider network. However, you cannot connect to a VLAN provider network (stacked VLANs are not supported). As an alternative that supports VLAN provider networks, you can edit a management or infrastructure interface to attach to a data network. For more information, see Editing Interface Settings on page 81.

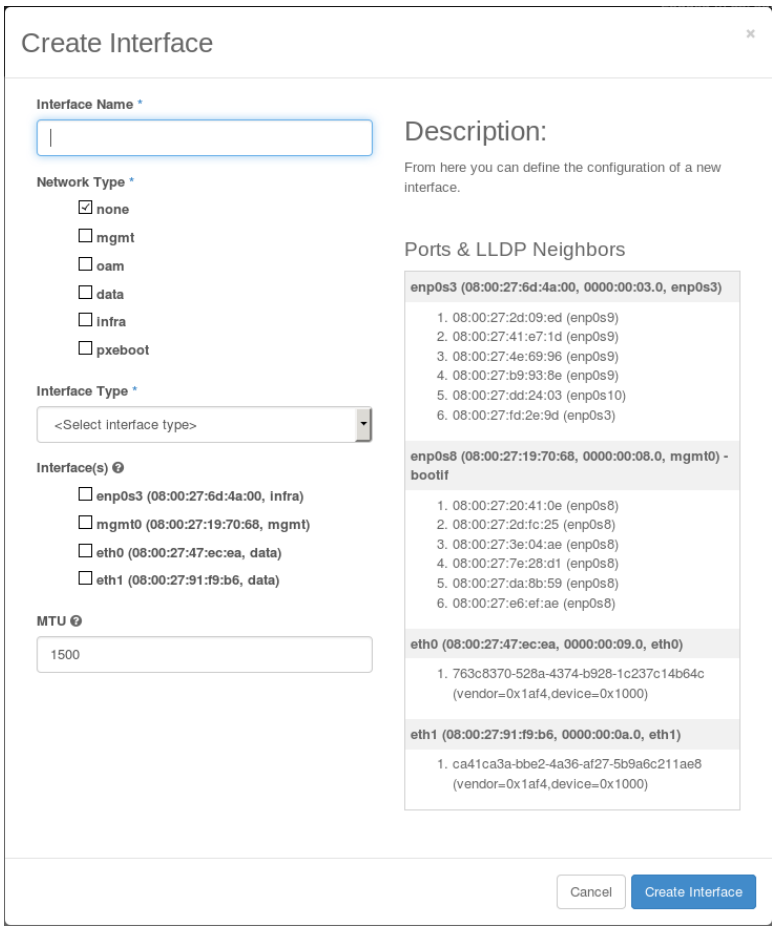
For more information about shared interfaces, see *HCG 4.0 Planning: Shared (VLAN) Ethernet Interfaces*.

Procedure

1. Open the **Inventory Detail** page for the host.
   a) Open the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane.
   b) Select the **Hosts** tab, and then in the **Host Name** column, click the name of the host.
2. Select the **Interfaces** tab.



3. Click **Create Interface**.



4. Select the type of network for the interface.

   For details, see Interface Settings on page 78.

5. Open the **Interface Type** drop-down menu, and select **vlan**.

   The **Interface Type** control appears when the **Network Type** is set to **mgmt**, **oam**, **data**, or **infra**.

6. In the **Vlan ID** field, type a unique VLAN identifier for the network.

7. From the **Interfaces** list, select the Ethernet interfaces used to attach this interface to the network.

   The Ethernet interfaces correspond to ports on the node. For more information, see Network Interface Provisioning on page 75.

8. Complete any other settings required for the Network Type. For more information, see Interface Settings on page 78.

9. To save your changes and close the dialog box, click **Create Interface**.

The interface is created and attached to the network.

Configuring VLAN Interfaces Using the CLI

You can use the CLI to attach VLAN interfaces to networks.

To create a VLAN interface and attach it to a network, use a command of the following form:

```
~(keystone_admin)$ system host-if-add hostname -V vlan_id \
-nt networktype ifname ethname [-p providernetworklist]
```

where

ifname

is a name for the interface

vlan_id

is the VLAN identifier for the network

hostname

is the name or UUID of the host

networktype

is the type of network to attach to

ethname

is the name or UUID of the Ethernet interface to use

providernetworklist

is a list of provider networks, delimited by quotes and separated by spaces; for example, "provider-net-a provider-net-b". To specify a single provider network, omit the quotes. This parameter is required only if the *networktype* is set to **data**.

For example, to attach a VLAN interface named **infra0** with VLAN ID **22** to the infrastructure network, using Ethernet interface **enp0s8** on **storage-0**:

```
~(keystone_admin)$ system host-if-add storage-0 -V 22 -nt infra infra0 vlan enp0s8
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| ifname           | infra0                               |
| networktype      | infra                                |
| iftype           | vlan                                 |
| ports            | []                                   |
| providernetworks | None                                 |
| imac             | 08:00:27:f2:0d:68                    |
| imtu             | 1500                                 |
| aemode           | None                                 |
| schedpolicy      | None                                 |
| txhashpolicy     | None                                 |
| uuid             | 8ca9854e-a18e-4a3c-8afe-f050da702fdf |
| ihost_uuid       | 3d207384-7d30-4bc0-affe-d68ab6a00a5b |
| vlan_id          | 22                                   |
| uses             | [u'enp0s8']                          |
| used_by          | []                                   |
| created_at       | 2015-02-04T16:23:28.917084+00:00     |
| updated_at       | None                                 |
+------------------+--------------------------------------+
```

where

ifname

is a name for the interface

mtu

is the MTU for the interface

aemode

is the link aggregation mode

policy

is the balanced tx distribution hash policy

hostname

is the name or UUID of the host

ethname1, ethname2

are the names or UUIDs of the member interfaces

Configuring Data Interfaces for VXLANs

For VXLANs, static endpoint IP addresses are required on compute host data interfaces.

For complete information about configuring VXLANs and assigning static IP address to data interfaces, see *Helion OpenStack Carrier Grade 4.0 System Administration:**Using VXLANs on page 34*.

Starting a HCG 4.0 Cluster

You can use a recommended procedure to restart an entire HCG 4.0 cluster.

This may be necessary, for instance, after the underlying hardware has been shut down and physically moved.

Procedure

1. Power on **controller-0**.

   Ensure that the host is fully booted by logging in to a console, and confirm that it is unlocked from the output of the **system host-list** command before proceeding.

2. Power on **controller-1**.

   Ensure that the host is fully booted by logging in to a console, and confirm that it is unlocked from the output of the **system host-list** command before proceeding.

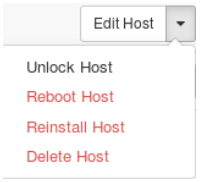
3. Power on **storage-0**.

   Ensure that the host is fully booted by logging in to a console, and confirm that it is unlocked from the output of the **system host-list** command before proceeding.

4. Power on and unlock **storage-1**.

   Ensure that the host is fully booted by logging in to a console before proceeding.

5. Power on and unlock each compute node.
   a) Follow the instructions for the node's hardware to power it up.
   b) On the Hosts tab of the **Admin** > **Platform** > **Host Inventory** page, select **Edit Host** > **Unlock Host**.



6. Start the virtual machines.

Shutting Down a HCG 4.0 Cluster

You can perform a controlled shutdown of an entire HCG 4.0 cluster.

This may be necessary if, for instance, you need to physically move the underlying hardware.

Procedure

1. Swact to controller-0.

   From the **Admin** > **Platform** > **Host Inventory** page, on the Hosts tab, select **Edit Host** > **Swact Host** for controller-0.

2. Shut down all virtual machine instances.

   Shutdown procedures vary between operating systems. Follow the instructions provided in your operating system documentation.

3. Lock and shut down each compute node.
   a) From the **Admin** > **Platform** > **Host Inventory** page, on the Hosts tab, select **Edit Host** > **Lock Host**.
   b) From the terminal of the compute node, issue a **shutdown** command.

```
# shutdown -hP now
```

   Wait until the node is completely shut down before proceeding to the next step.

4. Lock and shut down **storage-1**.

   Wait for several minutes to ensure ceph has detected and reacted to the missing storage node. You can use **ceph -s** to verify that the OSDs on storage-1 are down.

5. Shut down **storage-0**.

   You cannot lock this storage node, because Ceph storage requires a quorum of two unlocked storage nodes and at least one unlocked controller.

```
# shutdown -hP now
```

Wait until the node is completely shut down before proceeding to the next step.

6. On a cluster that uses controller storage, lock **controller-1**.

NOTE: This applies only to LVM-backed systems (systems without storage nodes). On a Ceph-backed system with dedicated storage nodes, **controller-1** cannot be locked.

7. Shut down **controller-1**.

```
# shutdown -hP now
```

Wait until the node is completely shut down before proceeding to the next step.

8. Shut down **controller-0**.

```
# shutdown -hP now
```

Postrequisites

For information on restarting the cluster, see Starting a HCG 4.0 Cluster on page 97.

LLDP Overview

HCG 4.0 supports the Link Layer Discovery Protocol (LLDP).

The Link Layer Discovery Protocol (LLDP), defined in the *IEEE 802.1AB Station and Media Access Control Connectivity Discovery* specification, enables devices attached to the network to advertise their properties to other devices on the same network.

HCG 4.0 supports both the sending and receiving of LLDP messages on all physical interfaces.

LLDP neighbor information is displayed in the LLDP tab of the Inventory Detail window, or through system CLI commands.

LLDP information can be used to verify cabling to the next hop device (typically the Top-of-Rack switch).

NOTE: The neighboring device must be capable of, and enabled for, transmitting LLDP frames.

Devices differ in the level of information sent in an LLDP packet data unit (PDU). This can often be configured on the neighboring device. Refer to the documentation for the device for specific information.

Viewing LLDP Information

You can view LLDP information on the **LLDP** tab in the Inventory Details window.

Procedure

1. Select **Admin** > **Platform** > **Host Inventory**.
2. Select the **Hosts** tab.
3. Click the name of the host for which you want to view LLDP information in the **Host Name** column.

   The Inventory Details screen appears.
4. Select the **LLDP** tab to view the LLDP information for this host.

   The **LLDP** tab provides the following information about each LLDP-enabled neighbor device:

   Table 3 **LLDP Details**

Field	Description
Name	The name of the local port connected to the LLDP neighbor.
Neighbor	The port identifier of the LLDP neighbor port.
Port Description	The port description of the LLDP neighbor port.
Time To Live	The time until the neighbor is timed out (if no further LLDP frames are received from it).
System Name	The system name of the neighbor.
Max Frame Size	The maximum frame size supported by the neighbor port.

If the neighbor is sending additional information, the information is shown when you click on the port to which the neighbor is connected. The extra information can include zero or more of the following items:

Table 4 **LLDP Port Details**

Field	Description
Chassis	The chassis identifier of the neighbor. Usually a MAC address, IP address, or locally assigned name identifying the neighbor.
MAC Service Access Point	A concatenation of the chassis identifier and port identifier, uniquely identifying the particular neighbor device/port.

Field	Description
System Capabilities	The system capabilities of the neighbor. For example, bridging, routing enabled.
Management Address	The management address of the neighbor device.
Dot1 Link Aggregation	The 802.1 link aggregation status of the neighbor.
Dot1 Proto Ids	The 802.1 protocol identifiers supported by the neighbor.
Dot1 Proto Vids	The 802.1 port and protocol VLAN identifiers supported by the neighbor.
Dot1 Vid Digest	The 802.1 VLAN identifier digest of the neighbor.
Dot1 Management Vid	The 802.1 management VLAN identifier of the neighbor.
Dot1 Vlan Names	The 802.1 VLAN names of the neighbor port.
Dot3 Power MDI	The 802.3 power MDI status of the neighbor.
Dot3 MAC status	The 802.3 MAC status of the neighbor port.

Displaying LLDP Neighbor Information Using the CLI

You can use CLI commands to view information about LLDP neighbors.

The following commands are available for displaying LLDP neighbors:

Viewing Host Neighbor List

To see the LLDP neighbors of a host:

```
$ system host-lldp-neighbor-list host name|id
```

Viewing LLDP Neighbor Information

To view LLDP neighbor information:

```
$ system lldp-neighbor-show neighbor uuid
```

Example

The following example shows the usage for these commands. Use **system host-lldp-neighbor-list** to get the neighbor IDs, then use the IDs with the **system lldp-neighbor-show** command to get details for a specific LLDP neighbor.

```
$ system host-lldp-neighbor-list controller-0

+--------------------------------------+----------+---------+----------+...
| uuid                                 | local_po | remote_ | chassis_ |...
```

```
|                                      | rt       | port    | id       |...
+--------------------------------------+----------+---------+----------+...
| 081cc900-0569-47cb-95c9-dcb6b53c2a70 | enp0s10  | 08:00:2 | 08:00:27 |...
|                                      |          | 7:6d:4a | :47:ec:e |...
|                                      |          | :00     | a        |...
|                                      |          |         |          |...
|                                      |          |         |          |...
| 68046495-9e09-4fe2-b8a4-ebc3daf728d7 | enp0s10  | 08:00:2 | 08:00:27 |...
|                                      |          | 7:fd:2e | :23:f8:f |...
|                                      |          | :9d     | 2        |...
|                                      |          |         |          |...
|                                      |          |         |          |...
| 24832b54-6a71-4925-9353-51398b2248f6 | enp0s10  | 08:00:2 | 08:00:27 |...
|                                      |          | 7:b9:93 | :4a:d9:2 |...
|                                      |          | :8e     | 9        |...
|                                      |          |         |          |...
|                                      |          |         |          |...
| da09d634-5dd8-4c9e-8620-933f6e910238 | enp0s10  | 08:00:2 | 08:00:27 |...
|                                      |          | 7:4e:69 | :08:fc:f |...
|                                      |          | :96     | 1        |...
|                                      |          |         |          |...
|                                      |          |         |          |...

...--------------------------------------+--------------+--------------------+
... system_name                          | system_descr | management_address |
...                                      | iption       |                    |
...--------------------------------------+--------------+--------------------+
... compute-0:7ee03cf1-ac2b-             | HCG 4.0      | 192.168.205.185, f |
... 40f3-ae11-d68275df71c1               |              | e80::a00:27ff:fe6d |
...                                      | version      | :4a00              |
...                                      | 4.0          |                    |
...                                      |              |                    |
... compute-1:7ee03cf1-ac2b-             | HCG 4.0      | 192.168.205.237, f |
... 40f3-ae11-d68275df71c1               |              | e80::a00:27ff:fefd |
...                                     | version      | :2e9d              |
...                                      | 4.0          |                    |
...                                      |              |                    |
... storage-0:7ee03cf1-ac2b-             | HCG 4.0      | 192.168.204.192, f |
... 40f3-ae11-d68275df71c1               |              | e80::a00:27ff:fee6 |
...                                      | version      | :efae              |
...                                      | 4.0          |                    |
...                                      |              |                    |
... storage-1:7ee03cf1-ac2b-             | HCG 4.0      | 192.168.204.222, f |
... 40f3-ae11-d68275df71c1               |              | e80::a00:27ff:fe7e |
...                                      | version      | :28d1              |
...                                      | 4.0          |                    |
...                                      |              |                    |
```

$ **system lldp-neighbor-show 5742ce56-0420-42df-9096-d13b0a118521**

```
+---------------------+-------------------------------------------------...+
| Property            | Value                                                |
+---------------------+-------------------------------------------------...+
| uuid                | 081cc900-0569-47cb-95c9-dcb6b53c2a70                 |
| host_uuid           | a0c44be2-6d3b-4ada-9748-7f8c92e62496                 |
| created_at          | 2016-06-24T17:25:12.280967+00:00                     |
| updated_at          | None                                                 |
| uuid                | 081cc900-0569-47cb-95c9-dcb6b53c2a70                 |
| local_port          | enp0s10                                              |
| chassis_id          | 08:00:27:47:ec:ea                                    |
| port_identifier     | 08:00:27:6d:4a:00                                    |
| ttl                 | 117                                                  |
| msap                | 08:00:27:47:ec:ea,08:00:27:6d:4a:00                  |
| system_description  | HCG 4.0 version 4.0                                  |
| system_name         | compute-0:7ee03cf1-ac2b-40f3-ae11-d68275df71c1       |
| system_capabilities | router, station                                      |
| management_address  | 192.168.205.185, fe80::a00:27ff:fe6d:4a00            |
| port_description    | enp0s3                                               |
| dot1_lag            | capable=y,enabled=n                                  |
| dot1_port_vid       | None                                                 |
| dot1_vlan_names     | None                                                 |
| dot1_proto_vids     | None                                                 |
| dot1_proto_ids      | None                                                 |
| dot3_mac_status     | auto-negotiation-capable=y,auto-negotiation-enabl..|
```

```
| dot3_max_frame      | None                                                  |
+---------------------+-------------------------------------------------...+
```

Configuring Hosts with Board Management

You can activate board management on a host by provisioning the host with information about the attached board management module.

For some board management modules, you can also configure reporting for hardware sensors. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: Sensors Tab on page 70*.

Prerequisites

To use board management on a host, the host must be equipped with a supported HP Integrated Lights Out (iLO) module (iLO3, iLO4, or Quanta). To provision a host with board management, you need the MAC address, user name, and password for the board management module. The module must also be configured to use DHCP for a board management network that uses internal access, or static IP addressing for a network that uses external access. For more information, consult the user documentation for the module.

If the board management is configured for external access, you also need an IP address to assign to the module. For this information, consult your configuration plan.

You can use the Web administration interface or the CLI to provision the host. For CLI instructions, see Configuring a Host for Board Management Using the CLI on page 104.

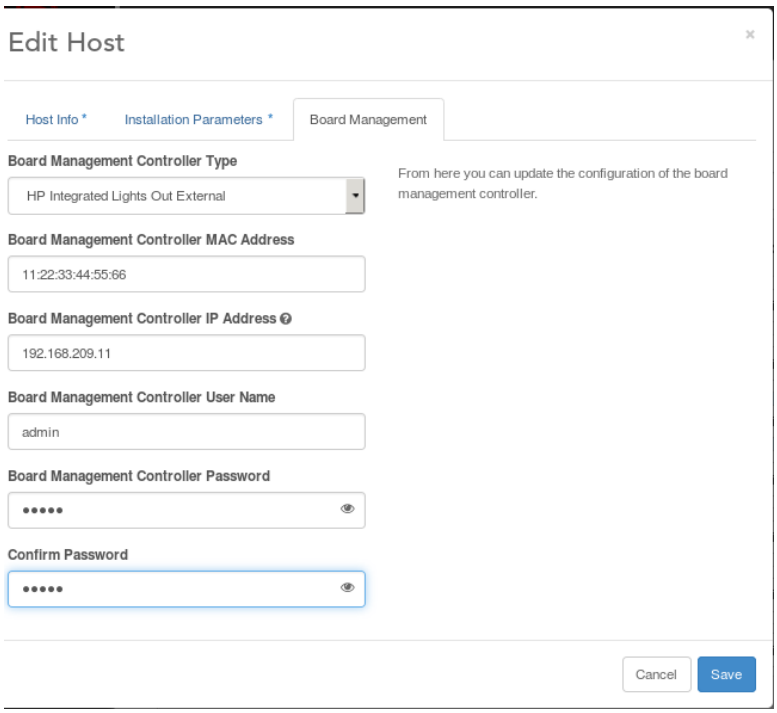
Procedure

1. Open the **Hosts** list.

   On the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane, select **Inventory**.

2. Click **Edit Host** for the host.

3. Select the **Board Management** tab.



4. Complete the form as follows.

Field	Comments
Controller Type	Select the type of iLO module attached to the host.
Controller MAC Address	Provide the MAC address of the iLO module.
Controller IP Address	This field is present if the board management network is configured for external access. Provide the IP address of the iLO module.
User Name Password Confirm Password	Provide the user name and password configured for the iLO module.

5. Click **Save**.

Configuring a Host for Board Management Using the CLI

To use board management on a host, you must provision the host with information about the attached board management module. If you prefer, you can do this from the command-line interface.

For some board management modules, you can also configure reporting for hardware sensors. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Sensors Tab on page 70*.

Prerequisites

To complete this task, you need the board type (iLO3, iLO4, or Quanta), MAC address, user name, and password of the board management module. The module must also be configured to use DHCP for a board management network that uses internal access, or static IP addressing for a network that uses external access. For more information, consult the user documentation for the module.

If the board management is configured for external access, you also need an IP address to assign to the module. For this information, consult your configuration plan.

Procedure

1. Provision the host with the MAC address and module type of the attached iLO module.

   ```
   ~(keystone_admin)$ system host-update hostname bm_mac=MAC_address
   bm_type=module_type
   ```

   For example:

   ```
   ~(keystone_admin)$ system host-update compute-0 bm_mac=b4:b5:2f:ee:ae:90
   bm_type=ilo4
   ```

2. Provision the host with the user name and password of the iLO module.

   ```
   ~(keystone_admin)$ system host-update hostname bm_username=user_name \
   bm_password=password
   ```

3. If the board management network is configured for external access, provision the host with the IP address of the iLO module.

   ```
   ~(keystone_admin)$ system host-update hostname bm_ip=ip_address
   ```

Replacing Controller Hardware

You can replace controller hosts or hardware components while the system is running.

The HCG 4.0 requires two controllers. You can lock and remove one controller temporarily to replace faulty hardware, including primary or secondary disks.

NOTE: If you are replacing disks in order to increase the controller storage capacity, follow the instructions for Increasing Storage Space Allotments on the Controller on page 127.

Procedure

1. Lock the standby controller.
   a) On the **Admin** menu of the Web administration interface, in the **System** section, select **Inventory**.
   b) Select the **Hosts** tab.

c) In the **Actions** column, open the drop-down list for the host, and then select **Lock Host**.

d) Wait for the host to be reported as **Locked**.

The standby controller is shown as **Locked**, **Disabled**, and **Online**.

2. Delete the standby controller from the inventory.

NOTE: Ensure that the host is online, so that its disk is erased when it is deleted from the inventory. This ensures that the host boots from the network when it is powered up for re-installation. If the host is not online when it is deleted from the inventory, you may need to force a network boot during re-installation.

In the **Actions** column, open the drop-down list for the host, and select **Delete Host**.

The standby controller is removed from the **Hosts** list, and the HCG 4.0 software is removed from its hard drive.

3. Power down the host manually and make any required hardware changes.

HCG 4.0 does not provide controls for powering down a host. Use the BMC or other control unit.

4. Reinstall the standby controller.

⚠ **CAUTION:** Before attempting to unlock the controller, be sure to specify the correct disk for the Ceph monitor, if required. This is necessary if Ceph storage has been added to a system with LVM-backed controller storage after installation, and the Ceph monitor has been assigned to a disk other than the **rootfs** disk.

⚠ **CAUTION:** *You must do this before unlocking the reinstalled controller for the first time*. Otherwise, the controller reboots continuously on unlock, and must be installed again.

To specify the correct disk, use a command of the following form:

```
~(keystone_admin)$ system ceph-mon-modify controller_name device_node=diskUUID
```

For example:

```
~(keystone_admin)$ system ceph-mon-show controller-1
+--------------+--------------------------------------+
| Property     |                                Value |
+--------------+--------------------------------------+
| uuid         | ce4a1913-ce1f-4fda-90c0-c49f313d0adc |
| device_node  | None                                 |
| ceph_mon_gib | 30                                   |
| created_at   | 2016-10-15T00:16:56.423442+00:00     |
| updated_at   | None                                 |
+--------------+--------------------------------------+
~(keystone_admin)$ system ceph-mon-modify controller-1 \
device_node=cbc483ad-d7cb-47a8-8622-8846d9444f27
+--------------+--------------------------------------+
| Property     | Value                                |
+--------------+--------------------------------------+
| uuid         | ce4a1913-ce1f-4fda-90c0-c49f313d0adc |
| device_node  | /dev/sdc                             |
| ceph_mon_gib | 30                                   |
| created_at   | 2016-10-15T00:16:56.423442+00:00     |
| updated_at   | None                                 |
+--------------+--------------------------------------+

System configuration has changed.
 please follow the administrator guide to complete configuring system.
~(keystone_admin)$ system ceph-mon-show controller-1

+--------------+--------------------------------------+
| Property     | Value                                |
+--------------+--------------------------------------+
| uuid         | ce4a1913-ce1f-4fda-90c0-c49f313d0adc |
| device_node  | /dev/sdc                             |
| ceph_mon_gib | 30                                   |
| created_at   | 2016-10-15T00:16:56.423442+00:00     |
| updated_at   | 2016-10-15T00:35:44.181413+00:00     |
+--------------+--------------------------------------+
```

For more informaton about reinstalling the controller, see *HCG 4.0 Installation: Installing Software on Controller-1 or a Compute or Storage Host*.

5. If the same hardware change is required on both controllers, make the change to the other controller.
   a) Open the drop-down menu for the active controller and then select **Swact Host**.

      Up to 20 minutes can be required to complete the swact.

NOTE: During the swact, access to the Web administration interface is temporarily interrupted, and the login screen is displayed. Wait for a few minutes, and then log in. The new active controller is shown as **Degraded**, and then changed to **Available**.

The **Controller-Active** and **Controller-Standby** personalities are updated in the Hosts List.

Host Name	Personality	Admin State	Operational State	Availability State	Uptime	Status	Actions
compute-0	Compute	Unlocked	Enabled	Available	21 hours, 13 minutes		Edit Host
compute-1	Compute	Locked	Disabled	Online	21 hours, 14 minutes		Edit Host
controller-1	Controller-Active	Unlocked	Enabled	Available	21 minutes		Edit Host
controller-0	Controller-Standby	Unlocked	Enabled	Available	21 hours, 27 minutes		Edit Host
storage-0	Storage	Unlocked	Enabled	Available	21 hours, 18 minutes		Edit Host
storage-1	Storage	Unlocked	Enabled	Available	19 hours, 33 minutes		Edit Host

Displaying 6 items

b) Return to Step 1 and repeat the procedure for the new standby controller.

The updated controllers are now in service.

Compute Node Management

The compute nodes in HCG 4.0 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:

- You can add or remove hosts to increase or decrease the size of the pool.
- You can replace a host with another that has different resources (for example, memory, or number of CPU cores).
- You can adjust the resources on an existing host.
- You can 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.

Complete instructions for adding a compute node are provided in *HCG 4.0 Installation*.

Displaying Compute Node Information

You can view compute node resources from the Web administration interface or the CLI. You can also view data interface assignments graphically from the Web administration interface.

Using the Web administration interface, you can obtain information about compute hosts in two places:

- The Provider Network Topology view. This is a graphical representation of all compute nodes on the system and their data interface connections. You can select individual compute hosts to view details. You can also review active alarms for the data interface connections. For more information, see The Provider Network Topology View on page 23.

NOTE: You cannot make changes from this view.

- The Hosts tab on the Host Inventory page. This contains a list of all hosts on the system, showing their current status. You can select an individual compute host to obtain more information or to edit its resources and connection details. For more information, see Inventory Detail on page 58.

Adjusting Resources on a Compute Node

You can adjust the resources of a compute node while it is offline.

Procedure

1. Lock the host to make changes.
   a) On the **Admin** menu of the Web administration interface, in the **System** section, select **Inventory**.
   b) Select the **Hosts** tab.
   c) In the **Actions** column, open the drop-down list for the host, and then select **Lock Host**.
   d) Wait for the host to be reported as **Locked**.
2. Delete the host from the inventory.
   It is recommended that you delete the host and re-install it to ensure that any resource changes, such as device name reassignments, are correctly recorded in the inventory.

NOTE: Ensure that the host is **Online**, so that its disk is erased when it is deleted from the inventory. This ensures that the host boots from the network when it is powered up for re-installation. If the host is not online when it is deleted from the inventory, then during re-installation you may need to force a network boot.

   In the **Actions** column, open the drop-down list for the host, and then select **Delete Host**.

The storage node is removed from the **Hosts** list, and the HCG 4.0 software is removed from its hard drive.

3. Power off the host.
4. 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.

5. Install the modified host as a node on HCG 4.0.

   To ensure that changes to the host are correctly recorded in the system inventory, perform a full initialization and configuration. For detailed instructions, refer to *HCG 4.0 Installation*.

When the host is reported as **Unlocked**, **Enabled**, and **Available**, it is ready for use with the adjusted resources.

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-real-time tasks for multiple VMs, freeing other cores on the host for dedicated high-load tasks.

Procedure

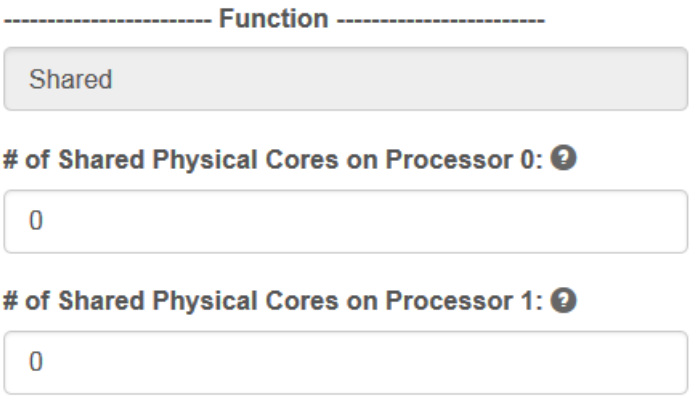
1. Lock the host to make changes.
   a) On the **Admin** menu of the Web administration interface, in the **System** section, select **Inventory**.
   b) Select the **Hosts** tab.
   c) In the **Actions** column, open the drop-down list for the host, and then select **Lock Host**.
   d) Wait for the host to be reported as **Locked**.
2. Open the **Inventory Detail** page for the locked host.

   In the **Host Name** column, click the name of the host.

3. Select the **Processor** tab.
4. Click **Edit CPU Assignments**.

   This control is available only if the host is locked.

5. In the Edit CPU Assignments dialog box, 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.)

6. Unlock the host to make the changes take effect.

Postrequisites

To configure a VM to use a shared physical CPU, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Pinning a vCPU to a Shared Physical CPU*.

Designating Shared Physical CPUs on a Compute Host Using the CLI

You can use the CLI to set up shared physical CPUs.

To add or remove a shared physical CPU from the CLI, use a command of the following form:

```
~(keystone_admin)$ system host-cpu-modify -f shared -pprocessor 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
```

Changing the Hyper-threading Status

The hyper-threading status is controlled by the BIOS settings of the host.

Procedure

1. Lock the host to prepare it for configuration changes.

   In the **Hosts** list, click **More** for the host, and then select **Lock Host**.

   The host is locked and reported as **Locked**, **Disabled**, and **Online**.

2. Edit the host BIOS settings to enable or disable hyper-threading.

   For more about editing the BIOS, refer to the documentation provided by the maker of the host computer.

   NOTE:

   Changes to the host BIOS must be made while it is locked and the host must not be subsequently unlocked until it comes back online (locked-disabled-online), when the Inventory would have the updated Hyperthreading settings.

   a) Boot the host in BIOS mode.

   b) Update the host BIOS settings to enable or disable hyper-threading.

   c) To apply the changes, allow the host to boot to a locked state with the updated hyper-threading settings.

3. Unlock the host to make it available for use.

   In the **Hosts** list, on the row associated with the node, open the drop-down menu and select **Unlock Host**.

   The host is rebooted, and its **Availability State** is reported as **In-Test**. After a few minutes, it is reported as **Unlocked**, **Enabled**, and **Available**.

4. Confirm the hyper-threading status in HCG 4.0.

   The hyper-threading status is reported on the **Processor** tab for the host. For more information, see Processor Tab on page 60.

Exposing a Device for Use by VMs

You can expose PCI passthrough or SR-IOV devices so that they are accessible for use by VMs.

You can enable or disable exposure from the Web administration interface or the CLI. You can also change the name of the device as listed in the system inventory.

From the CLI, you can use the **system host-device-modify** command, as shown in the following example:

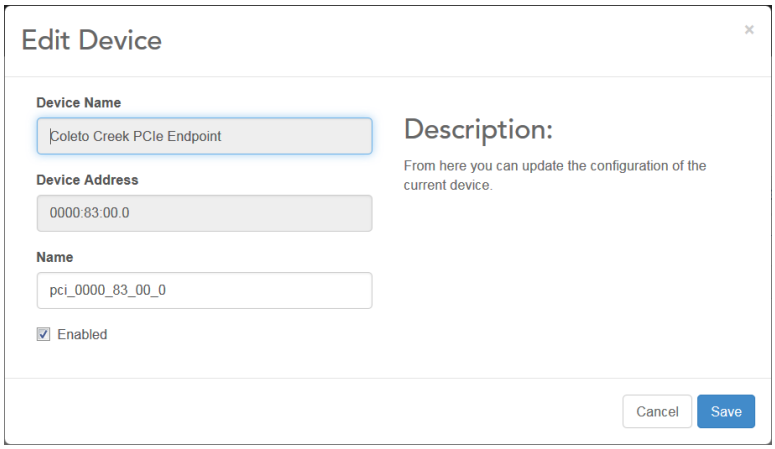
```
~(keystone_admin)$ system host-device-modify --name="Encryption1" --enable=True
compute-0
```

Prerequisites

To edit a device, you must first lock the host.

Procedure

1. Lock the host.
2. Select the **Devices** tab on the Inventory Detail page for the host.
3. Click **Edit Device**.



4. Update the information as required.

   Name

   Sets the system inventory name for the device.

   Enabled

   Controls whether the device is exposed for use by VMs.

Postrequisites

To access the device from a VM, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Accessing a PCI Device from a VM*.

Host Memory Provisioning

For each NUMA node on a host, you can adjust the amount of memory reserved for platform use, and the size and number of memory pages allocated for use by VMs.

Memory not reserved for platform use is made available as VM memory. By default, the VM memory is partitioned 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 performance for systems with large amounts of virtual memory and many running instances.

You can use the **system host-memory-list** and **system host-memory-show** commands to see how much memory is available for VMs. This information is also shown on the **Memory** tab of the Host Inventory page (see Memory Tab on page 62).

After setting the memory allocations for a host, you can save them as a *memory profile*, and then apply the profile to other hosts. For more information, see *HCG 4.0 Installation: Hardware Profiles*.

For individual VMs, you can specify which page size to use. For more information, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Specifying a Page Size for a VM*.

Allocating Host Memory for VM Pages or Platform Use

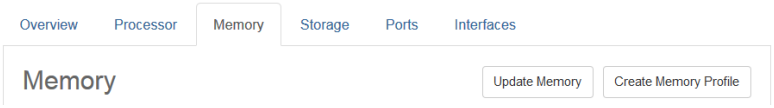
You can edit the platform and VM page memory allocations for a NUMA node from the Web administration interface using the **Memory** tab on the Host Inventory pane.

Prerequisites

Before requesting huge pages on a host, ensure that the host has enough available memory. For details, see Host Memory Provisioning on page 113. If a huge page request cannot be allocated from the available memory, an informative message is displayed.

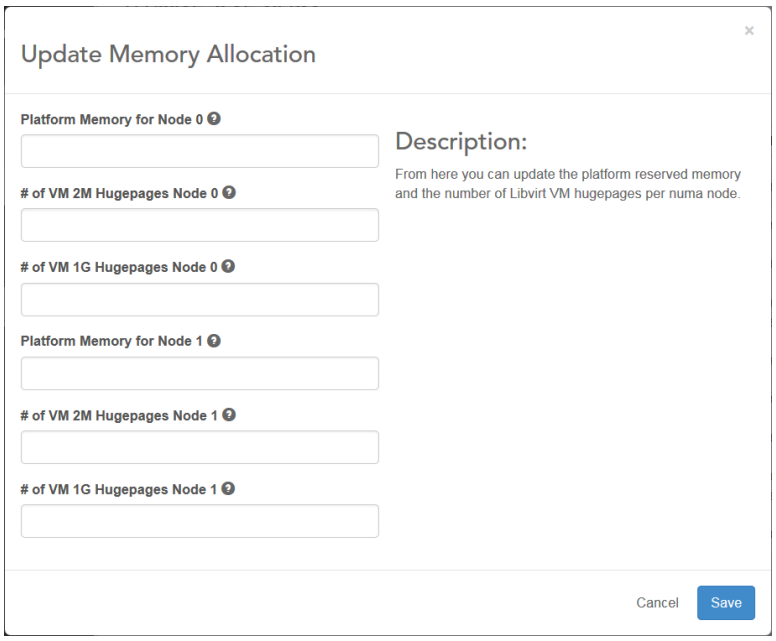
Procedure

1. On the **Inventory** pane, lock the host you want to edit.
2. Click **Host Name** to open the settings for the host.
3. On the **Memory** tab, click **Update Memory**.



4. Use the Update Memory Allocation dialog box to set the memory allocations for each NUMA node.

   For each available NUMA node, three fields are supplied, as illustrated in the following example screen for two NUMA nodes.



Platform Memory for Node *n*

The amount of memory to reserve for platform use on the NUMA Node, in MiB. To see the minimum requirement, hover over the information icon next to the field.

# of VM 2M Hugepages Node *n*

The number of 2 MiB huge pages to reserve for VM use on the NUMA Node. If no 2 MiB pages are required, type 0.

# of VM 1G Hugepages Node *n*

The number of 1 GiB huge pages to reserve for VM use on the NUMA Node. If no 1 GiB pages are required, type 0.

To see how many huge pages of a given size you can successfully request on a node (assuming that pages of another size are not also requested), hover over the information icon next to the field.

Any unused memory is automatically allocated as 4 KiB pages of regular memory for VMs. You must use the Memory Page Size extra spec, or suitable image metadata, to use these 4 KiB pages as the backing mechanism for VM memory allocation requests. See *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Specifying a Page Size for a VM* for details.

5. Click **Save**.

6. Unlock the host and wait for it to be reported as **Available**.

Allocating Host Memory Using the CLI

You can edit the platform and huge page memory allocations for a NUMA node from the CLI.

Procedure

1. Lock the affected host.

```
(keystone_admin)$ system host-lock hostname
```

2. Use the following command to set the memory allocations.

```
(keystone_admin)$ system host-memory-modify hostname processor [-m reserved] [-2M
2Mpages] [-1G 1Gpages]
```

where

hostname

is the host name or ID of the compute node

processor

is the NUMA node of the compute node (0 or 1)

reserved

(if the optional **-m** argument is included) the amount of memory reserved for platform use, in MiB

2Mpages

(if the optional **-2M** argument is included) the number of 2 MiB huge pages to make available

1Gpages

(if the optional **-1G** argument is included) number of 1 GiB huge pages to make available

For example, to allocate four 2 MiB huge pages for use by VMs on NUMA node 1 of compute node **compute-0** :

```
(keystone_admin)$ system host-memory-modify compute-0 1 -2M 4
```

3. Unlock the host.

```
(keystone_admin)$ system host-unlock hostname
```

4. Wait for the host to be reported as **available**.

```
(keystone_admin)$ system host-list hostname
+----+--------------+-------------+----------------+-------------+--------------+
| id | hostname     | personality | administrative | operational | availability |
+----+--------------+-------------+----------------+-------------+--------------+
| 1  | controller-0 | controller  | unlocked       | enabled     | available    |
| 2  | controller-1 | controller  | unlocked       | enabled     | available    |
| 3  | compute-0    | compute     | unlocked       | enabledd    | available      |
+----+--------------+-------------+----------------+-------------+--------------+
```

Replacing Compute Node Hardware

You can replace compute hosts or their hardware components, or remove a compute host 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.

Prerequisites

CAUTION: Before locking a host, ensure that sufficient resources are available on other hosts to migrate any running instances.

Procedure

1. Lock the host to be removed.

   Open the **Hosts** tab on the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane.

   Click **More** > **Lock Host** for the host.

   Wait for the procedure to complete.

2. Delete the host from inventory.

   It is recommended that you delete the host and re-install to ensure that any resource changes are correctly recorded in the inventory.

   NOTE: Ensure that the host is **Online** so that its disk is erased when it is deleted from the inventory. This ensures that the host boots from the network when it is powered up for re-installation. If the host is not online when it is deleted from the inventory, you may need to force a network boot during re-installation.

   Click **More** > **Delete Host** for the host.

3. Power down the host.

4. If hardware changes are required, make them, and then reinstall the host.

   To ensure that changes to the host are correctly recorded in the system inventory, perform a full initialization and configuration. For detailed instructions, refer to *HCG 4.0 Installation*.

Replacing Storage Node Hardware

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.

You can add disks to a storage node to increase capacity, and you can replace a faulty host.

NOTE: The storage nodes in a HCG 4.0 are paired to provide redundancy for High Availability. It is recommended to have a balanced storage capacity in which each host has sufficient independent resources to meet the operational requirements of the system.

Procedure

1. Lock the host to be modified or replaced.

   Open the **Hosts** tab on the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane.

   Click **More** > **Lock Host** for the host.

   Wait for the procedure to be completed.

2. Delete the host from the inventory.

   It is recommended that you delete the host and re-install to ensure that any resource changes, such as device name reassignments, are correctly recorded in the inventory.

   NOTE: Ensure that the host is **Online** so that its disk is erased when it is deleted from the inventory. This ensures that the host boots from the network when it is powered up for re-installation. If the host is not online when it is deleted from the inventory, you may need to force a network boot during re-installation.

   In the **Actions** column, open the drop-down list for the host, and select **Delete Host**.

   The storage node is removed from the **Hosts** list, and the HCG 4.0 software is removed from its hard drive.

3. Power down the host and make any required hardware changes.

   This can involve replacing or adding disks, or replacing the host completely.

4. Install the modified host as a node on HCG 4.0.

   To ensure that changes to the host are correctly recorded in the system inventory, perform a full initialization and configuration. For detailed instructions, refer to *HCG 4.0 Installation*.

Adjusting Sensor Actions and Audit Intervals

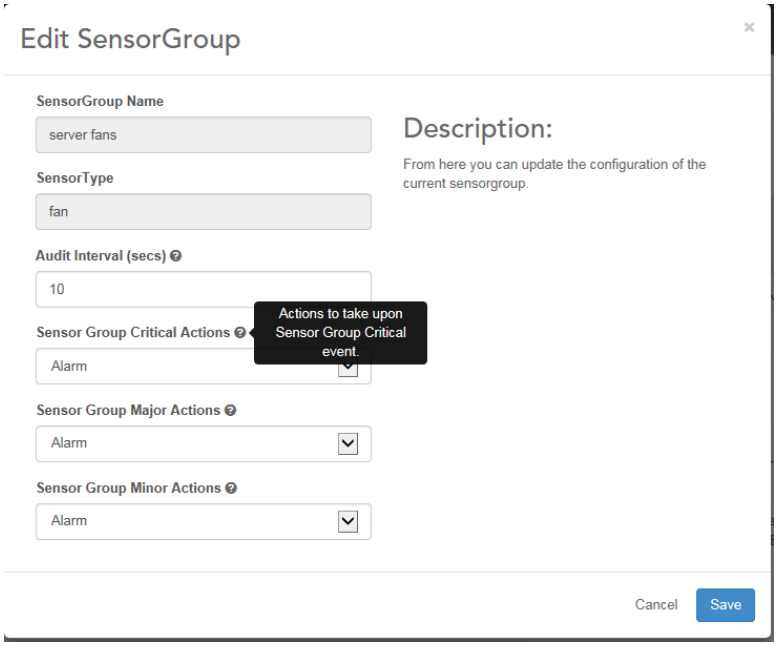
You can configure audit intervals and actions for groups of sensors.

For more information about sensors and sensor groups, see Sensors Tab on page 70.

To use the command-line interface, see CLI Commands for Managing Sensors on page 121.

Procedure

1. Open the **Inventory Detail** page for the host.
   a) Open the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane.
   b) Select the **Hosts** tab, and then in the **Host Name** column, click the name of the host.
2. Select the **Sensors** tab.
3. In the **Sensor Groups** list, click **Edit SensorGroup** for the group you want to configure.



In the Edit SensorGroup dialog box, change the settings as required.

Audit Interval

The time, in seconds, to wait between sensor audits. At each audit, the sensor status reading is refreshed. Changes to the audit interval do not take effect until the current interval expires.

Sensor Group Critical Actions

The action to take if the sensor status is **Critical**. If this is set to **Alarm**, then when this status is reported, a corresponding HCG 4.0 alarm is generated, and the host availability is set to **Degraded**.

Sensor Group Major Actions

The action to take if the sensor status is **Major**. If this is set to **Alarm**, then when this status is reported, a corresponding HCG 4.0 alarm is generated, and the host availability is set to **Degraded**.

Sensor Group Minor Actions

The action to take if the sensor status is **Minor**. If this is set to **Alarm**, then when this status is reported, a corresponding HCG 4.0 alarm is generated.

Suppressing Sensor Actions

You can suppress the configured **Action** for individual sensors or groups of sensors

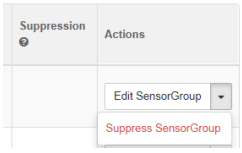
If a sensor is faulty, or is generating frequent minor alarms for a known condition that cannot be addressed immediately, you can prevent it from generating further alarms. Suppressed sensors are still audited, and their status is reported in the **Sensors** list.

For more information about sensors and sensor groups, see Sensors Tab on page 70.

To use the command-line interface, see CLI Commands for Managing Sensors on page 121.

Procedure

1. Open the **Inventory Detail** page for the host.
   a) Open the Host Inventory page, available from **Admin** > **Platform** > **Host Inventory** in the left-hand pane.
   b) Select the **Hosts** tab, and then in the **Host Name** column, click the name of the host.
2. Select the **Sensors** tab.
3. Use the controls on the **Sensors** tab to suppress actions for individual sensors or sensor groups.
   - To suppress actions for a group of sensors, open the **Actions** menu for the group, and then select **Suppress SensorGroup**.



   - To suppress actions for an individual sensor, locate the sensor in the **Sensors** list, and click **Suppress Sensor**.

The **Suppression** field in the list is updated to show that actions are suppressed for the sensor.

CLI Commands for Managing Sensors

You can use the command-line interface to list sensor information and change sensor settings.

The following CLI commands are available for working with sensors. For complete syntax information, refer to the help command.

- **system host-sensor-list**
- **system host-sensor-modify**

  You can modify sensors using the **suppress** parameter (**True** or **False**).
- **system host-sensor-show**
- **system host-sensorgroup-list**
- **system host-sensorgroup-modify**

  You can modify sensor groups using the following parameters:
  - **actions_critical_group** (valid values are **alarm** or **ignore**)
  - **actions_major_group** (valid values are **alarm** or **ignore**)
  - **actions_minor_group** (valid values are **alarm** or **ignore**)
  - **audit interval_group** (time in seconds)
  - **suppress** (**True** or **False**)
- **system host-sensorgroup-show**

For example:

```
~(keystone_admin)$ system host-sensor-modify controller-0 \
d9af9433-44dd-4526-b0fd-8d7a0cdb877b suppress=True
```

For more information about sensors and sensor groups, see Sensors Tab on page 70.

5

Storage Configuration

Storage Planning

HCG 4.0 uses storage resources on the controller and compute hosts, as well as on storage hosts if they are present.

The storage resources are related to system requirements and the type of storage being configured.

For detailed storage requirement calculations, refer to the *HCG 4.0 Engineering Guidelines*.

Storage Flexibility on HCG 4.0

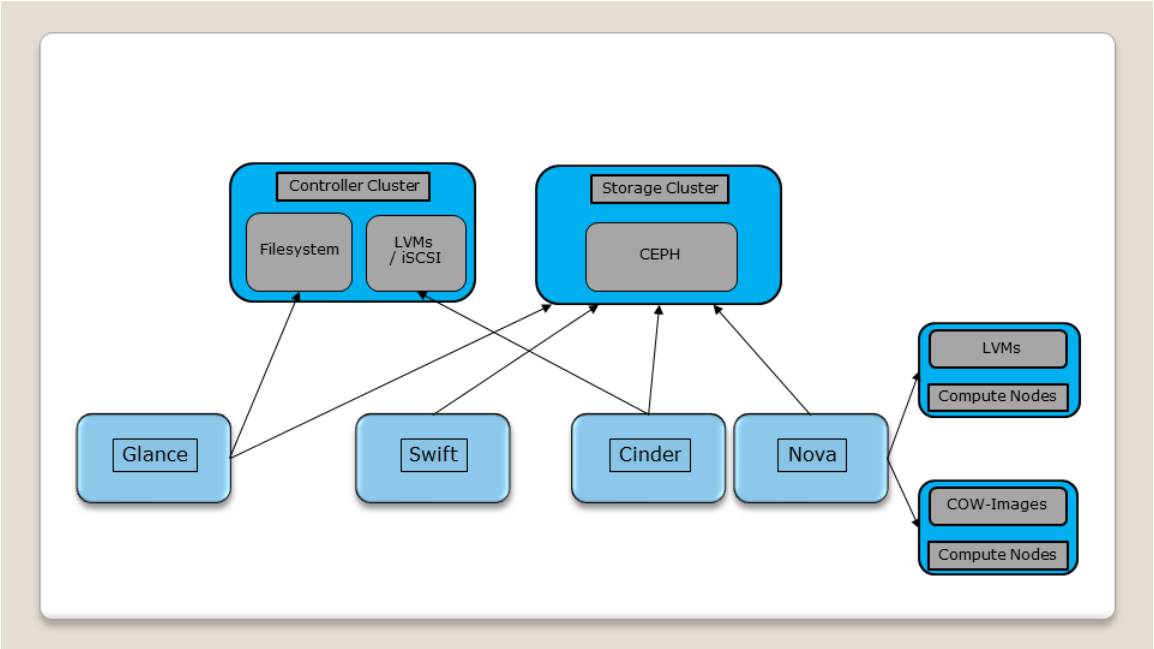
HCG 4.0 provides a range of storage options for flexibility and for scaling. Multiple storage services are supported simultaneously, including:

- Cinder
- Nova

- Swift
- Glance

The figure below shows the storage options and backends.

Figure 2: HCG 4.0 Storage Options and Backends



As shown in the figure above, the backends for each of these storage services include:

- Cinder - persistent HA-protected block storage for virtual disks
  - Backends:
    - LVM on Controller Nodes
    - CEPH on Storage Nodes
    - Remote EMC SAN Cluster
- Nova - ephemeral block storage for virtual disks
  - Backends:
    - LVM on Compute Nodes
    - COW-Image on Compute Nodes
    - CEPH on Storage Nodes
- Glance
  - Backends:

  - LVM
  - CEPH
- Swift
  - Backends:
    - CEPH

Related Links

Storage Tab on page 63
The **Storage** tab on the Inventory Detail page presents storage details for a host.

Storage on Controller Hosts

Controller hosts provide storage for the system database, and for system backup operations. On systems with controller storage, they also provide persistent storage for virtual machine images, using a secondary disk.
Controller storage is configured initially at installation, using the controller configuration script. To utilize the maximum available space on the storage media, it is recommended that you use the default settings. You can change the allocations at any time after installation. Controller hosts provide the following types of storage:

Database storage
: the storage allotment for the OpenStack database

Image storage
: for a system that provides LVM-backed controller storage for VMs, the size of the partition to use for image storage

Backup storage
: the storage allotment for backup operations

Volume storage
: for a system that provides LVM-backed controller storage for VMs, the storage allotment for all Cinder volumes used by guest instances; also called *Cinder storage*

Image Conversion Space
: the storage allotment for image caching and temporary image conversion

Ceph Mon Storage
: for a system using Ceph storage, the storage allotment on the controller for Ceph monitoring

NOTE: For clusters using a Ceph backend, volume storage and image storage are allotted on storage nodes, not on the controller node. To change the Cinder volume storage for a Ceph backend, see *Helion OpenStack Carrier Grade 4.0 System Administration: Replacing Storage Node Hardware on page 118*.

The storage allotments are configured initially during software installation. You can change them using the Web administration interface or the CLI. For more information, see *Helion OpenStack Carrier Grade 4.0 Administration:* *Increasing Storage Space Allotments on the Controller on page 127*).

To accommodate changes, there must be enough disk space on the controller, including headroom needed to complete the operation. The headroom required is 45 GiB on the primary disk for a cluster using controller storage with an LVM backend, or 65 GiB for a cluster using dedicated storage with a Ceph backend. This is in addition to the space required for any new allotments. The requested changes are checked against available space on the affected disks; if there is not enough, the changes are disallowed.

To provide more space, you can replace the affected disk or disks. Database, image, and backup storage use space on the primary disk. Cinder volume storage (on a cluster with an LVM backend) uses space on a disk selected by device node number during controller configuration. The replacement disk must occupy the same device node number. Changes to the Cinder volume storage can also affect the primary disk because of the headroom requirement.

Ceph monitor storage uses the primary disk by default. If a Ceph backend is added to an existing system, and there is insufficient space on the primary disk for the requested Ceph monitor storage, you can specify a secondary disk. Note that this requires a controller re-installation.

To pass the disk-space checks, any replacement disks must be installed before the allotments are changed.

Storage for System Use

Internal database storage is provided using DRBD-synchronized partitions on the controller primary disks. The size of the database grows with the number of system resources created by the system administrator and the tenants. This includes objects of all kinds such as compute nodes, provider networks, images, flavors, tenant networks, subnets, virtual machine instances, and NICs. As a reference point, consider the following deployment scenario:

- two controllers
- four compute nodes with dual Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz each.
- 40 virtual machine instances
- 120 tenant networks
- steady collection of power management statistics

The size of the database in this case is approximately 9 GB. With a suggested default of 20 GB, there is still plenty of room to grow. However, you should periodically monitor the size of the database to ensure that it does not become a bottleneck when delivering new services.

For more information, see *HCG 4.0 System Engineering Guidelines*.

Controller Storage

The active controller provides storage for the HCG 4.0, and if the system is configured for LVM-backed controller storage, for VM images and persistent volumes. Controller hosts provide the following types of storage:

Database storage

the storage allotment for the OpenStack database

Image storage

for a system that provides LVM-backed controller storage for VMs, the size of the partition to use for image storage

Backup storage

the storage allotment for backup operations

Volume storage

for a system that provides LVM-backed controller storage for VMs, the storage allotment for all Cinder volumes used by guest instances; also called *Cinder storage*

Image Conversion Space

the storage allotment for image caching and temporary image conversion

Ceph Mon Storage

for a system using Ceph storage, the storage allotment on the controller for Ceph monitoring

NOTE: For clusters using a Ceph backend, volume storage and image storage are allotted on storage nodes, not on the controller node. To change the Cinder volume storage for a Ceph backend, see Replacing Storage Node Hardware on page 118.

The storage allotments are configured initially during software installation. You can change them using the Web administration interface or the CLI. For more information, see Increasing Storage Space Allotments on the Controller on page 127).

To accommodate changes, there must be enough disk space on the controller, including headroom needed to complete the operation. The headroom required is 45 GiB on the primary disk for a cluster using controller storage with an LVM backend, or 65 GiB for a cluster using dedicated storage with a Ceph backend. This is in addition to the space required for any new allotments. The requested changes are checked against available space on the affected disks; if there is not enough, the changes are disallowed.

To provide more space, you can replace the affected disk or disks. Database, image, and backup storage use space on the primary disk. Cinder volume storage (on a cluster with an LVM backend) uses space on a disk selected by device node number during controller configuration. The replacement disk must occupy the same device node number. Changes to the Cinder volume storage can also affect the primary disk because of the headroom requirement.

Ceph monitor storage uses the primary disk by default. If a Ceph backend is added to an existing system, and there is insufficient space on the primary disk for the requested Ceph monitor storage, you can specify a secondary disk. Note that this requires a controller re-installation.

To pass the disk-space checks, any replacement disks must be installed before the allotments are changed.

Increasing Storage Space Allotments on the Controller

You can increase the allotments for controller-based storage at any time after installation.

CAUTION: Decreasing the file system size is not supported, and can result in synchronization failures requiring system re-installation. Do not attempt to decrease the size of the file system.

For more about controller-based storage, see Controller Storage on page 126.

If you prefer, you can use the CLI; see Increasing Storage Space Allotments on the Controller Using the CLI on page 130.

Prerequisites

Before changing storage allotments, prepare as follows:

- Calculate your system storage requirements using the *HCG 4.0 System Engineering Guidelines*. Include the headroom required for changes to the storage space allotments.
- Record the current configuration settings in case they need to be restored (for example, because of an unexpected interruption during changes to the system configuration). Consult the configuration plan for your system.
- Ensure that the BIOS boot settings for the host are appropriate for a reinstall operation. Changes to the storage allotments require a re-installation of the HCG 4.0 host software on the controllers, even if the primary disk is not replaced.

Procedure

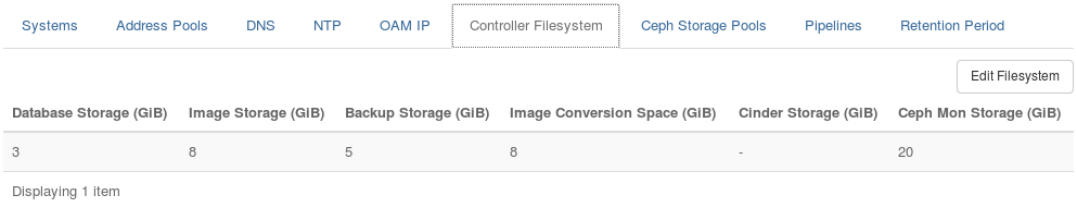
1. If necessary, install replacement disks in the controllers.

   If you do not need to replace disks, you can skip this step. To determine whether you need to replace disks, calculate your storage requirements using the *HCG 4.0 Engineering Guidelines*. Be sure to include the headroom required on the primary disk.

   To replace disks in the controllers, see Replacing Controller Hardware on page 105.

2. Edit the disk storage allotments.
   a) In the HCG 4.0 Web administration interface, open the System Configuration pane. The System Configuration pane is available from **Admin** > **Platform** > **System Configuration** in the left-hand pane.
   b) Select the **Controller Filesystem** tab.

      The Controller Filesystem page appears, showing the currently defined storage allotments.

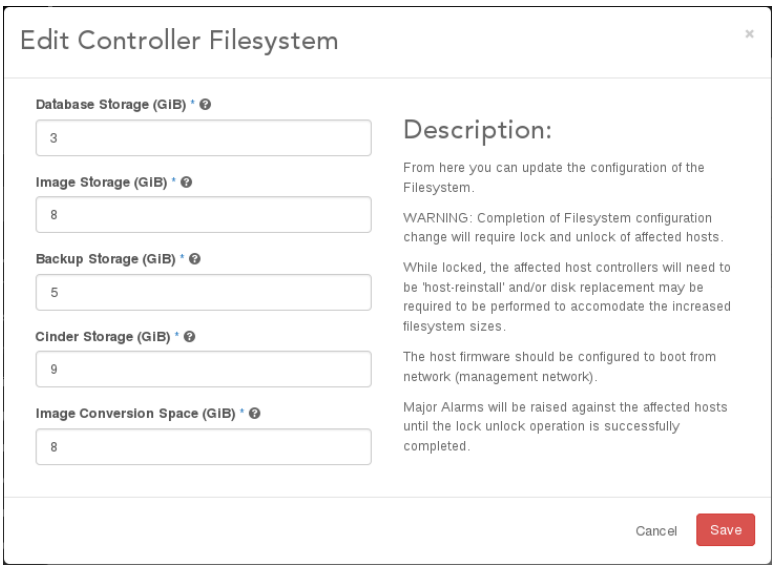


NOTE: Cinder Storage is shown only for systems with controller storage.

Ceph Mon Storage is shown only for systems with dedicated storage.

   c) Click **Edit Filesystem**.

      The Edit Controller Filesystem dialog box appears.



NOTE: The **Cinder storage (GiB)** field is present only for systems with controller storage.

A **Ceph Mon Storage (GiB)** field (not shown) is present for systems with dedicated storage.

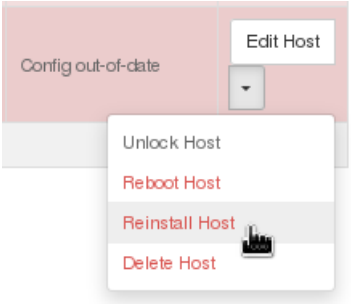
d) Replace the storage allotments as required.

e) Click **Save**.

This raises major alarms against the controllers (**250.001 Configuration out-of-date**). You can view the alarms on the Fault Management page. In addition, the status **Config out-of-date** is shown for the controllers in the Hosts list.

3. Lock the standby controller.

4. Re-install the HCG 4.0 software on the standby controller.



This step is required to update the system configuration, even if you have already re-installed the HCG 4.0 software as part of the disk replacement procedure.

The host is restarted and the operating system is re-installed; then the host is rebooted to the system prompt.

Wait for the standby controller to be reported as **Locked**, **Disabled**, and **Online**.

5. Unlock the standby controller.

Wait for the standby controller to be reported as **Unlocked**, **Enabled**, and **Available**.

The **Config out-of-date** status against the standby controller is cleared.

6. Swact the controllers.
   Open the drop-down menu for the active controller and select **Swact Host**.
   A **Swact: Request** is reported, followed by **Swact: In Progress**.
   During the swact, the Web administration interface is disconnected. Wait a few minutes for the swact to finish, and then log in again to resume the procedure.
   Under some circumstances, the **Config out-of-date** message for the new standby controller can be cleared by the swact. A host re-installation is still required to complete the procedure.
7. Lock the new standby controller.
8. Re-install the HCG 4.0 software on the controller.
9. Unlock the controller.
10. Confirm that the **250.001 Configuration out-of-date** alarms are cleared for both controllers.

Postrequisites

After making these changes, ensure that the configuration plan for your system is updated with the new storage allotments and disk sizes.

Increasing Storage Space Allotments on the Controller Using the CLI

You can use the CLI to view or increase the storage allotments for a controller.

⚠ **CAUTION:** Decreasing the file system size is not supported, and can result in synchronization failures requiring system re-installation. Do not attempt to decrease the size of the file system.

Before proceeding, review the prerequisites given for Increasing Storage Space Allotments on the Controller on page 127.

To view the existing storage configuration, use the following command.

```
~(keystone_admin)$ system controllerfs-show
    +--------------------+----------------------------------+
| Property             | Value                            |
+----------------------+----------------------------------+
| database_gib         | 10                               |
| cgcs_gib             | 10                               |
| backup_gib           | 30                               |
| img_conversions_gib  | 10                               |
| created_at           | 2016-10-27T20:10:24.307707+00:00 |
| updated_at           | None                             |
+----------------------+----------------------------------+
```

To change an allotment, use the following command syntax, where the allotments are in GiB.

```
~(keystone_admin)$ system controllerfs-modify \
database_gib=database_allotment \
image_gib=image_allotment \
backup_gib=backup_allotment \
cinder_gib=cinder_volume_allotment
```

For example:

```
~(keystone_admin)$ system controllerfs-modify \
database_gib=10 image_gib=13 backup_gib=22 action=apply
```

On a system with controller storage, you can modify the backend using the following command:

```
~(keystone_admin)$ system storage-backend-modify lvm_cinder_gib=cinder_volume_allotment
```

On a system with dedicated storage, you can modify the backend using the following command:

```
~(keystone_admin)$ system ceph-mon-modify controller
ceph_mon_gib=cinder_volume_allotment
```

After changing the controller storage configuration, you must lock each controller and re-install the HCG 4.0 software, even if you have already done so as part of changing the controller disks. You can use the following command:

```
~(keystone_admin)]$ system host-reinstall controller_name
```

Then you can unlock the controller to clear any **Configuration out-of-date** alarms. A controller swact is required to update both controllers.

Storage on Compute Hosts

Compute hosts provide local ephemeral storage for virtual machine (VM) disks.

This is the default type of storage for VM swap and ephemeral disks, and for boot-from-image root disks; you must configure this storage at installation before you can unlock a compute host. You can change the configuration after installation; for more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: Adjusting Resources on a Compute Node on page 109*. Note that live migration is not always supported for VM disks using this type of storage. For more information, seeVM Storage Settings for Migration, Resize, or Evacuation on page 159 .

On compute nodes, dedicated local storage space is required by the **nova** service. For flexibility and scalability, this space is implemented as a local volume group, called **nova-local**. The group can include one or more non-root disks as physical resources. Depending on whether LVM-backed or CoW-image-backed local storage is configured on the compute host, **nova-local** contains one or more volumes.

NOTE: As an alternative to LVM-backed local storage, compute hosts can be configured to offer image-backed local storage. For more information, see *Helion OpenStack Carrier Grade 4.0* System *Administration: Managing Local Volume Groups on page 133*.

The first volume in **nova-local** is called the *instances logical volume*, or **Instances LV**. It contains the **/etc/nova/instances** file system, and is used for the following:

- the nova image cache, containing images downloaded from Glance
- various small nova control and log files, such as the **libvirt.xml** file, which is used to pass parameters to **libvirt** at launch, and the **console.log** file
- on a host configured for CoW-image-backed local storage, the CoW image files that constitute the local disks for VMs

For CoW-image-backed local storage, the **Instances LV** is the only volume in **nova-local**. For LVM-backed local storage, additional volumes are required to realize local disks for VMs. To reserve space for these volumes, the size of the **Instances LV** must be appropriately configured.

By default, no size is specified for the **Instances LV**. The minimum required space is 2 GB for a **nova-local** volume group with a total size less that 80 GB, and 5 GB for a **nova-local** volume group larger or equal than 80 GB; you must specify at least this amount. You can allocate more **Instances LV** space to support the anticipated number of boot-from-image VMs, up to 50% of the maximum available storage of the local volume group. At least 50% free space in the volume group is required to provide space for allocating logical volume disks for launched instances. The value provided for the **Instance LV Size** is limited by this maximum.

Instructions for allocating the **Instances LV Size** using the Web administration interface or the CLI are included in *HCG 4.0 Installation* as part of configuring the compute nodes. For the command syntax, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Managing Local Volume Groups on page 133*.

CAUTION: If less than the minimum required space is available, the compute host cannot be unlocked.

Local Volume Groups

Local volume groups are used to designate one or more physical volumes on a compute host as collective storage space.

Local volume groups are used to designate one or more physical volumes on a compute host as collective storage space. HCG 4.0 uses one local volume group, called **nova-local**. This provides cache and file storage for the nova service, as well as disk storage for use by VMs. You can use the Web administration or the CLI to create this mandatory local volume group, and to change the settings.

NOTE: Use non-root disks exclusively for **nova-local** storage. Using a root disk to provide **nova-local** storage is not a supported configuration.

The exact storage implementation depends on the **Instance Backing** type. You can set this individually for each host to use local LVM or CoW-image backing, or remote Ceph backing on a system that uses storage hosts.

LVM and CoW backing use an *instances logical volume*, or **Instances LV** on the local compute node to hold the nova image cache and various nova control files. For CoW image backing, the **Instances LV** is also used to hold CoW-image disk files for use as VM disk storage. For LVM backing, separate volumes are used to provide VM disk storage. To ensure that enough space remains for this purpose, you must limit the **Instances LV Size**; suggested sizes are indicated in the Web administration interface. For more information about the Instances LV, see Storage on Compute Hosts on page 131.

Ceph backing uses a Ceph storage pool, configured from the storage-host resources on a Ceph system. For more information, see Ceph Storage Pools on page 148.

Compute hosts are grouped into host aggregates based on whether they offer LVM, CoW, or Ceph-backed storage. The host aggregates are used for instantiation scheduling. For more information, see *HCG 4.0 Tenant User's Guide: Host Aggregates*.

You can control whether a VM is instantiated with LVM, CoW, or Ceph-backed storage by setting a flavor extra specification. For more information, see Specifying the Storage Type for VM Ephemeral Disks on page 158.

Managing Local Volume Groups

You can add, delete, and review local volume groups on a compute host.

Prerequisites

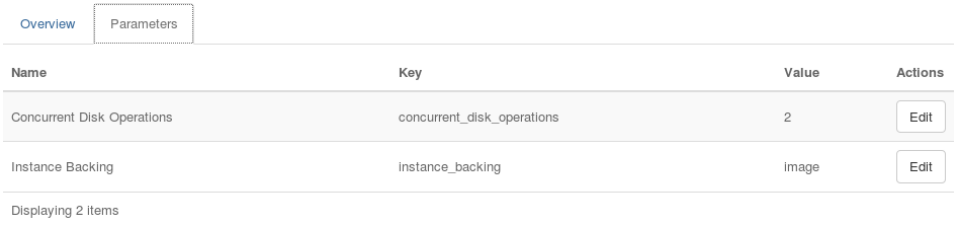
Before you can modify the settings for a host, you must lock the host:

```
~(keystone_admin)$ system host-lock hostname
```

Procedure

1. Lock the host.
2. Open the Storage page for the host.
3. In the **Local Volume Groups** list, click the **Name** of the group (**nova-local**).

   The settings are accessible on the **Parameters** tab of the Local Volume Group Detail page.



Managing Local Volume Groups Using the CLI

You can use CLI commands to manage local volume groups.

The following CLI commands are availabe for managing local volume groups:

```
~(keystone_admin)$ system host-lvg-list hostname

~(keystone_admin)$ system host-lvg-show hostname groupname

~(keystone_admin)$ system host-lvg-add hostname groupname

~(keystone_admin)$ system host-lvg-delete hostname groupname

~(keystone_admin)$ system host-lvg-modify [-b instance_backing] \
[-c concurrent_disk_operations] [-s size] hostname groupname
```

Where:

instance_backing

is the storage method for the local volume group (**lvm**, **image**, or **remote**)

concurrent_disk_operations

is the number of I/O intensive disk operations, such as glance image downloads or image format conversions, that can occur at the same time

size

is the space in MB to allot for instances logical volume space (specified only if the storage method is **lvm**)

hostname

is the name of the host

groupname

is the name of the local volume group

NOTE: The only valid **groupname** is **nova-local**. This parameter is *not* required for **system host-lvg-modify**.

Managing Physical Volumes on a Compute Host

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 more information, see the instructions for configuring a compute node in *HCG 4.0 Installation*.

As each physical volume is created, it is added to an existing local volume group.

Prerequisites

Before you can modify the settings for a host, you must lock the host:

```
~(keystone_admin)$ system host-lock hostname
```

Before you can add a physical volume, a local volume group must exist on the host. To create one, see Managing Local Volume Groups on page 133

The following CLI commands are available for managing physical volumes.

```
~(keystone_admin)$ system host-pv-add hostname groupname disk_uuid
```

where:

- **groupname** is the name of the local volume group to which the physical volume is added.

NOTE: The only valid **groupname** is **nova-local**.

- **disk_uuid** is the identifier of the disk to use.

CAUTION: For **nova-local** storage, use of the root disk is not a supported configuration.

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.

```
~(keystone_admin)$ system host-pv-delete hostname nova-local disk_uuid

~(keystone_admin)$ system host-pv-list hostname

~(keystone_admin)$ system host-pv-show hostname
```

NOTE: Commands related to physical volumes, such as **system host-pv-list**, apply to compute hosts only. They are intended for use when provisioning noval local storage. You can use **system host-disk-list** to obtain disk information for any type of node.

Storage on Storage Hosts

Storage hosts provide persistent and highly available storage for virtual machine (VM) images and disk volumes.

They can also be used to provide remote ephemeral storage for virtual machine disks, making live migration possible for VM ephemeral and swap disks, as well as boot-from-image root disks.

To use storage hosts, a HCG 4.0 with Ceph-backed storage is required. You can configure this at installation using the controller configuration script. On systems with controller-based storage, you can also add support for Ceph-backed storage later from the CLI; for more information, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Dedicated Storage for Systems Using Controller Storage on page 145*.

Storage hosts are paired for redundancy. On a system using Ceph-backed storage, at least one pair is required , and up to four pairs are supported. You can add up to eight object storage

devices (OSDs) per storage host for data storage. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: Provisioning Storage on a Storage Host on page 138*.

Space on the storage hosts must be configured at installation before you can unlock the hosts. You can change the configuration after installation by adding resources to existing storage hosts (see *Helion OpenStack Carrier Grade 4.0 System Administration: Replacing Storage Node Hardware on page 118*) or adding more storage hosts (see the installation procedure in the *HCG 4.0 Installation* document that pertains to your HCG 4.0 configuration).

HCG 4.0 creates default Ceph storage pools for images, volumes, ephemeral data, and object data. You can modify the storage pools after installation. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: Ceph Storage Pools on page 148*.

Storage hosts can achieve faster data access using SSD-backed transaction journals (*journal functions*) or additional hosts in a caching tier configuration, or both. Caching tier hosts overlay fast SSD-backed storage pools over the slower HDD-backed storage pools used in the standard backing tier.

NOTE: SSD-backed journals cannot be used on a storage host assigned to the caching tier.

Journal Functions

Each OSD on a storage host has an associated Ceph transaction journal, which tracks changes to be committed to disk for data storage and replication, and if required, for data recovery. This is a full Ceph journal, containing both metadata and data. By default, it is collocated on the OSD, which typically uses slower but less expensive HDD-backed storage. For faster commits and improved reliability, you can use a dedicated solid-state drive (SSD) installed on the host and assigned as a *journal function*. You can dedicate more than one SSD as a journal function.

NOTE: You can also assign an SSD for use as an OSD, but you cannot assign the same SSD as a journal function.

If a journal function is available, you can configure individual OSDs to use journals located on the journal function. Each journal is implemented as a partition. You can adjust the size and location of the journals. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: Storage Functions: OSDs and SSD-backed Journals on page 138*.

For OSDs implemented on rotational disks, it is strongly recommended that you use a journal function. For OSDs implemented on SSDs, collocated journals can be used with no performance cost.

Cache Tier

For systems where the same few data objects are accessed frequently, you can improve read-write times by implementing a cache tier. This uses a dedicated set of Ceph-caching storage hosts equipped with SSDs, in addition to a set of Ceph-backing storage hosts. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: Cache Tiering on page 152*.

NOTE: Since all disks on a caching host are SSDs, journal functions are neither required nor supported on caching-tier hosts.

HCG 4.0's cache tiering support is based on the Ceph cache tiering functionality. To ensure cache tiering is appropriate for your requirements, review the Ceph public documentation for caveats surrounding the use of this feature (http://docs.ceph.com/docs/master/rados/operations/cache-tiering/?highlight=tier#a-word-of-caution).

For valid HCG 4.0 storage cluster configurations when using cache tiering, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Valid Storage Cluster Configurations for Cache Tiering on page 156*

Storage Clusters (Replication Groups)

The storage hosts on Ceph systems are organized into clusters called *replication groups*.

Each replication group contains two hosts, referred to as *peers*. Each peer independently replicates the same data. For best performance, it is recommended to have a balanced storage capacity, in which each peer has sufficient resources to meet the operational requirements of the system.

Allocations for ephemeral, image, volume, and object storage are rebalanced dynamically to preserve redundancy and operational efficiency.

⚠ **CAUTION:** If one peer in a replication group is locked or goes out of service, replication is suspended, and a warning is added to the alarms list. New data is written to the unlocked peer only.

It is not possible to lock both peers in a replication group.

Replication groups are created automatically for each new storage pair. They are shown on the Hosts Inventory page, in association with the storage hosts. You can also use the following CLI commands to obtain information about replication groups:

```
~(keystone_admin)$ system cluster-list

+--------+-----------------+------+--------------+
| uuid   | cluster_uuid    | type | name         |
+--------+-----------------+------+--------------+
| 641... | 6414610c-482... | ceph | ceph_cluster |
|        |                 |      |              |
+--------+-----------------+------+--------------+


~(keystone_admin)$ system cluster-show

+--------------------+---------------------------------------- ...
| Property           | Value
+--------------------+----------------------------------------
| uuid               | 6414610c-482b-4703-9c1d-7c97fefae5a0
| cluster_uuid       | 6414610c-482b-4703-9c1d-7c97fefae5a0
| type               | ceph
| name               | ceph_cluster
| replication_groups | ["group-0:['storage-0', 'storage-1']",
+--------------------+---------------------------------------- ...

... ----------------------------------------+
                                            |
    ----------------------------------------+
                                            |
                                            |
                                            |
                                            |
     "group-1:['storage-3', 'storage-2']"] |
... ----------------------------------------+
```

Storage Clusters and Cache Tiering

When cache tiering is enabled, two types of replication groups are shown: **group-n** and **group-cache-n**, where *n* is the peer group number. You can use this information to identify peer hosts and to determine in which tier they reside.

NOTE: When adding a storage host, you must complete any incomplete peer group before starting a new peer group in a different tier. You cannot have an odd number of hosts in either tier.

Storage Functions: OSDs and SSD-backed Journals

Disks on storage hosts are assigned *storage functions* in HCG 4.0 to provide either OSD storage or Ceph journal storage.

Rotational disks on storage hosts are always assigned as object storage devices (OSDs) to provide storage for VM disks. Solid-state disks (SSDs) can be assigned as OSDs, or as *journal functions* to provide space for Ceph transaction journals associated with OSDs.

On systems configured for cache tiering, the hosts in the caching tier always use SSDs for high performance. The SSDs in this tier must be assigned as OSDs; they cannot be used for journal functions.

To assign storage-host disks as OSDs, see Provisioning Storage on a Storage Host on page 138. To create SSD-backed journals, see Adding SSD-backed Journals on page 142.

Provisioning Storage on a Storage Host

You can define object storage devices (OSDs) on storage hosts to provide VM disk storage.

For more about OSDs, see *Helion OpenStack Carrier Grade 4.0 System Administration: Storage on Storage Hosts on page 135*.

If you prefer, you can use the CLI. See Provisioning Storage on a Storage Host Using the CLI on page 140.

Prerequisites

To create or edit an OSD, you must lock the storage host. The system must have at least two other unlocked hosts with Ceph monitors. (Ceph monitors run on **controller-0**, **controller-1**, and **storage-0** only).

Procedure

1. Lock the host to prepare it for configuration changes.

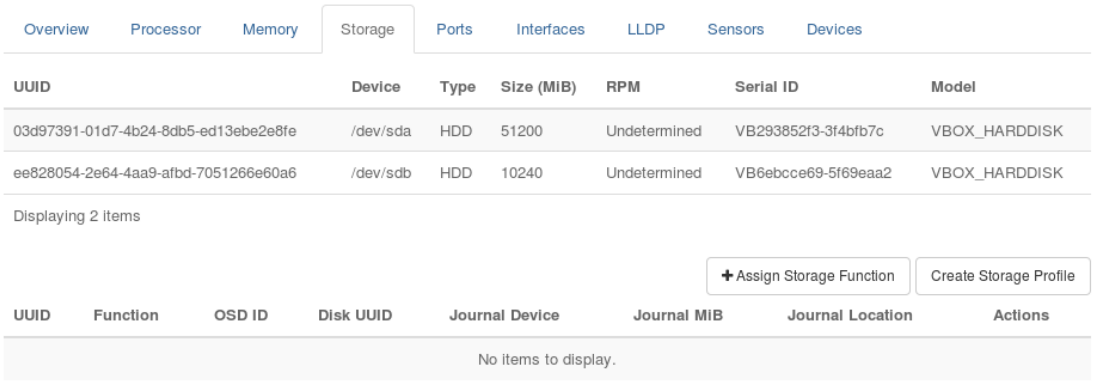
   On the **Hosts** tab of the Host Inventory page, open the drop-down list for the host, and then select **Lock Host**.

   The host is locked and reported as **Locked**, **Disabled**, and **Online**.

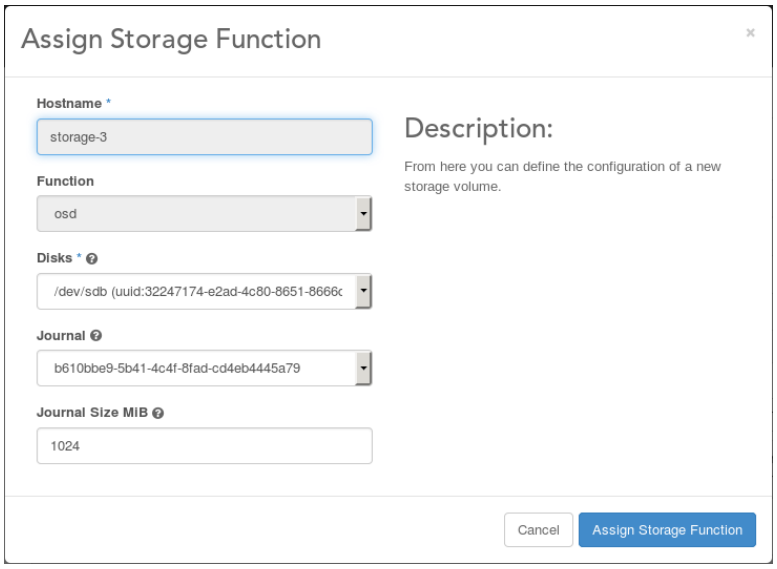
2. Open the Inventory Detail page for the host.

   To open the Inventory Detail page, click the name of the host on the **Hosts** tab of the System Inventory page.

3. Select the **Storage** tab to view the disks and storage functions for the node.



4. Add an OSD storage device.
   a) Click **Assign Storage Function** to open the Assign Storage Function dialog box.



   b) In the **Disks** field, select the OSD to use for storage.

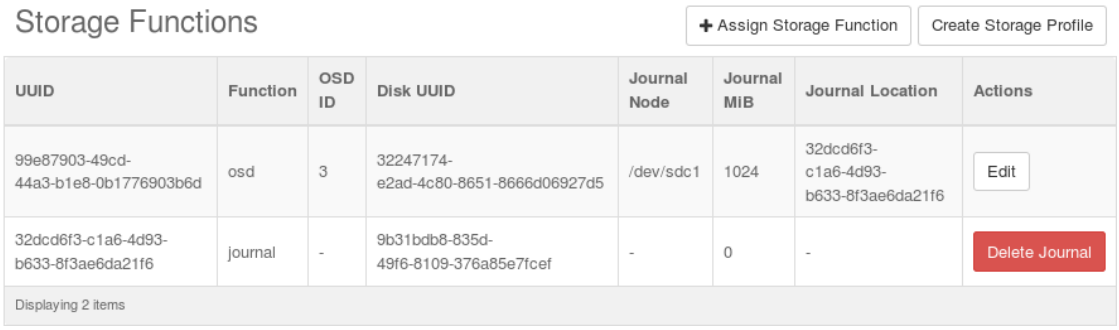
      You cannot use the rootfs disk (**dev/sda**) for storage functions.

   c) If applicable, specify the size of the Ceph journal.

      If an SSD-backed Ceph journal is available, the **Journal** for the OSD is automatically set to use the SSD device assigned for journals. For more about SSD-backed Ceph journals, see *Helion OpenStack Carrier Grade 4.0 System Administration: Adding SSD-backed Journals on page 142*. You can optionally adjust the **Journal Size**. For sizing considerations, refer to the *HCG 4.0 Engineering Guidelines*.

      If no journal function is configured on the host, then the **Journal** is set to **Collocated with OSD**, and the **Journal Size** is set to a default value. These settings cannot be changed.

The storage function is added.



5. Unlock the host to make it available for use.

   On the **Hosts** tab of the Host Inventory page, open the drop-down list for the host, and then select **Unlock Host**.

   The host is rebooted, and its **Availability State** is reported as **In-Test**. After a few minutes, it is reported as **Unlocked**, **Enabled**, and **Available**.

Postrequisites

You can re-use the same settings with other storage nodes by creating and applying a storage profile. See *HCG 4.0 Installation:Hardware Profiles*.

Provisioning Storage on a Storage Host Using the CLI

You can use the command line to define object storage devices (OSDs) on storage hosts.

For more about OSDs, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Storage on Storage Hosts on page 135*.

To use the Web administration interface, see Provisioning Storage on a Storage Host on page 138.

Prerequisites

To create or edit an OSD, you must lock the storage host. The system must have at least two other unlocked hosts with Ceph monitors. (Ceph monitors run on **controller-0**, **controller-1**, and **storage-0** only).

Procedure

1. List the available physical disks.

```
~(keystone_admin)$ system host-disk-list storage-3

+-------+-------------+------------+-------------+----------+------+-----------+
| uuid  | device_node | device_num | device_type | size_mib | rpm  | serial_id |
+-------+-------------+------------+-------------+----------+------+-----------+
| ba7...| /dev/sda    | 2048       | HDD         | 51200    | Un...| VB7127 .. |
| e87...| /dev/sdb    | 2064       | HDD         | 10240    | Un...| VB9987... |
| ae8...| /dev/sdc    | 2080       | SSD         | 8192     | N/A  | VB14d7... |
+-------+-------------+------------+-------------+----------+------+-----------+
```

2. Create a storage function (an OSD).

NOTE: You cannot add a storage function to the root disk (**/dev/sda** in this example).

```
~(keystone_admin)$ system host-stor-add host_name device_uuid \
[--journal-location journal_uuid] [--journal-size size]
```

where *device_uuid* identifies an OSD. For example:

```
~(keystone_admin)$ system host-stor-add storage-3 e8751efe-6101-4d1c-
a9d3-7b1a16871791
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| osdid            | 3                                    |
| state            | None                                 |
| function         | osd                                  |
| journal_location | e639f1a2-e71a-4f65-8246-5cd0662d966b |
| journal_size_mib | 1024                                 |
| journal_node     | /dev/sdc1                            |
| uuid             | fc7b2d29-11bf-49a9-b4a9-3bc9a973077d |
| ihost_uuid       | 4eb90dc1-2b17-443e-b997-75bdd19e3eeb |
| idisk_uuid       | e871b3a9-b436-47b0-b33b-88ce6dcbd967 |
| created_at       | 2016-06-02T20:23:40.298387+00:00     |
| updated_at       | 2016-06-02T20:23:40.522195+00:00     |
+------------------+--------------------------------------+
```

In this example, an SSD-backed journal function is available. For more about SSD-backed journals, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Storage Functions: OSDs and SSD-backed Journals on page 138*. The Ceph journal for the OSD is automatically created on the journal function using a default size of 1024 MiB. You can use the **--journal-size** option to specify a different size in MiB.

If multiple journal functions exist (corresponding to multiple dedicated SSDs), then you must include the **--journal-location** option and specify the journal function to use for the OSD. You can obtain the UUIDs for journal functions using the **system host-stor-list** command:

```
~(keystone_admin)$ system host-stor-list storage-3
+--------------------------------------+----------+-------+--------------...
| uuid                                 | function | osdid | capabilities
|                                      |          |       |
+--------------------------------------+----------+-------+--------------...
| e639f1a2-e71a-4f65-8246-5cd0662d966b | journal  | None  | {}
| fc7b2d29-11bf-49a9-b4a9-3bc9a973077d | osd      | 3     | {}
+--------------------------------------+----------+-------+--------------...

...+--------------------------------------+-------------+------------------+
   | idisk_uuid                           | journal_nod | journal_size_mib |
   |                                      | e           |                  |
... +--------------------------------------+-------------+------------------+
   | ae8b1434-d8fa-42a0-ac3b-110e2e99c68e | None        | 0                |
   | e871b3a9-b436-47b0-b33b-88ce6dcbd967 | /dev/sdc1   | 1024             |
... +--------------------------------------+-------------+------------------+
```

If no journal function exists when the storage function is created, the Ceph journal for the OSD is collocated on the OSD.

If an SSD is available on the host, you can add a journal function. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Adding SSD-backed Journals Using the CLI on page 144*. You can update the OSD to use a journal on the SSD by referencing the journal function UUID, as follows:

```
~(keystone_admin)$ system host-stor-update osd_uuid \
--journal-location journal_function_uuid [--journal-size size]
```

Postrequisites

Unlock the host to make the changes take effect. Wait for the host to be reported as unlocked, online, and available in the hosts list.

You can re-use the same settings with other storage nodes by creating and applying a storage profile. See *HCG 4.0 Installation: Managing Hardware Profiles Using the CLI*.

Adding SSD-backed Journals

On storage hosts with SSDs, you can use SSD-backed Ceph journals for improved I/O performance.

If you prefer, you can use the CLI. For more information, see Adding SSD-backed Journals Using the CLI on page 144.

For more information about SSD-backed journals, see Storage on Storage Hosts on page 135.

NOTE: SSD-backed journals cannot be used on a storage host assigned to the caching tier.

Prerequisites

A storage host with a solid-state drive (SSD) is required.

To create or edit an SSD-backed journal, you must lock the host. The system must have at least two other unlocked hosts with Ceph monitors. (Ceph monitors run on **controller-0**, **controller-1**, and **storage-0** only).

Procedure

1. Lock the host to prepare it for configuration changes.

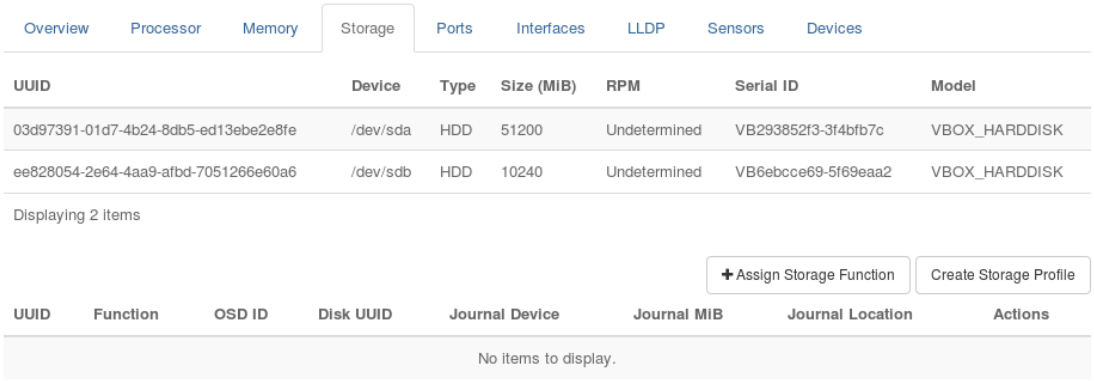
   On the **Hosts** tab of the Host Inventory page, open the drop-down list for the host, and then select **Lock Host**.

   The host is locked and reported as **Locked**, **Disabled**, and **Online**.

2. Open the Inventory Detail page for the host.

   To open the Inventory Detail page, click the name of the host on the **Hosts** tab of the Host Inventory page.

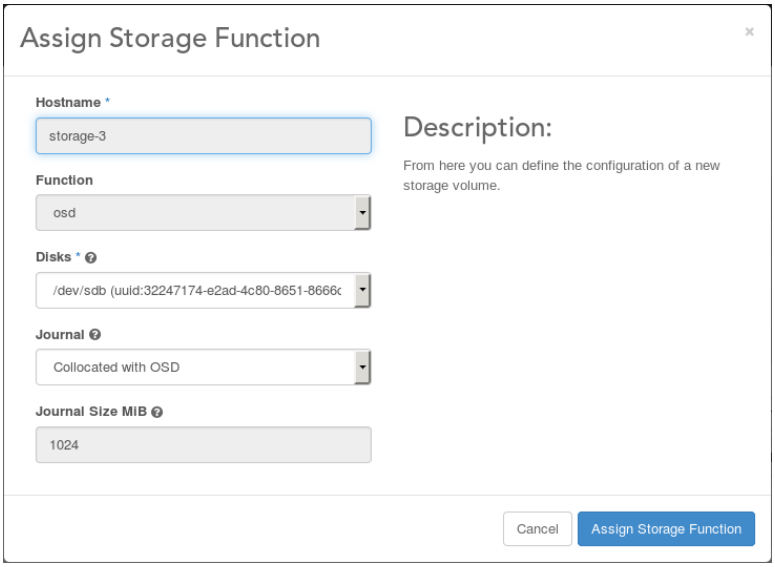
3. Select the **Storage** tab to view the **Disks** and **Storage Functions** for the node.



4. Assign the SSD to use for Ceph journals.

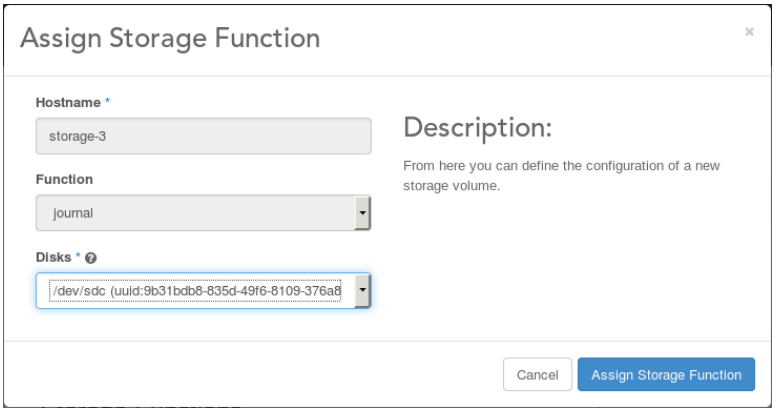
NOTE: This option is available only if the storage host is equipped with at least one SSD.

a) Click **Assign Storage Function** to open the Assign Storage Function dialog box.



b) In the **Function** field, select **Journal**.

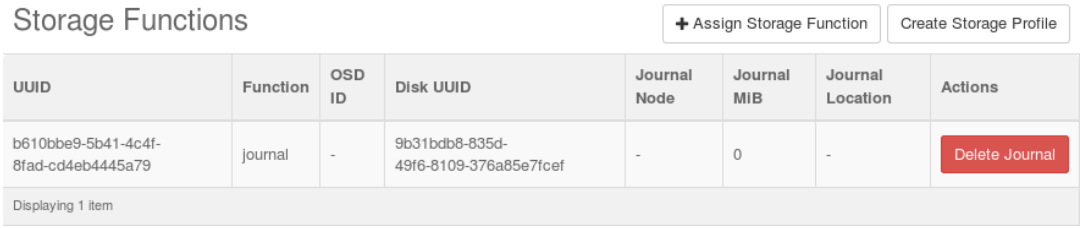
A simplified dialog is displayed.



c) In the **Disks** field, select the SSD device.

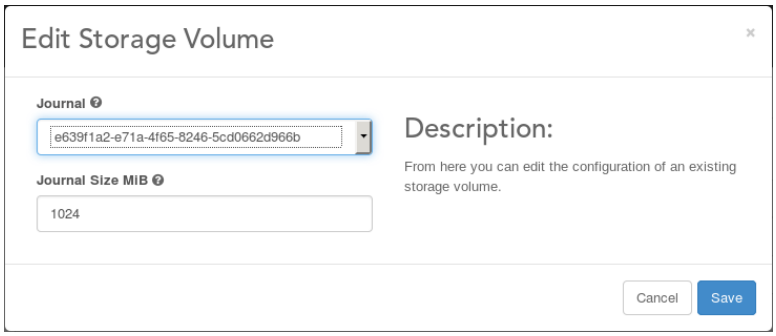
d) Click **Assign Storage Function**.

The journal function is assigned to the SSD.



5. Assign the journal function for use by one or more OSDs.

Use the **Edit** button for the OSD to open the Edit Storage Volume dialog box, and then select the **Journal** to use with the OSD.



6. Unlock the host to make it available for use.

   On the **Hosts** tab of the Host Inventory page, open the drop-down list for the host, and then select **Unlock Host**.

   The host is rebooted, and its **Availability State** is reported as **In-Test**. After a few minutes, it is reported as **Unlocked**, **Enabled**, and **Available**.

Adding SSD-backed Journals Using the CLI

You can use the command line to define SSD-backed journals.

For more about SSD-backed journals, see Storage on Storage Hosts on page 135.

To use the Web administration interface, see Adding SSD-backed Journals on page 142.

NOTE: SSD-backed journals cannot be used on a storage host assigned to the caching tier.

Prerequisites

A storage host with a solid-state drive (SSD) is required.

To create or edit an SSD-backed journal, you must lock the host. The system must have at least two other unlocked hosts with Ceph monitors. (Ceph monitors run on **controller-0**, **controller-1**, and **storage-0** only).

Procedure

1. List the available physical disks.

```
~(keystone_admin)$ system host-disk-list storage-3

+-------+-------------+------------+-------------+----------+------+-----------+
| uuid  | device_node | device_num | device_type | size_mib | rpm  | serial_id |
+-------+-------------+------------+-------------+----------+------+-----------+
| ba7...| /dev/sda    | 2048       | HDD         | 51200    | Un...| VB7127 .. |
| e87...| /dev/sdb    | 2064       | HDD         | 10240    | Un...| VB9987... |
| ae8...| /dev/sdc    | 2080       | SSD         | 8192     | N/A  | VB14d7... |
+-------+-------------+------------+-------------+----------+------+-----------+
```

2. Create a journal function.

Use the **system host-stor-add** command:

```
~(keystone_admin)$ system host-stor-add host_name journal device_uuid
```

where *host_name* is the name of the storage host (for example, storage-3), and *device_uuid* identifies an SSD.

For example:

```
~(keystone_admin)$ system host-stor-add storage-3 journal
ae885ad3-8be7-4103-84eb-93892d7182da
|------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| osdid            | None                                 |
| state            | None                                 |
| function         | journal                              |
| journal_location | None                                 |
| journal_size_mib | 0                                    |
| journal_node     | None                                 |
| uuid             | e639f1a2-e71a-4f65-8246-5cd0662d966b |
| ihost_uuid       | 4eb90dc1-2b17-443e-b997-75bdd19e3eeb |
| idisk_uuid       | ae8b1434-d8fa-42a0-ac3b-110e2e99c68e |
| created_at       | 2016-06-02T20:12:35.382099+00:00     |
| updated_at       | None                                 |
+------------------+--------------------------------------+
```

3. Update one or more OSDs to use the journal function.

```
~(keystone_admin)$ system host-stor-update osd_uuid \
--journal-location journal_function_uuid [--journal-size size]
```

Postrequisites

Unlock the host to make the changes take effect. Wait for the host to be reported as unlocked, online, and available in the hosts list.

Dedicated Storage for Systems Using Controller Storage

On systems that do not already have it, you can add dedicated Ceph storage for Cinder volumes and Glance images at any time after installation.

HCG 4.0 can be configured at installation to use different types of storage backends. If you choose to install it with a backend other than Ceph, you can add Ceph storage later. This provides an additional backend for Cinder volumes and Glance images.

If a Ceph backend is present, it is used by default for new images or volumes. Existing volumes and images are unaffected by the addition of a Ceph backend, and continue to use their existing backends.

For a new image, you can specify a different backend manually by including the **--store** parameter with the **glance image-create** command, and setting its value to **file** (for an LVM backend) or **rbd** (for a Ceph backend).

For a new volume, you can specify a backend manually by referencing a volume type when using **cinder create**. The volume type must be defined in advance using **cinder type-create**, and then associated with a backend using **cinder type-key**. For complete information, refer to the public OpenStack documentation.

To add Ceph storage to a system, you must use CLI commands. This operation is not supported from the Web administration interface.

As part of the new Ceph storage, a Ceph monitor logical volume is created. By default, it uses space on the rootfs disk of the controller. If the rootfs disk does not have enough free space, an additional disk is required (the disk assigned for Cinder volumes cannot be used for this purpose). To add disks to a controller, see Replacing Controller Hardware on page 105.

The size of the Ceph monitor volume is shown in the **CEPH Mon Storage (GiB)** field on the **Controller Filesystem** tab, accessible from the **Admin** > **System** > **System Configuration** page of the Web administration interface. You can change the size using the CLI or the Web administration interface. For more information, see Increasing Storage Space Allotments on the Controller on page 127.

Ceph storage also requires an infrastructure network. To add one, see Adding an Infrastructure Network on page 16.

NOTE: You cannot add Ceph storage to a HCG 4.0 CPE system.

Adding Ceph Storage

You can add Ceph storage to a system using the CLI. This operation is not available from the Web administration interface.

For more information about adding Ceph storage, see Dedicated Storage for Systems Using Controller Storage on page 145.

CAUTION: Once you start configuring the Ceph backend, do not perform any other installation or reconfiguration activities such as patching or upgrade until all compute nodes are reconfigured successfully.

Prerequisites

- a standard HCG 4.0 configuration, not HCG 4.0 CPE
- an infrastructure network
- no other ongoing installation or configuration activities (such as patching or upgrade activities)
- at least 20 GiB free space for the Ceph monitor on the controller primary disk or an additional disk

Procedure

1. If the system does not already have one, add an infrastructure network.

   For details, see Adding an Infrastructure Network on page 16.

2. Estimate whether there is enough space on the primary disk for the Ceph monitor logical volume.

   a) List the space on the rootfs drive used for database, image, backup, and image conversion:

```
~(keystone_admin)$ system controllerfs-show
    +--------------------+----------------------------------+
| Property           | Value                            |
+--------------------+----------------------------------+
| database_gib       | 10                               |
| cgcs_gib           | 10                               |
| backup_gib         | 30                               |
| img_conversions_gib | 10                               |
```

```
| created_at           | 2016-10-27T20:10:24.307707+00:00 |
| updated_at           | None                             |
+----------------------+----------------------------------+
```

b) Calculate the space already used on the rootfs disk.

(**database_gib** x 2) + **image_gib** + **backup_gib** + **img_conversions_gib** = **space_used**

(3 x 2) + 8 + 5 + 8 = 27

- Double the **database_gib** space, to allow for space reserved for upgrade operations.
- Do not include **cinder_gib**, which uses space on the Cinder volume.

c) Subtract the **space_used** from the total available disk space, allowing at least 5 additional GiB of physical disk space for losses related to drive sectoring.

(**disk_size_gib** - 5) - **space_used** = **space_available**

50 - 5 - 27 = 18

If the **space_available** is less than the minimum 20 GiB requirement for the Ceph monitor, you must use another disk on the controller (you cannot use the Cinder disk for this purpose). To add a disk, see Replacing Controller Hardware on page 105.

3. On the active controller, become the Keystone **admin** user.

4. On the active controller, run the CLI command to add the Ceph backend.

Use a command of the following form:

```
~(keystone_admin)$ system storage-backend-add ceph \
[--ceph-mon-gib partition_size] [--ceph-mon-dev device_name]
```

where

partition_size

is the size of the partition to allocate on a controller disk for the Ceph monitor logical volume, in GiB (the default value is 20)

device_name

is the device to use on each controller (for example, **/dev/sdc**)

NOTE: If you need to specify a different device on each controller, you can use an alternative form of the command:

```
~(keystone_admin)$ system storage-backend-add ceph \
[--ceph-mon-gib partition_size] \
[--ceph-mon-dev-controller-0 disk_uuid1 --ceph-mon-dev-controller-1 disk_uuid2]
```

where

disk_uuid1

is the unique identifier for the **controller-0** disk to use

disk_uuid2

is the unique identifier for the **controller-1** disk to use

---

For example:

```
~(keystone_admin)$ system storage-backend-add ceph --ceph-mon-dev /dev/sdc

WARNING : THE OPERATION IS NOT REVERSIBLE AND CANNOT BE CANCELLED.
By continuing this operation, CEPH backend will be created.
Minimum 2 storage nodes are required to complete the configuration.
Please refer to hardware guide for minimum spec for storage nodes.

Continue [yes/N]: yes
System configuration has changed. Please follow the administrator guide to complete
configuring system.

+---------+-------------+---------------------+
| backend | state       | task                |
+---------+-------------+---------------------+
| ceph    | configuring | reconfig-controller |
| lvm     | configured  | None                |
+---------+-------------+---------------------+
```

If you omit the **ceph-mon-dev** option, the default rootfs disk is used for the Ceph monitor.

If there is not enough space on the specified disk, an error message appears.

```
Total target configured size 47 GigaBytes for database_gib (doubled for upgrades),
image_gib, img_conversions_gib, backup_gib and ceph_mon_gib exceeds limit of 45
GigaBytes.
```

Specify a smaller partition size, or use the **ceph-mon-dev** option to specify another disk.

This command starts the process of adding a Ceph storage backend. Both controllers are marked as **Config out-of-date Reboot Required** in the Web administration interface.

5. Lock and unlock each controller to apply the configuration.
   a) Lock and unlock the standby controller.

      Wait for the controller to be reported as **Unlocked**, **Available**, and **Online**.

   b) Swact the controllers.

   c) Lock and unlock the new standby controller.

      Wait for the controller to be reported as **Unlocked**, **Available**, and **Online**.

6. Add storage hosts **storage-0** and **storage-1**, and unlock them. For complete instructions, see *HCG 4.0 Installation for Ceph-backed Systems: Installing Software on Controller-1 or a Compute or Storage Host* .

   Once both storage hosts are unlocked, the system enables a Ceph-monitor check process, which ensures that at least two Ceph monitors are available at all times.

7. Add more storage-host pairs as required, up to the maximum supported by the system (four pairs).

Ceph Storage Pools

On a system that uses a Ceph storage backend, storage pools for images, volumes, ephemeral data, and object data are configured on the storage hosts.

HCG 4.0 uses four pools:

- Cinder Volume Storage pool
- Glance Image Storage pool
- Nova Ephemeral Disk Storage pool
- Swift Object Storage pool

These pools share the available Ceph storage provided by the storage host resources.

Initial quotas for each pool are defined during system installation. Within the bounds of these quotas, storage for each of the pools is allocated dynamically as required. To optimize resource usage, you can adjust the quota on each pool. The sum of the quotas must equal the total available space in gibibytes (GiB).

If you set a quota to **0**, the quota is deactivated. The pool size is not restricted, and can grow to fill the entire available storage space.

If you set the quota to less than its current size, new space allocation requests are served only after the pool size drops below the new ceiling.

If you set quotas so that the total value exceeds the available Ceph storage, restrictions on all allocation requests are removed.

To view and change the size of the storage pools, see Changing Ceph Storage Pool Sizes on page 149.

NOTE: To increase the available storage, you can also add storage hosts, up to a maximum of four pairs. For instructions, see *HCG 4.0 Installation for Ceph-backed Systems: Installing Software on Controller-1 or a Compute or Storage Host*.

Changing Ceph Storage Pool Sizes

You can use the Web administration interface to adjust the storage pool quotas on a Ceph-based system.

For more information about storage pools, see Ceph Storage Pools on page 148.

If you prefer, you can use the CLI to make changes; see Changing Ceph Storage Pool Sizes Using the CLI on page 151.

Prerequisites

Before changing storage pool sizes, review the Fault Management page and ensure that any existing system alarms are cleared.

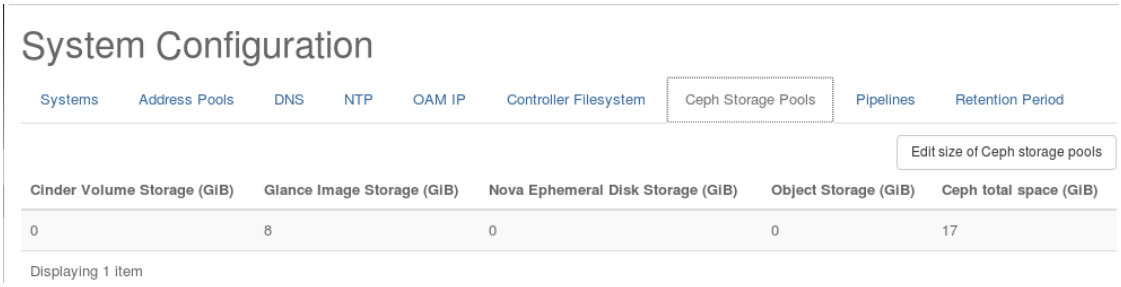
Procedure

1. In the HCG 4.0 Web administration interface, open the System Configuration page.

   The System Configuration page is available from **Admin** > **Platform** > **System Configuration** in the left-hand pane.

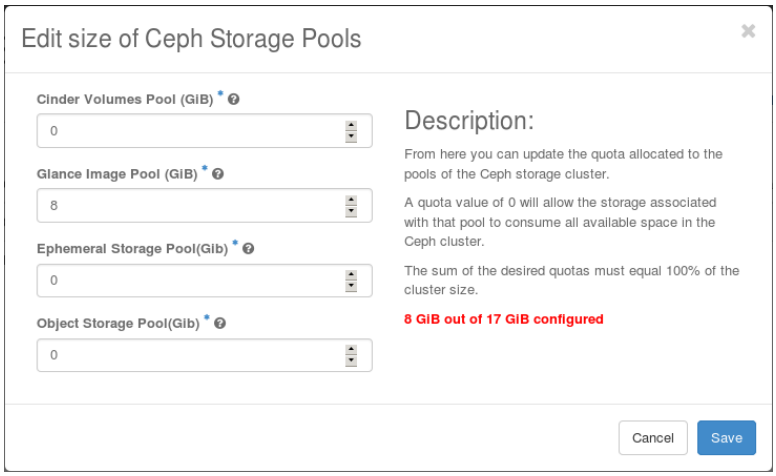
2. Select the **Ceph Storage Pools** tab.

   The Ceph Storage Pools page appears, showing the currently defined pools and their sizes.



3. Click **Edit size of Ceph storage pools**.

   The Edit size of Ceph Storage Pools dialog box appears.



4. Edit the pool settings as required.

NOTE: A value of **0** deactivates the quota. The Glance Image Pool size is not restricted in any way when its value is configured to **0** and can grow to fill the entire available storage space.

Setting a Glance Image Pool size that is less than the current storage space allocated to the Glance Image Pool does not have an adverse effect on the system; space allocation requests are served only after the pool size drops under the new ceiling.

Setting the Glance Image Pool size bigger than all existing Ceph storage space removes restrictions on all allocation requests.

In the event that the storage system/Ceph is unavailable, the **Save** action fails and an error message is displayed. The old value is used when Ceph becomes available again.

5. Click **Save**.

Changing Ceph Storage Pool Sizes Using the CLI

You can use the CLI to adjust the storage pool quotas on a Ceph-based system.

Prerequisites

Before changing storage pool sizes, review the Fault Management page and ensure that any existing system alarms are cleared.

On a system that uses a Ceph storage backend, storage pools for images and volumes are configured from the available space on the storage hosts during installation, using a default value of 20 GB.

For more information about storage pools, see Ceph Storage Pools on page 148.

If you prefer, you can use the Web administration interface to make changes; see Changing Ceph Storage Pool Sizes on page 149.

To view pool sizes, use the following command:

```
$ system storage-backend-show ceph

+--------------------+--------------------------------------+
| Property           | Value                                |
+--------------------+--------------------------------------+
| cinder_pool_gib    | 10                                   |
| glance_pool_gib    | 20                                   |
| ephemeral_pool_gib | 0                                    |
| object_pool_gib    | 0                                    |
| ceph_total_space   | 30                                   |
| object_gateway     | False                                |
| created_at         | 2016-03-15T04:54:44.311120+00:00     |
| updated_at         | 2016-03-15T08:00:18.031909+00:00     |
+--------------------+--------------------------------------+
```

To set pool quotas, use a command of the following form:

```
~(keystone_admin)$ system storage-backend-modify ceph \
[glance_pool_gib=size] \
[cinder_pool_gib=size] \
[ephemeral_pool_gib=size] \
[object_pool_gib=size
```

Where *size* is the size of the associated storage pool in GiB. You must ensure that the pools for Glance + Cinder + Ephemeral + Object = 100% of available storage.

For example:

```
$ system storage-backend-modify ceph cinder_pool_gib=20 glance_pool_gib=10

+--------------------+--------------------------------------+
| Property           | Value                                |
+--------------------+--------------------------------------+
| cinder_pool_gib    | 20                                   |
| glance_pool_gib    | 10                                   |
| ephemeral_pool_gib | 0                                    |
| object_pool_gib    | 0                                    |
| ceph_total_space   | 30                                   |
| object_gateway     | False                                |
| created_at         | 2016-03-15T04:54:44.311120+00:00     |
| updated_at         | 2016-03-15T08:00:18.031909+00:00     |
+--------------------+--------------------------------------+
```

Cache Tiering

You can use cache tiering to improve read-write performance for frequently accessed objects.

When cache tiering is enabled, Ceph storage for the cluster is divided into a *cache tier* and a *storage tier*. Each tier uses a pool of dedicated storage hosts, designated as either **Ceph caching** or **Ceph backing** hosts at installation. For valid cluster configurations, see Valid Storage Cluster Configurations for Cache Tiering on page 156.

NOTE: SSD-backed journals cannot be used on a storage host assigned to the caching tier.

The cache tier is implemented on storage hosts with SSDs to provide fast read-write performance. Data is migrated to the cache tier when it is needed, maintained there for read-write operations, and removed when it is no longer required. Modified objects are removed to the storage tier (*flushed*), and unmodified objects are discarded (*evicted*). These operations are managed automatically by the *Ceph objecter*, which determines which tier to use for an object, and the *cache tiering agent*, which handles data migration between the tiers.

The decision to flush modified objects takes into account the percentage of total available space used by modified objects (the *dirty ratio*). The decision to evict unmodified objects takes into account the percentage of total available space used by unmodified objects (the *cache_target_full_ratio*).

Normally cache tiering operates in *writeback mode*, in which data is migrated to the cache tier when needed, and then written back to the storage tier. It can also operate in *read-proxy mode*, in which data is never migrated to the cache tier; if it is not already in the cache tier, then the storage tier is used for read-write operations. Read-proxy mode is useful for draining a cache in order to disable it.

CAUTION: Cache tiering can degrade performance in systems where many objects are accessed frequently, by introducing thrashing. It is more useful in situations where only a few objects receive a high number of requests. To ensure that cache tiering is appropriate for your requirements, review the Ceph public documentation for caveats surrounding the use of this feature:

http://docs.ceph.com/docs/master/rados/operations/cache-tiering/?highlight=tier#a-word-of-caution)

Cache tiering uses *hit sets* to determine whether an object belongs in the cache tier. A hit set is a set of all recent access requests. When configuring a cache tier, you can specify hit set parameters, including the length of time covered by the hit set (the *hit set period*), the number of hit sets to retain for analysis (the *hit set count*), and the filtering method for identifying eligible objects (the *hit set type*).

Configuring Cache Tiering

You can configure the parameters for cache tiering from the command line.

This procedure is required before you can add a Ceph tiering storage host.

Basic information is provided here. For help selecting parameter values for optimal performance, refer to the *HCG 4.0 Engineering Guidelines*. For additional parameters and configuration information, consult the public Ceph documentation.

Procedure

1. Specify the number of hit sets to include for analysis.

   A hit set is a set of access requests used to identify frequently accessed objects.

   ```
   ~(keystone_admin)$ system service-parameter-add ceph cache_tiering \
   hit_set_count=count
   ```

   where *count* is the number of hit sets to retain and use.

2. Specify the length of time covered by each hit set.

   ```
   ~(keystone_admin)$ system service-parameter-add ceph cache_tiering \
   hit_set_period=period
   ```

   where *period* is the duration in seconds.

3. Specify the filtering method for identifying frequently accessed objects.

   A filter is applied to the hit sets to determine which objects belong in the cache tier. Currently the only supported method is Bloom filtering.

   ```
   ~(keystone_admin)$ system service-parameter-add ceph cache_tiering \
   hit_set_type=bloom
   +----------+--------------------------------------+
   | Property | Value                                |
   +----------+--------------------------------------+
   | uuid     | 2a9223d6-1e18-42de-bb06-7241ff8c5423 |
   | service  | ceph                                 |
   | section  | cache_tiering                        |
   | name     | hit_set_type                         |
   | value    | bloom                                |
   +----------+--------------------------------------+
   ```

4. Specify the percentage of total available space used by modified objects that triggers flushing of modified objects to the storage pool.

   ```
   ~(keystone_admin)$ system service-parameter-add ceph \
   cache_target_dirty_ratio=dirty-ratio
   ```

   where *dirty-ratio* is the percentage expressed as a decimal value (0.0 to 1.0).

5. Specify the percentage of total available space used by unmodified objects that triggers eviction of unmodified objects from the cache.

   ```
   ~(keystone_admin)$ system service-parameter-add ceph \
   cache_target_full_ratio=full-ratio
   ```

   where *full-ratio* is the percentage expressed as a decimal value (0.0 to 1.0).

6. Enable the cache tiering feature.

   ```
   ~(keystone_admin)$ system service-parameter-modify ceph \
   cache_tiering feature_enabled=true
   +----------+--------------------------------------+
   | Property | Value                                |
   +----------+--------------------------------------+
   | uuid     | 95881e60-4049-486e-9df2-f6de6f5819ce |
   | service  | ceph                                 |
   | section  | cache_tiering                        |
   | name     | feature_enabled                      |
   ```

```
| value     | true                                  |
+-----------+---------------------------------------+
```

7. Apply the service parameter changes.

```
~(keystone_admin)$ system service-parameter-apply ceph

Applying ceph service parameters
```

Postrequisites

After cache tiering is configured on the system, you can add storage hosts configured for Ceph caching. For valid cluster configurations, see Valid Storage Cluster Configurations for Cache Tiering on page 156.

Monitoring and Tuning Cache Tiering

To ensure optimal cache tiering performance, you must monitor the system regularly and adjust the cache pool configurations as needed.

The HCG 4.0 implementation of cache tiering allows the feature to be enabled or disabled easily. You must adjust the initial configuration for your system requirements, and monitor and tune the system performance at regular intervals.

For best results:

- Monitor the pool usage statistics daily using the **ceph df detail** command. For more information, consult the public Ceph documentation.
- Tune the pools individually after initial setup.

  During initial setup, the available pools are configured globally with default settings by the **system service-parameter** command. You must adjust the settings for each pool individually.

  images-cache

  the Glance image storage pool

  cinder-volumes-cache

  the Cinder block storage pool

  ephemeral-cache

  the Nova storage pool

  .rgw.buckets-cache

  the Swift object storage pool

For each pool, you must tune the following parameters:

- **target_max_bytes**

  NOTE: This value is calculated when the cache is enable, based on the size of the cache tier and the quotas for the corresponding backing tier pool. It is not set (and cannot be set) globally using the **system service-parameter** command.

- **target_max_objects**

You must set this value to ensure that deleted objects are evicted from the caching tier and the backing tier. If this parameter is not set, then the backing pool may to become full due to undeleted objects.

NOTE: This value is not set (and cannot be set) globally using the **system service-parameter** command.

- **cache_min_flush_age**
- **cache_min_evict_age**
- **cache_target_dirty_ratio**
- **cache_target_full_ratio**

You can tune these parameters using the **ceph osd pool set** and **ceph osd pool get** commands. For more information, consult the public Ceph documentation.

The following example adjusts the target_max_bytes setting for the **images-cache** pool as part of a cache purge:

- Get the current setting:

```
~(keystone_admin)$ ceph osd pool get images-cache target_max_bytes
~(keystone_admin)$ target_max_bytes: 9312209408
```

- Set it (along with other parameters, not shown) to initiate a cache purge:

```
~(keystone_admin)$ ceph osd pool set images-cache target_max_bytes 0
~(keystone_admin)$ set pool 6 target_max_bytes to 0
```

- Restore the setting (along with others, not shown) to re-enable the cache:

```
~(keystone_admin)$ ceph osd pool set images-cache target_max_bytes 9312209408
~(keystone_admin)$ set pool 6 target_max_bytes to 9312209408
```

Troubleshooting Notes for Cache Tiering

Incorrect cache pool tuning can result in a variety of monitoring and performance issues.

- Promotion, flushing, or eviction operations occur before the associated thresholds are crossed

  This can appear to happen because the cache tiering agent relies on statistics for individual placement groups within the pool, rather than on the statistics for the pool as a whole as shown in the **ceph df detail** command. No corrective action is required.

- Backing tier pool quota changes are denied

  This can happen because of a discrepancy between the backing data and the cache data during regular operations, due to normal transaction delays.

  You can correct this by tuning the pool parameters to lower the backing tier pool usage below the desired quota.

- I/O activity is blocked by a full backing pool

  Blocked I/O activity can present itself in a variety of ways, such as failed instance launches, failed volume creations, VM freezes, or other issues related to storage access. This can happen when high activity levels cause a backlog of objects to be deleted in the backing tier, and the unreleased objects consume all available space.

You can correct this by manually purging the cache, and then reinstating the caching parameters, in particular the **target_max_object** parameter, using more appropriate values.

CAUTION: Purging the cache can take several hours, depending on the size of the cache tier pool, the amount of data to be flushed or evicted, and the current cache client I/O rate.

The following example flushes or evicts the cache so that the backing pool is updated on the outstanding transactions taken by the caching pool.

NOTE: Prior to performing this operation, save the current values so that you can use them to re-enable the cache.

```
~(keystone_admin)$ ceph osd pool set pool target_max_bytes 0
~(keystone_admin)$ ceph osd pool set pool target_max_objects 1
~(keystone_admin)$ ceph osd pool set pool cache_min_flush_age 0
~(keystone_admin)$ ceph osd pool set pool cache_min_evict_age 0
~(keystone_admin)$ ceph osd pool set pool cache_target_dirty_ratio 0
~(keystone_admin)$ ceph osd pool set pool cache_target_full_ratio 0
```

- Writes are allowed in excess of the backing pool quota

  To ensure that the cache tier does not provide additional storage beyond the backing pool limits prior to flushing, configure the cache tier for write-through operation.

Valid Storage Cluster Configurations for Cache Tiering

For cache tiering, specific storage host cluster configurations are supported.

Total Storage Hosts	Caching Tier Hosts	Backing Tier Hosts
2	0	2
4	0	4
	2	2
6	0	6
	2	4
8	0	8
	2	6
	4	4

Block Storage for Virtual Machines

Virtual machines use HCG 4.0 storage resources for root and ephemeral disks. You can allocate root disk storage for virtual machines using the following:

- a Cinder volume
- ephemeral storage; one of
  - ephemeral local storage on compute nodes, backed by LVM
  - ephemeral local storage on compute nodes, backed by image file
  - ephemeral remote storage on storage nodes, backed by Ceph

The use of a Cinder volume or ephemeral storage is determined by the **Instance Boot Source** setting when an instance is launched. **Boot from volume** results in the use of a Cinder volume, while **Boot from image** results in the use of ephemeral storage

Cinder-backed persistent storage for virtual machines is provided using either Ceph-backed OSD disks on high-availability storage hosts, or LVM-backed, DRBD-synchronized controller secondary disks on systems that do not use storage hosts.

For a controller-based LVM Cinder backend, you can configure HCG 4.0 at installation to use thin or thick provisioning. Thin provisioning allocates space for the volume dynamically on the underlying physical disk. Thick provisioning creates a fixed-size volume. Thin provisioning offers support for fast secure deletion, but requires longer volume creation times. You can improve volume creation times by using SSDs for the underlying disks.

⚠ **CAUTION:** The choice of thick or thin provisioning cannot be changed after installation.

Ephemeral storage for virtual machines, including swap disk storage, ephemeral disk storage, and root disk storage if the **Instance Boot Source** is set to **Boot from Image**, is by default provided locally on the compute nodes where the VMs are instantiated (local ephemeral storage). On Ceph systems, you can change this configuration to use storage node resources instead (remote ephemeral storage).

On each individual compute host, you can configure the ephemeral storage to use:

- a local LVM-based backend, to optimize run-time I/O performance
- a CoW (Copy on Write) sparse-image-format backend, to optimize launch and delete performance
- a Ceph backend (on a system with storage nodes), to optimize migration capabilities

The ephemeral storage type is defined during installation, and can be modified using the Web administration interface or the CLI. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration Guide:* *Managing Local Volume Groups on page 133* .

⚠ **CAUTION:** Unlike Cinder-based storage, ephemeral storage does not persist if the instance is terminated or the compute node fails.

In addition, for local ephemeral storage, migration and resizing support depends on the storage backing type specified for the instance, as well as the boot source selected at launch.

The choice of storage type affects migration behavior. For more information, see VM Storage Settings for Migration, Resize, or Evacuation on page 159.

Specifying the Storage Type for VM Ephemeral Disks

You can specify the ephemeral storage type for virtual machines (VMs) by using a flavor with the appropriate extra specification.

Each new flavor is automatically assigned a Storage Type extra spec that specifies, as the default, instantiation on compute hosts configured for image-backed local storage (**Local CoW Image Backed**). You can change the extra spec to specify instantiation on compute hosts configured for LVM-backed local storage (**Local LVM Backed**) or Ceph-backed remote storage, if this is available (**Remote Storage Backed**). Ceph-backed remote storage is available only on systems configured with a Ceph storage backend.

The designated storage type is used for ephemeral disk and swap disk space, and for the root disk if the virtual machine is launched using boot-from-image. Local storage is allocated from the Local Volume Group on the host, and does not persist when the instance is terminated. Remote storage is allocated from a Ceph storage pool configured on the storage host resources, and persists until the pool resources are reallocated for other purposes. The choice of storage type affects migration behavior; for more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: VM Storage Settings for Migration, Resize, or Evacuation on page 159*.

If the instance is configured to boot from volume, the root disk is implemented using persistent Cinder-based storage allocated from the controller (for a system using LVM) or from storage hosts (for a system using Ceph).

To specify the type of storage offered by a compute host, see *Helion OpenStack Carrier Grade 4.0 System Administration: Managing Local Volume Groups on page 133*.

⚠ **CAUTION:** Unlike Cinder-based storage, ephemeral storage does not persist if the instance is terminated or the compute node fails.

In addition, for local ephemeral storage, migration and resizing support depends on the storage backing type specified for the instance, as well as the boot source selected at launch.

To change the storage type using the Web administration interface, click **Edit** for the existing **Storage Type** extra specification, and select from the **Storage** drop-down menu. To access the extra specification, see *Helion OpenStack Carrier Grade 4.0 Cloud Administration: Flavor Extra Specifications*.

⚠ **CAUTION:** If the **Storage Type** extra spec is not specified, the VM can be instantiated on any host. To ensure that instantiated VMs use storage of a known type, do not delete this extra spec.

You can also specify the extra spec from the CLI by setting the following parameter for a flavor:

```
aggregate_instance_extra_specs:storage=storage_type
```

where *storage_type* is one of the following:

local_lvm

Specifies hosts with LVM-backed local storage for use by the VM.

local_image

Specifies hosts with image-backed local storage for use by the VM.

remote

Specifies hosts with Ceph-backed remote storage for use by the VM.

For example:

```
~(keystone_admin)$ nova flavor-key flavor_name \
set aggregate_instance_extra_specs:storage=local_image
```

The local storage key is added by default on flavor creation and set for **local_image** storage.

VM Storage Settings for Migration, Resize, or Evacuation

The migration, resize, or evacuation behavior for an instance depends on the instance boot configuration and the type of ephemeral storage used.

The following table summarizes the boot and local storage configurations needed to support various behaviors.

Instance Boot Type and Ephemeral and Swap Disks from flavor	Local Storage Backing	Live Migration with Block Migration	Live Migration w/o Block Migration	Cold Migration	Local Disk Resize	Evacuation
From Cinder Volume (no local disks)	N/A	N	Y	Y	N/A	Y
From Cinder Volume (w/ remote Ephemeral and/or Swap)	N/A	N	Y	Y	N/A	Y
From Cinder Volume (w/ local Ephemeral and/or Swap)	LVM	N	N	Y Ephemeral/ Swap data loss	Y Data loss if to new node	Y Ephemeral/ Swap data loss
	CoW	N	N	Y	Y	Y Ephemeral/ Swap data loss
From Glance Image (all flavor disks are local)	LVM	N	N	Y Local disk data loss	Y Data loss if to new node	Y Local disk data loss
	CoW	Y	N	Y	Y	Y Local disk data loss
From Glance Image (all flavor disks are	LVM	N	N	Y Local disk data loss	Y Data loss if to new node	Y Local disk data loss

Instance Boot Type and Ephemeral and Swap Disks from flavor	Local Storage Backing	Live Migration with Block Migration	Live Migration w/o Block Migration	Cold Migration	Local Disk Resize	Evacuation
local + attached Cinder Volumes)	CoW	N	N	Y	Y	Y Local disk data loss

NOTE: The **Local Storage Backing** is a consideration only for instances that use local ephemeral or swap disks.

The boot configuration for an instance is determined by the **Instance Boot Source** selected at launch. For more information, see *Helion OpenStack Carrier Grade 4.0 Tenant User's Guide: Launching Virtual Machine Instances*.

The type of ephemeral-disk storage backing used by an instance is determined by a flavor extra specification. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration: Specifying the Storage Type for VM Ephemeral Disks on page 158*.

Swift Object Storage

Systems with dedicated storage hosts can provide object storage using OpenStack Swift. VMs and system users can use this to store and exchange Ceph-backed files.

Swift object storage uses *Swift containers*. These are similar to directories in a file system, except that they cannot be nested. However, each Swift container can contain areas called *folders*, which you can use to organize content. Hierarchies of folders are supported.

VMs and OpenStack users (including OpenStack services) can create Swift containers for public or private use, and then access them for file uploads and downloads.

In HCG 4.0, a storage pool implemented on Ceph-backed storage hosts is used to hold Swift containers and objects. The pool is created when the Swift service is started. For VMs, this offers a place to store files that persist independently and can be exchanged with other VMs or with the HCG 4.0 platform.

You can add Swift support from the command line at any time after installation. For more information, see *Helion OpenStack Carrier Grade 4.0 System Administration:Configuring Swift Object Storage on page 161*.

System administrators and tenant users can manage Swift containers and their contents from the CLI or the Web administration interface. VMs can use a Swift client or the Swift REST API to manage and access Swift containers and objects. For more information, consult the public OpenStack documentation.

Configuring Swift Object Storage

On systems with dedicated storage hosts, you can configure Swift object storage for use by VMs at any time after installation.

For more information, see Swift Object Storage on page 160.

Prerequisites

Storage hosts are required to support Swift.

The storage cluster must be healthy for Swift support to be configured.

Procedure

1. Log in to the active controller as the Keystone **admin** user.
2. Ensure that the Ceph storage backend is configured.

```
~(keystone_admin)$ system storage-backend-list
+---------+------------+------+
| backend | state      | task |
+---------+------------+------+
| ceph    | configured | None |
+---------+------------+------+
```

3. Ensure that the Ceph cluster is healthy.

```
~(keystone_admin)$ ceph -s

    cluster 720283dd-f14e-40d7-a3b5-ec0ca3ccde95
    health HEALTH_WARN
           too many PGs per OSD (2100 > max 2048)
    monmap e1: 3 mons at
{controller-0=192.168.205.3:6789/0,controller-1=192.168.205.4:6789/0,storage-0=192.1
68.205.5:6789/0}
           election epoch 14, quorum 0,1,2 controller-0,controller-1,storage-0
    osdmap e33: 2 osds: 2 up, 2 in
     pgmap v869: 2100 pgs, 10 pools, 1970 MB data, 1409 objects
           4058 MB used, 14351 MB / 18409 MB avail
               2100 active+clean
```

4. Add a Ceph Object Gateway backend.

   The Ceph Object Gateway (RADOS Gateway) supports Swift client or Swift REST API access.

```
~(keystone_admin)$ system storage-backend-modify ceph object_gateway=true
+----------------------+----------------------------------+
| Property             | Value                            |
+----------------------+----------------------------------+
| cinder_pool_gib      | 0                                |
| glance_pool_gib      | 8                                |
| ephemeral_pool_gib   | 0                                |
| object_pool_gib      | 0                                |
| ceph_total_space_gib | 17                               |
| object_gateway       | True                             |
| created_at           | 2016-09-21T18:19:17.981485+00:00 |
| updated_at           | 2016-09-22T13:57:40.165109+00:00 |
+----------------------+----------------------------------+

System configuration has changed.
Please follow the administrator guide to complete configuring the system.
```

   Config out-of-date alarms are raised on both controllers.

5. Confirm that the new backend is queued for configuration.

```
~(keystone_admin)$ system storage-backend-list
+---------+------------+--------------------+
| backend | state      | task               |
+---------+------------+--------------------+
| ceph    | configured | add-object-gateway |
+---------+------------+--------------------+
```

6. Lock and unlock the controllers to make the configuration take effect.

   a) Lock the standby controller.

      Wait for the lock operation to be completed.

   b) Unlock the standby controller.

      Wait for the host to become available. Its configuration is updated, and its error message is cleared.

   c) Perform a swact on the active controller.

      Click **Edit Host** > **Swact Host** > for the active controller.

      Web administration access is interrupted, and the HCG 4.0 login screen appears. Wait briefly for the Web service to stabilize, and then log in again.

   d) Lock the original controller (now in standby mode).

      Wait for the lock operation to be completed.

   e) Unlock the original controller.

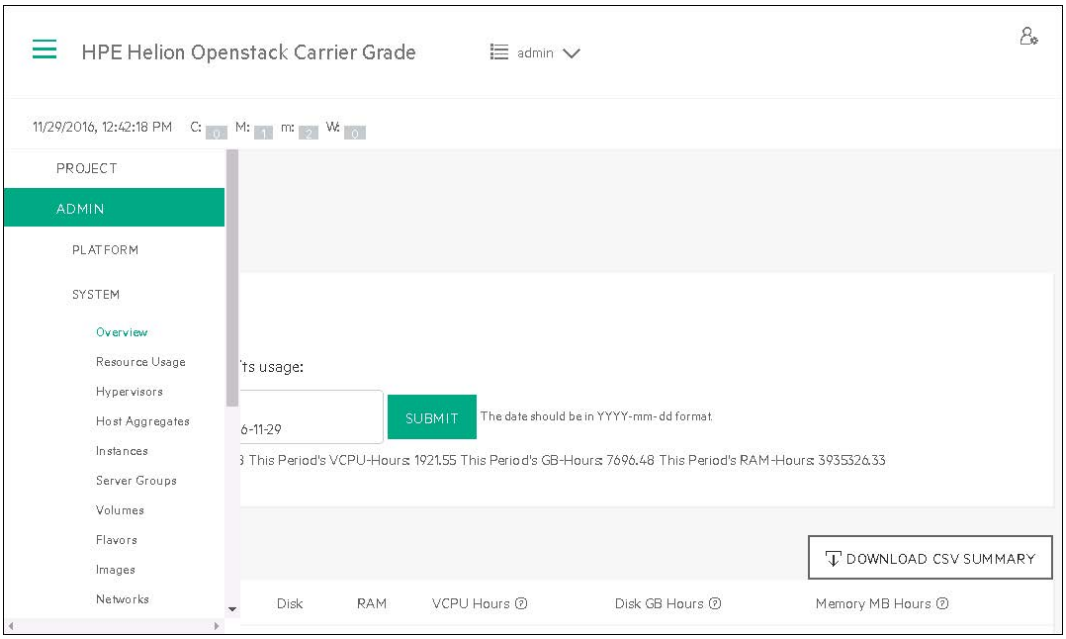
      Wait for it to become available. Its configuration is updated, and its error message is cleared.

7. At the command line, confirm that object storage is configured.

```
~(keystone_admin)$ system storage-backend-list
 +---------+------------|------+
 | backend | state      | task |
 +---------------------+------+
 | ceph    | configured | none |
 +---------+------------|------+
```

Swift storage is configured on the system.

In the Web administration interface, the **Object Store** selection is added to the Project menu. Allow about two minutes for this update to be propagated, and then log into the Web administration interface again.



NOTE: The **Object Store** selection does not appear until the next time you log in to the Web administration interface.

Storage Profiles

A storage profile is a named configuration for a list of storage resources on a storage node or compute node.

Storage profiles for storage nodes are created using the **Create Storage Profile** button on the storage node Inventory Detail page.

Storage profiles for compute nodes are created using the **Create Storage Profile** button on the compute node Inventory Detail page.

Storage profiles are shown on the **Storage Profiles** tab on the Host Inventory page.

Each storage resource consists of the following elements:

Name

This is the name given to the profile when it is created.

Disk Configuration

A Linux block storage device, such as **/dev/sdb**, identifying an entire hard drive.

Storage Configuration

This field provides details on the storage type. The details differ depending on the intended type of node for the profile.

Profiles for storage nodes indicate the type of storage backend, such as **osd**.

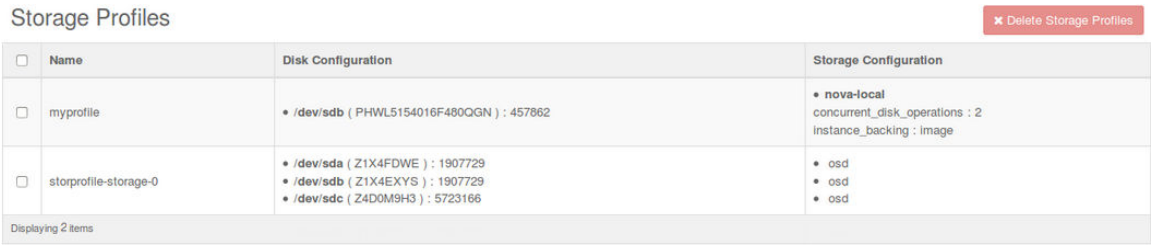
Profiles for compute nodes provide details for the **nova-local** volume group used for instance local storage. The details include the local storage backing type (LVM or CoW-Image), and for LVM-backed local storage, the size of the Instances LV volume. The maximum number of concurrent disk operations supported is also shown; this is for information only, and is not user-adjustable.

NOTE: Storage profiles for compute-based or CPE ephemeral storage (that is, storage profiles containing volume group and physical volume information) can be applied in two scenarios:

- on initial installation where a nova-local volume group has not been previously provisioned
- on a previously provisioned host where the nova-local volume group has been marked for removal

On a previously provisioned host, delete the nova-local volume group prior to applying the profile.

The example Storage Profiles screen below lists a storage profile that uses the hard drive **/dev/sdb** for image-backed **nova-local** storage, suitable for compute hosts, and a storage profile that uses hard drives **/dev/sda**, **/dev/sdb**, and **/dev/sdc** for **osd** storage, suitable for storage hosts.



To delete storage profiles, select the check boxes next to the profile names, and then click **Delete Storage Profiles**. This does not affect hosts where the profiles have already been applied.

Storage-related CLI Commands

You can use CLI commands when working with storage.

Modify CEPH Monitor Volume Size

You can change the space allotted for the Ceph monitor, if required. For considerations affecting Ceph monitor storage, refer to the *HCG 4.0 Systems Engineering Guidelines*.

```
~(keystone_admin)$  system ceph-mon-modify controller ceph_mon_gib=size
```

where *partition_size* is the size in GiB to use for the Ceph monitor. The value must be between 20 and 40 GiB.

```
~(keystone_admin)$  system ceph-mon-modify controller-0 ceph-mon-gib=20

+--------------------------------------+---------+-------+--------------+
| uuid                                 | device_ | ceph_ | hostname     |
|                                      | node    | mon_g |              |
|                                      |         | ib    |              |
+--------------------------------------+---------+-------+--------------+
| 3007f58c-c212-480a-8cde-e3e8922ec3da | None    | 35    | controller-0 |
| 4346814a-df7b-4de2-b70c-a02eafd6280f | None    | 35    | controller-1 |
+--------------------------------------+---------+-------+--------------+

NOTE: ceph_mon_gib for both controllers are changed.
```

```
System configuration has changed.
Please follow the administrator guide to complete configuring system.
```

List Storage Backend

You can use this command to list the storage backend types installed on a system.

```
~(keystone_admin)$  system storage-backend-list

+---------+------------+------+
| backend | state      | task |
+---------+------------+------+
| lvm     | configured | None |
+---------+------------+------+
| ceph    | configured | None |
+---------+------------+------+
```

NOTE: The value **rbd** (RADOS block device) indicates a Ceph backend for Glance images.

Display File System

You can use the **system controllerfs show** command to view the storage space allotments on a host.

```
~(keystone_admin)$  system controllerfs-show
+--------------------+----------------------------------+
| Property           | Value                            |
+--------------------+----------------------------------+
| database_gib       | 10                               |
| cgcs_gib           | 10                               |
| backup_gib         | 30                               |
| img_conversions_gib | 10                               |
| created_at         | 2016-10-27T20:10:24.307707+00:00 |
| updated_at         | None                             |
+--------------------+----------------------------------+
```

For a system with controller storage:

```
~(keystone_admin)$  system storage-backend-show lvm
+---------------+----------------------------------+
| Property      | Value                            |
+---------------+----------------------------------+
| cinder_device | /dev/sdb                         |
| cinder_gib    | 110                              |
| created_at    | 2016-10-27T20:10:24.304134+00:00 |
| updated_at    | None                             |
+---------------+----------------------------------+
```

For a system with dedicated storage:

```
~(keystone_admin)$  system ceph-mon-show controller-0
+--------------+--------------------------------------+
| Property     | Value                                |
+--------------+--------------------------------------+
| uuid         | cc038848-a3ff-4039-9637-9242d499b243 |
| device_node  | None                                 |
| ceph_mon_gib | 20                                   |
| created_at   | 2016-09-27T20:44:28.452379+00:00     |
| updated_at   | None                                 |
+--------------+--------------------------------------+
```

List Glance Images

You can use this command to identify the storage backend type for Glance images. (The column headers in the following example have been modified slightly to fit the page.)

```
~(keystone_admin)$  glance -v image-list
+----+------+-------+--------+-----------+------+--------+------------+-----------+
| ID | Name | Store | Disk   | Container | Size | Status | Cache Size | Raw Cache |
|    |      |       | Format | Format    |      |        |            |           |
+----+------+-------+--------+-----------+------+--------+------------+-----------+
| .. | img1 | rbd   | raw    | bare      | 1432 | active |            |           |
| .. | img2 | file  | raw    | bare      | 1432 | active |            |           |
+----+------+-------+--------+-----------+------+--------+------------+-----------+
```

NOTE: The value **rbd** indicates a Ceph backend.

Show Glance Image

You can use this command to obtain information about a Glance image.

```
~(keystone_admin)$  glance image-show <image-id>
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| checksum         | c11edf9e31b416c46125600ddef1a8e8     |
| name             | ubuntu-14.014.img                    |
   .  .   .
| store            | rbd                                  |
| owner            | 05be70a23c81420180c51e9740dc730a     |
+------------------+--------------------------------------+
```

The Glance **store** value can be either **file** or **rbd**. The **rbd** value indicates a Ceph backend.

6

Security

Overview of HCG 4.0 Security

HCG 4.0 provides a broad number of features related to system security.

- HCG 4.0 protects the availability and reliability of platform infrastructure nodes by:
  - monitoring and recovering critical platform processes on all nodes
  - monitoring and reacting to resources on all nodes.
- HCG 4.0 protects the connectivity and availability of the platform cluster by:
  - implementing a robust 1:1 HA Controller Node Cluster
  - real-time monitoring and reacting to connectivity between all platform nodes
  - optional HTTPS protocol on an OAM network
  - configurable firewall on an OAM network

- HCG 4.0 protects the availability and reliability of the Hypervisor using:
  - real-time monitoring and recovery of the KVM/QEMU Hosting Container
- HCG 4.0 protects and ensures the authenticity of HCG 4.0 code base through:
  - Controller Node Services Program Store signature validation
- HCG 4.0 controls access to tenant data and prevents tampering:
  - Guest VM volumes are accessible only through private closed network
  - Guest VM volumes are mountable by one and only one VM

Confidentiality

- HCG 4.0 protects internal HCG 4.0 private information:
  - a Keyring Database is used for storage of encrypted passwords
- HCG 4.0 ensures authenticity and privacy of tenant and infrastructure communication:
  - ACL filters of authenticity of connectivity to Guest VMs
  - optional VM Source MAC Filtering (anti-MAC-spoofing)
  - quality-of-service (QoS) for protection of connectivity to Guest VMs, dropping lower priority traffic in denial-of-service (DoS) attacks

AAA

- Linux Access
  - Local LDAP for Centralized Management of Linux User Accounts
    - User Account Distribution across all nodes
  - support for secure passwords (for example, mininmum length, upper/lower characters, numbers, and special characters)
  - support for password aging
  - restricted access to the root account after initial installation
  - restricted shell for non-root accounts
  - configurable pre-login and post-login warning messages
  - auto-logout of local and SSH connections after a period of inactivity
  - account usage is logged for liability purposes
- OpenStack Access
  - SSL support for both Web server and OpenStack REST APIs to for authentication and data encryption
  - auto-logout of GUI after a period of inactivity
  - leverages Keystone key management infrastructure
    - supporting a default local database backend
    - supporting a remote LDAP backend

Licensing and Authentication

Licenses and CA-certificates are initially specified at installation time using the **config_controller** wizard and must be properly maintained and updated.

Updating a License

You can update a license by copying the new license file to a directory on the active controller host, and then running the **license-install** utility as shown in the following example:

```
$ sudo /usr/sbin/license-install license_file
```

WARNING: It is recommended that you update licenses before they expire. Manual recovery of VMs may be required if the license is upgraded after expiry.

Operational Behavior with Expired or Invalid Licenses

HCG 4.0 and HCG 4.0 CPE assume the operational behavior described below when an expired or invalid license is detected.

Mismatched licenses are considered invalid. For example, a HCG 4.0 license is considered an invalid license if the server is installed and provisioned as a HCG 4.0 CPE product.

Expired and invalid licenses cause the following behavior:

1. A service log (401.003) is logged every 1 hour.
2. A service alarm (400.003) is triggered 8 hours after the expired or invalid license is detected, and every 1 hour thereafter.
3. 72 hours after the expired or invalid license is detected for the first time, the controller stops service.

Updating a digital certificate

You can update a CA-signed or self-signed certificate by copying the new certificate to a directory on the active controller host, and then running the **https-certificate-install** utility as shown in the following example:

```
$ sudo /usr/sbin/https-certificate-install pem_file
```

Linux User Accounts

Linux user accounts are available on all hosts for administration and operation.

Linux user accounts have no inherent relation to OpenStack Keystone user accounts. For more about Keystone accounts, see OpenStack Accounts on page 176.

In HCG 4.0, you can set up Linux accounts with simplified and secure access for Keystone users using a built-in script. For more information, see Creating LDAP Linux Accounts for OpenStack Users on page 173.

Remote Access for Linux Accounts

You can log in remotely as a Linux user using SSH. You can specify the OAM floating IP address as the target to establish a connection to the currently active controller. However, if the OAM floating IP address moves from one controller node to another, the SSH session is blocked. To ensure access to a particular controller regardless of its current role, specify the controller physical address instead.

NOTE: Password-based access to the root account is not permitted over remote connections. To log in as root over SSH, you must first configure a key pair as described in Verifying the Controller Identity for Secure SSH Access on page 174.

The wrsroot Account

This is a local, per-host, account created automatically when a new host is provisioned. On controller nodes, this account is available even before the **config_controller** script is executed.

The default initial password is **wrsroot**.

- The initial password must be changed immediately when you log in to each host for the first time. For details, see *HCG 4.0 Installation*.
- After five consecutive unsuccessful login attempts, further attempts are blocked for approximately five minutes.

Additionally, you can configure an **Aging** value for the **wrsroot** password. This value constitutes the maximum number of days after which the **wrsroot** password expires, and therefore has to be changed. While this configuration is optional, it is recommended from a system security standpoint. An **Aging** value can be configured as follows:

- During initial system installation and provisioning, either through the **config_controller** script, or off-box **configutils**. For more information, see the *HCG 4.0 Software Development Kit: wrs-configutilities—Configuration Utilities*.
- On an active system using standard Linux commands, such as:

```
$ chage -M new age wrsroot
```

NOTE: When the **wrsroot** aging is changed using the Linux command on the active controller, a **config-out-of-sync** alarm is generated and logged in the Event log and all hosts in the system are updated with the new aging for **wrsroot**. The alarm is cleared after the password age is propagated to all the nodes and they are all updated.

NOTE: All password changes and password aging changes must be executed on the active controller to ensure that they propagate to all other hosts in the cluster. Otherwise, they remain local to the host where they were executed, and are overwritten on the next reboot to match the password and aging on the active controller.

- The default **Age** value is 45 days.

From the **wrsroot** account, you can execute commands requiring different privileges.

- You can execute non-root level commands as a regular Linux user directly.

If you do not have sufficient privileges to execute a command as a regular Linux user, you may receive a permissions error, or in some cases, the command may be reported as not found.

- You can execute root-level commands as the root user.

  To become the root user, use the **sudo** command to elevate your privileges, followed by the command to be executed. For example, to run the **config_controller** command as the root user:

  ```
  $ sudo config_controller
  ```

  If a password is requested, provide the password for the **wrsroot** account.

- You can execute OpenStack administrative commands as the Keystone **admin** user.

  To become the OpenStack **admin** user from the Linux **wrsroot** account, source the script **/etc/nova/openrc**:

  ```
  $ source /etc/nova/openrc
  [wrsroot@controller-0 ~(keystone_admin)]$
  ```

  The system prompt changes to indicate the new acquired privileges.

NOTE: The shell prompt set by the openrc script includes the Linux user name, the host name, the current working path, and the OpenStack/Keystone tenant name. For simplicity, this guide uses the following generic prompt instead:

```
~(keystone_admin)$
```

For more information on the active controller, see *HCG 4.0 Introduction: Controller Nodes and High Availability*.

Local Linux User Accounts

You can manage regular Linux user accounts on any host in the cluster using standard Linux commands. New accounts created on one host are not automatically propagated to other hosts.

Password changes are not enforced automatically on first login, and they are not propagated by the system (with the exception of the **wrsroot** account, for which passwords changed on the active controller are propagated to other hosts). You must manually configure any special considerations for these accounts, if there are any.

Local user accounts can be added to the *sudoers* list using the **visudo** command. They can also source the script **/etc/nova/openrc** to become OpenStack administrators when working on the active controller.

Backup and restore operations of home directories and passwords must be done manually. They are ignored by the system backup and restore utilities. For further details, see *HCG 4.0 Software Management: System Data Backup with Controller Storage*.

LDAP Linux User Accounts

You can create regular Linux user accounts using the HCG 4.0 LDAP service. LDAP accounts are centrally managed; changes made on any host are propagated automatically to all hosts on the cluster.

Apart from being centrally managed, LDAP user accounts behave as any local user account. They can be added to the sudoers list, and can acquire OpenStack administration credentials when executing on the active controller.

NOTE: HCG 4.0 includes a script for creating limited-shell or bash LDAP accounts intended for OpenStack users. For more information, seeCreating LDAP Linux Accounts for OpenStack Users on page 173.

LDAP user accounts share the following set of attributes:

- The initial password is the name of the account.
- The initial password must be changed immediately upon first login.
- Requirements for new passwords include:
  - at least eight characters long
  - at least one lowercase character
  - must differ in at least three characters from the previous password
  - must not be evidently trivial to guess, such as a2345678, or a reversed version of the old password
- Login sessions are logged out automatically after about 15 minutes of inactivity.
- The accounts block following five consecutive unsuccessful login attempts. They unblock automatically after a period of about five minutes.
- Home directories are created dynamically on first login. Note that home directories for local user accounts are created when the accounts are created.
- All authentication attempts are recorded in the **/var/log/auth.log** file on the target host.
- Home directories and passwords are backed up and restored by the system backup utilities.

The following LDAP user accounts are available by default on newly deployed hosts, regardless of their personality:

admin

A cloud administrative account, comparable to the default **admin** account used in the Web administration interface.

This user account operates on a restricted Linux shell, with limited access to native Linux commands. However, the shell is pre-configured to have administrative access to OpenStack commands, including the available HCG 4.0 CLI extensions.

operator

A host administrative account. It has access to all native Linux commands and is included in the sudoers list.

For increased security, the admin and operator accounts must be used from the console ports of the hosts; no SSH access is allowed.

Managing LDAP Linux User Accounts

Although the scope of operations for the LDAP user accounts is local (that is, they operate on the target host exclusively), management of these accounts operates at the cluster level. This means that operations such as password change, and addition or removal of users, are applied to the

entire cluster. For example, a password change executed while logged into controller-0, is effective immediately on all other hosts in the cluster.

Centralized management is implemented using two LDAP servers, one running on each controller node. LDAP server synchronization is automatic using the native LDAP content synchronization protocol.

A set of LDAP commands is available to operate on LDAP user accounts. The commands are installed in the **/usr/local/sbin** directory, and are available to any user account in the sudoers list. Included commands are **lsldap**, **ldapadduser**, **ldapdeleteuser**, and several others starting with the prefix **ldap**.

NOTE: It is recommended to use the **ldapusersetup** command for creating Linux accounts for OpenStack users. For more information , see Creating LDAP Linux Accounts for OpenStack Users on page 173.

Use the **--help** command option on any command to display a brief help message, as illustrated below.

```
$ ldapadduser --help
Usage : /usr/local/sbin/ldapadduser <username> <groupname | gid> [uid]
$ ldapdeleteuser --help
Usage : /usr/local/sbin/ldapdeleteuser <username | uid>
```

Creating LDAP Linux Accounts for OpenStack Users

HCG 4.0 includes a script for creating LDAP Linux accounts with built-in Keystone user support.

The **ldapusersetup** command provides an interactive method for setting up LDAP Linux user accounts with access to OpenStack commands. You can assign a limited shell or a bash shell.

Users have the option to provide Keystone credentials at login, and can establish or change Keystone credentials at any time during a session. Keystone credentials persist for the duration of the session.

Prerequisites

For convenience, identify the user's Keystone account user name in HCG 4.0.

Procedure

1. Log in as **wrsroot**, and start the **ldapusersetup** script.

   ```
   controller-0: ~$ sudo ldapusersetup
   ```

2. Follow the interactive steps in the script.
   a) Provide a user name.

      ```
      Enter username to add to LDAP:
      ```

For convenience, use the same name as the one assigned for the user's Keystone account. (This example uses **user1**). When the LDAP user logs in and establishes Keystone credentials, the LDAP user name is offered as the default Keystone user name.

```
Successfully added user user1 to LDAP
Successfully set password for user user1
```

b) Specify whether to provide a limited shell or a bash shell.

```
Select Login Shell option # [2]:
1) Bash
2) Lshell
```

To provide a limited shell with access to the OpenStack CLI only, specify the **Lshell** option.

If you select **Bash**, you are offered the option to add the user to the sudoer list:

```
Add user1 to sudoer list? (yes/No):
```

c) Optional: Specify a secondary user group for this LDAP user.

```
Add user1 to secondary user group (yes/No):
```

d) Optional: Change the password duration.

```
Enter days after which user password must be changed [90]:


Successfully modified user entry uid=ldapuser1, ou=People, dc=cgcs, dc=local in
LDAP
Updating password expiry to 90 days
```

e) Optional: Change the warning period before the password expires.

```
Enter days before password is to expire that user is warned [2]:


Updating password expiry to 2 days
```

On completion of the script, the command prompt is displayed.

```
controller-0: ~$
```

The LDAP account is created. For information about the user login process, see Establishing Keystone Credentials from a Linux Account on page 186.

Verifying the Controller Identity for Secure SSH Access

For secure SSH access to the controller, you must verify a fingerprint offered at login.

When you connect to a controller using SSH, you are asked to verify an ECDSA fingerprint.

```
ssh user@serverIP_or_FQDN
The authenticity of host '10.10.200.3 (10.10.200.3)' can't be established.
ECDSA key fingerprint is 8d:26:8e:a0:e4:47:5e:11:2c:52:27:90:c8:19:4e:4f.
Are you sure you want to continue connecting (yes/no)?
```

For security, HCG 4.0 strongly advises you to compare this fingerprint with the known fingerprint of the host before proceeding. To obtain the fingerprint of the host, log in at the console of either controller and use the following command:

```
ssh-keygen -l -f /etc/ssh/ssh_host_ecdsa_key.pub | grep ECDSA
256 8d:26:8e:a0:e4:47:5e:11:2c:52:27:90:c8:19:4e:4f  root@localhost (ECDSA)
```

Copy this fingerprint and save it for reference.

Linux Account Password Rules

HCG 4.0 enforces a set of strength requirements for new or changed passwords.

- The password must be at least seven characters long.
- The password must contain:
  - at least one lower-case character
  - at least one upper-case character
  - at least one numeric character
  - at least one special character
- Dictionary words or simple number sequences (for example, 123 or 321) are not allowed
- A changed password must differ from the previous password by at least three characters
- A changed password must not be a simple reversal of the previous password. For example, if nEtw!rk5 is the current password, 5kr!wtEn is not allowed as the new password.
- A changed password using only character case differences is not allowed. For example, if nEtw!rk5 is the current password, Netw!RK5 is not allowed as the new password.
- A changed password cannot use the older password that immediately preceded the current password. For example, if the password was previously changed from oP3n!sRC to the current password nEtw!rk5, then the new password cannot be oP3n!sRC.
- After five consecutive incorrect password attempts, the user is locked out for 5 minutes.

Password Recovery for Linux User Accounts

You can reset the password for a Linux user if required. The procedure depends on the class of user.

Linux System Users

This class includes the **wrsroot** account, and optionally other Linux system user accounts created to support a multi-admin scenario. If another Linux system account is available, you can use it to reset the password for this type of account as follows:

```
$ sudo passwd user temp_password
$ sudo chage -d 0 user
```

where *user* is the user name of the account to be reset (for, example, **wrsroot**) and *temp_password* is a temporary password. The **chage** command forces immediate expiration, so that the user must change the password at first login.

If no other Linux system user accounts have been created, then password recovery for **wrsroot** is not possible, and you must reinstall the HCG 4.0 software.

LDAP System Users

This class includes users created using LDAP utilities.

You can reset the password for an LDAP account as follows:

```
$ sudo ldapmodifyuser user replace userPassword temp_password
$ sudo ldapmodifyuser user replace shadowLastChange 0
```

where *user* is the user name, and *temp_password* is a temporary password. The second command forces a password change on first login.

Keystone Admin User

This class includes the OpenStack **admin** user.

You can reset the Keystone admin user password as follows:

```
$ sudo keyring set CGCS admin
$ Password for 'admin' in 'CGCS':temp_password
```

The Keystone admin user can change the password at any time using either the Identity panel in Horizon, or the **keystone user-password-update** command.

Keystone Tenant Users

This class includes OpenStack non-admin users (tenant users).

You can reset the Keystone admin user password from the OpenStack CLI as follows:

```
~(keystone_admin)$ keystone user-password-update --pass sudo temp_password user
```

where *user* is the user name and *temp_password* is a temporary password.

OpenStack Accounts

OpenStack uses tenant accounts to identify and manage tenants (projects), and user accounts to identify and manage access to OpenStack resources for individuals and system services.

You can create OpenStack tenants and users from the Web administration interface or the CLI. Tenants and users can also be managed using the OpenStack API.

In HCG 4.0, the default Keystone authentication method for OpenStack users is the local SQL Database Identity Service. You can optionally configure Keystone to use a remote LDAP Identity Service. For more information, see Keystone Account Authentication on page 180.

⚠ **CAUTION:** To ensure that all OpenStack users are managed by the LDAP identity service, configure the service *before* creating the OpenStack users.

Creating Users

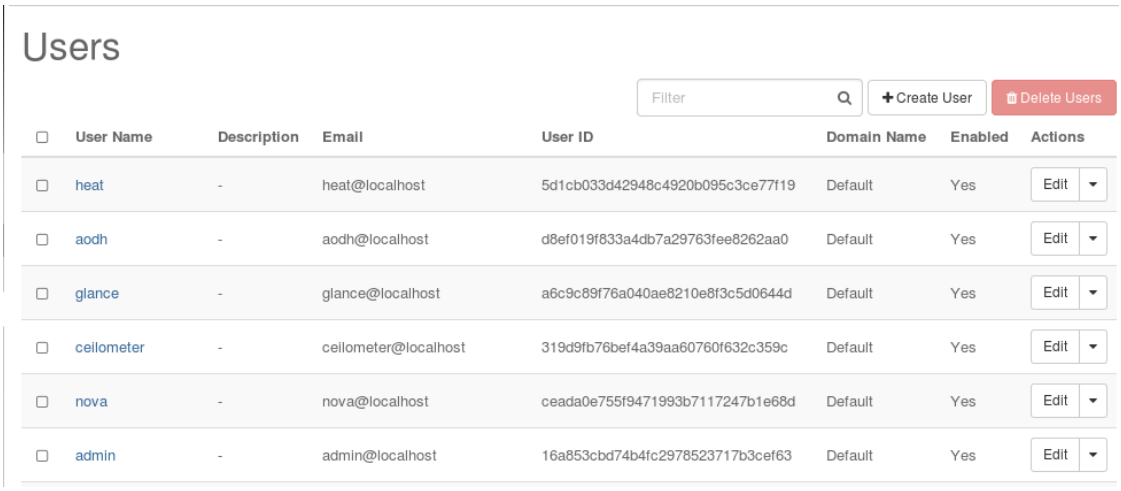
The **admin** user can create tenant users.

This exercise creates the **user1** user for the **tenant1-project** project.

Procedure

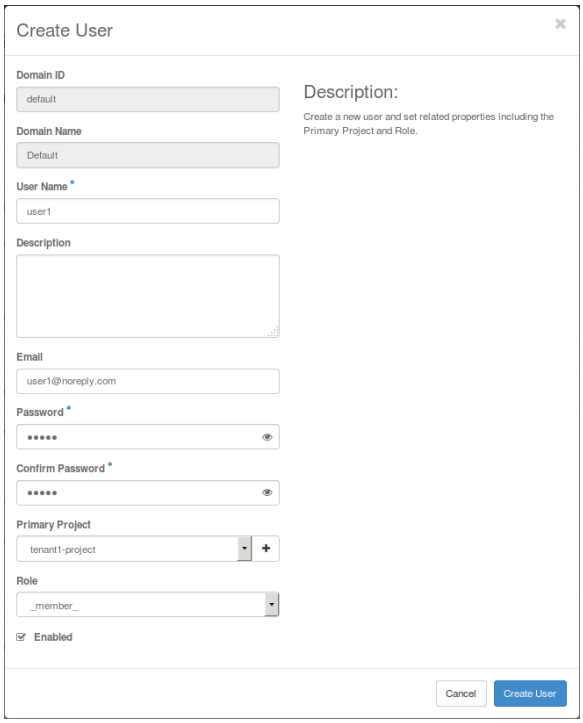
1. List the users currently defined on the system.

   Select **IdentityUsers** to open the Users page.



2. Create the **user1** user.

   Click **Create User** to open the Create User window. Fill in the information as illustrated below (use **user1** as the password):



Click **Create User** to commit the changes.

The user is added to the list on the Users page.

Creating Users Using the CLI

You can use the CLI to add users.

This exercise creates the **user1** and **user2** users, and associates each one with a tenant.

Procedure

1. Create the **user1** user.

```
~(keystone_admin)$ keystone user-create --name user1 --pass user1 \
--email user1@noreply.com --tenant ${tenant1_UUID}


+----------+----------------------------------+
| Property |              Value               |
+----------+----------------------------------+
|  email   |       user1@noreply.com          |
| enabled  |               True               |
|    id    | 4687426427034c778cf79351b5e1f870 |
|   name   |              user1               |
| tenantId | 27783a3c486841da9077aaf586d4c3d2 |
+----------+----------------------------------+
```

2. Create the **user2** user.

```
~(keystone_admin)$ keystone user-create --name user2 --pass user2 \
--email user2@noreply.com --tenant ${tenant2_UUID}


+----------+----------------------------------+
| Property |              Value               |
+----------+----------------------------------+
|  email   |       user1@noreply.com          |
| enabled  |               True               |
|    id    | 4687426427034c778cf79351b5e1f870 |
|   name   |              user1               |
| tenantId | 27783a3c486841da9077aaf586d4c3d2 |
+----------+----------------------------------+
```

The two new users now exist in the system. No UUID variables are defined because they are not needed in any subsequent commands.

Creating Login Environment Files for Users

Using the CLI, you can create scripts to define user login environments.

This exercise creates the **/etc/nova/openrc.user1** and **/etc/nova/openrc.user2** scripts. The new scripts are created by copying the original **admin** login environment script **/etc/nova/openrc**, and replacing the **admin** user identifier and its current password with new values.

Procedure

1. Create the login environment script for the **user1** user.
   a) Copy the environment script used by the **admin** user.

      ```
      $ cp /etc/nova/openrc /etc/nova/openrc.user1
      ```

   b) Edit the new file to include the new login credentials.

      The modified file looks similar to the following:

      ```
      export OS_USERNAME=user1
      export OS_PASSWORD=`TERM=linux /usr/bin/keyring get 'CGCS' user1`
      export PS1='[\u@\h \W(keystone_user1)]\$ '

      export OS_PROJECT_NAME=tenant1
      export OS_USER_DOMAIN_NAME=Default
      export OS_PROJECT_DOMAIN_NAME=Default
      export OS_IDENTITY_API_VERSION=3
      export OS_REGION_NAME=RegionOne
      export OS_INTERFACE=internal

      export OS_AUTH_URL=http://192.168.204.2:35357/v2.0/
      export CGTS_URL=http://192.168.9.204:6385
      ```

      NOTE: The IP address shown here is an example, based on the default controller node floating address suggested during the controller configuration script. Depending on your system configuration, the actual IP address may be different.

   The login environment script for **user1**, with password **user1**, is now available.

2. Create the login environment script for the **user2** user.
   a) Copy the environment script used by the **admin** user.

      ```
      $ cp /etc/nova/openrc /etc/nova/openrc.user2
      ```

   b) Edit the new file to include the new login credentials.

      The modified file looks similar to the following:

      ```
      export OS_USERNAME=user2
      export OS_PASSWORD=`TERM=linux /usr/bin/keyring get 'CGCS' user2`
      export PS1='[\u@\h \W(keystone_user2)]\$ '

      export OS_PROJECT_NAME=tenant2
      export OS_USER_DOMAIN_NAME=Default
      export OS_PROJECT_DOMAIN_NAME=Default
      export OS_IDENTITY_API_VERSION=3
      export OS_REGION_NAME=RegionOne
      export OS_INTERFACE=internal

      export OS_AUTH_URL=http://192.168.204.2:35357/v2.0/
      export CGTS_URL=http://192.168.9.204:6385
      ```

   The login environment script for **user2**, with password **user2**, is now available.

The two new user login environments are available. You can source them in order to execute commands with the corresponding user identities.

Using an Open RC File for Remote CLI Access

You can generate an Open RC file to configure a shell for remote CLI access.

To generate an Open RC file for a given user, you must be logged in as the appropriate user and tenant.

Procedure

1. Log into the HCG 4.0 Web administration interface as the applicable user.
2. Select the appropriate tenant.
3. In the Web administration interface page, select **Project** >**Compute**>**Access & Security** >**API Access**.
4. Click **Download OpenStack RC File**.
5. To obtain authentication, source the RC file.

   ```
   $ source tenantName-openrc.sh
   ```

   This establishes a shell with access to the HCG 4.0 command-line interface. It sets the tenant name, user name, and other shell parameters (including the HCG 4.0 URL), and prompts for the password. It also prompts for the optional CA Certificate if using HTTPS. For more information about certificates, see *HCG 4.0 Installation*.

   From within the shell, you can issue OpenStack commands directly to the HCG 4.0 CLI.

Keystone Account Authentication

OpenStack tenants and users are authenticated by the OpenStack Keystone identity service.

For tenant and user authentication, OpenStack supports a mixed backend that can use both SQL for local Keystone accounts and LDAP for centrally managed Keystone accounts. By default, HCG 4.0 uses the SQL identity service, and maintains the SQL database on the controller. For centrally managed acccounts, you can add an LDAP identity service for Keystone user accounts, and use a remote LDAP server backend. To add the LDAP identity service, see Configuring an LDAP Identity Service for Keystone Users on page 181.

⚠ **CAUTION:** To ensure that all OpenStack users are managed by the LDAP identity service, you must configure the service *before* creating the OpenStack users.

HCG 4.0 implements Keystone LDAP authentication using the Keystone API v2, preserving compatibility with earlier OpenStack releases. The implementation provides for LDAP user account management, while maintaining the SQL backend for service accounts to simplify the configuration process. All authentication requests are handled first by the SQL service. If no entry is found, they are referred to the LDAP service.

Configuring the Login Timeout for the Web Administration Interface

For security, login to the Web administration interface can be disabled for a user after several consecutive failed attempts. You can configure how many failed attempts are allowed before the user is locked out, and how long the user must wait before the lockout is reset.

⚠ **CAUTION:** This procedure requires the Web service to be restarted, which causes all current user sessions to be lost. To avoid interrupting user sessions, perform this procedure during a scheduled maintenance period only.

By default, after three consecutive failed login attempts, a user must wait five minutes (300 seconds) before attempting another login. During this period, all Web administration interface login attempts by the user are refused, including those using the correct password.

This behavior is controlled by the **lockout_retries** parameter and the **lockout_seconds** service parameter. To review their current values, use the **system service-parameter list** command.

You can change the duration of the lockout using the following CLI command:

```
~(keystone_admin)$ system service-parameter-add horizon auth \
lockout_seconds=duration
```

where *duration* is the time in seconds.

You can change the number of allowed retries before a lockout is imposed using the following CLI command:

```
~(keystone_admin)$ system service-parameter-add horizon auth \
lockout_retries=attempts
```

where *attempts* is the number of allowed retries.

For the changes to take effect, you must apply them:

```
~(keystone_admin)$ system service-parameter-apply horizon
```

Allow about 30 seconds after applying the changes for the Web service to restart.

Configuring an LDAP Identity Service for Keystone Users

You can configure HCG 4.0 to support LDAP authentication for Keystone users.

For more information about Keystone authentication, see Keystone Account Authentication on page 180.

Prerequisites

To configure the LDAP identity service for Keystone, you must become the **admin** user using the CLI.

Procedure

1. Confirm the current identity service.

```
~(keystone_admin)$ system service-parameter-list
+------+----------+------------+--------
```

```
+-----------------------------------------+
| uuid | service  | section    | name   |
value                                    |
+------+----------+------------+--------
+-----------------------------------------+
| a6...| identity | identity   | driver |
keystone.identity.backends.sql.Identity     |
| ac...| identity | assignment | driver |
keystone.assignment.backends.sql.Assignment |
+------+----------+------------+--------
+-----------------------------------------+
```

By default, HCG 4.0 uses the SQL identity service.

2. Add the URL of the LDAP server to the current identity service.

```
~(keystone_admin)$ system service-parameter-add identity ldap url=ldap://abc.com
+----------+--------------------------------------+
| Property | Value                                |
+----------+--------------------------------------+
| uuid     | b78e73ee-43df-4a27-964c-9a17dce6037f |
| service  | identity                             |
| section  | ldap                                 |
| name     | url                                  |
| value    | ldap://abc.com                       |
+----------+--------------------------------------+
```

This raises **250.001** configuration alarms against both controllers.

```
~(keystone_admin)$ system alarm-list
+------+----------+-------------------------------------------+...
| UUID | Alarm ID | Reason Text                               |...
+------+----------+-------------------------------------------+...
| 34...| 250.001  | controller-0 Configuration is out-of-date. |...
+----- +----------+-------------------------------------------+...
```

3. Add the DN suffix of the LDAP server.

```
~(keystone_admin)$ system service-parameter-add identity ldap suffix="dc=abc,dc=com"
```

4. Change the driver parameter from **sql** to **ldap**.

```
~(keystone_admin)$ system service-parameter-modify identity identity
driver=keystone.identity.backends.ldap.Identity
+----------+-------------------------------------------+
| Property | Value                                     |
+----------+-------------------------------------------+
| uuid     | a62c8aba-89e6-444f-a538-76802bbc5075      |
| service  | identity                                  |
| section  | identity                                  |
| name     | driver                                    |
| value    | keystone.identity.backends.ldap.Identity  |
+----------+-------------------------------------------+
```

5. Add a user name and password for querying the LDAP server.

   Specify an LDAP account with appropriate privileges.

```
~(keystone_admin)$ system service-parameter-add identity ldap \
user="cn=admin,dc=abc,dc=com" password="admin-password"
```

6. Configure secure access to the LDAP server.

Keystone provides Transport Layer Security support for secure access. The following commands enable support, provide the path and name of a certificate, and specify that a certificate is required for access:

NOTE: If the certificate authority is not included in those bundled with the default Linux distribution, the LDAP server certificate cannot be validated and the **tls_req_cert** parameter must be set to **never**.

```
~(keystone_admin)$ system service-parameter-add identity ldap use_tls=True
~(keystone_admin)$ system service-parameter-add identity ldap \
tls_cacertfile="/etc/keystone/ssl/certs/cacert.pem"
~(keystone_admin)$ system service-parameter-add identity ldap \
tls_cacertdir="/etc/keystone/ssl/certs"
~(keystone_admin)$ system service-parameter-add identity ldap tls_req_cert="demand"
```

7. Apply the service-parameter changes.

```
~(keystone_admin)$ system service-parameter-apply identity
Applying identity service parameters
```

This causes Keystone to reload the configuration file and use the LDAP Identity service. Changes to the **keystone.openstack.common.service** child processes are logged in the **/var/log/keystone/keystone-all.log** file.

8. Confirm that the **250.001** alarms against the controllers are cleared.

```
~(keystone_admin)$ system alarm-history-list -l 2

...------------------+------ ...+----------+...------------------------------+...
...                  | Alarm ...| Alarm ID |...                             |...
...------------------+------ ...+----------+...------------------------------+...
... T19:21:02.334671 | clear ...| 250.001  |...Configuration is out-of-date. |...
... T19:20:25.168683 | set   ...| 250.001  |...Configuration is out-of-date. |...
...------------------+-------...+----------+...------------------------------+...
```

Postrequisites

To enable LDAP users in Keystone, see Configuring Enabled User Emulation on page 183.

Depending on the LDAP identity service you are using and the features you require, additional mandatory or optional parameters may be needed. For a sample configuration, see Sample Configuration for LDAP-backed Keystone on page 184. For more information, refer to the LDAP identity service documentation.

For general configuration commands, see Commands for Managing LDAP-backed Keystone on page 185 .

Configuring Enabled User Emulation

For LDAP-backed Keystone, special steps may be required to enable users in Keystone, depending on the LDAP implementation.

Some LDAP implementations, such as OpenLDAP, do not have an attribute for enabling users. You can emulate one for use with Keystone by designating an LDAP group to identify enabled users, and then populating the group. You can then set service parameters to specify the group in Keystone and enable its use.

NOTE: If the LDAP implementation includes a Boolean attribute for enabling users, you can use the **set_user_enabled** service parameter to identify the attribute for use in Keystone. For details, see the public OpenStack documentation (for example, Configuring an Identity Provider).

If the LDAP implementation uses an integer-based attribute for enabling users, you can configure Keystone to use the integer-based attribute. For details, see the public OpenStack documentation.

Procedure

1. Enable the use of a group to emulate an **enabled** attribute for users.

```
~[keystone_admin]$ system service-parameter-add identity ldap
user_enabled_emulation=True
```

2. If required, create a **groupOfNames** object to contain the users.

   This is required for a read-only LDAP-backed Keystone configuration. The LDAP server administrator must create the object.

3. Specify the group in Keystone.

   For example:

```
~[keystone_admin]$ system service-parameter-add identity ldap \
user_enabled_emulation_dn="cn=enabled_users,ou=Users,dc=openstack,dc=org"
```

4. To enable users, add them to the group.

   You can also disable users by removing them from the group.

Sample Configuration for LDAP-backed Keystone

For guidance, a sample service parameter configuration is presented, based on the OpenLDAP Server.

```
BASEDN=dc=openstack,dc=org
LDAPHOST=ldapserver-example.openstack.org
LDAPUSER=admin
LDAPPW=badpassword


# mandatory server configuration
system service-parameter-add identity ldap url="ldap://${LDAPHOST}" user="cn=$
{LDAPUSER},${BASEDN}" password="${LDAPPW}" suffix="${BASEDN}"

# DN values will be defaulted to Users suffix
# system service-parameter-add identity ldap user_tree_dn="ou=Users,${BASEDN}"

# openldap requires an emulated user enabled attribute which is a groupOfNames object
with members for each enabled user
system service-parameter-add identity ldap user_enabled_emulation=true

# DN can be derived from user_tree_dn assuming CN is enabled_users
system service-parameter-add identity ldap
user_enabled_emulation_dn="cn=enabled_users,ou=Users,${BASEDN}"

# members attribute is a required parameter, use dummy
system service-parameter-add identity ldap use_dumb_member=true
```

```
# enable user default_project_id
system service-parameter-add identity ldap user_attribute_ignore=tenants
system service-parameter-add identity ldap
user_default_project_id_attribute=departmentNumber

# modify identity backend to LDAP driver
system service-parameter-modify identity identity
driver="keystone.identity.backends.ldap.Identity"

# modify to use TLS (set tls_req_cert to never to prevent cert validation error if
using self-signed certificate or unknown root CA)
system service-parameter-add identity ldap use_tls=true tls_cacertdir=/etc/ssl/certs
tls_req_cert=never

# modify to use connection pool (pool defaults not updated)
system service-parameter-add identity ldap use_pool=true

# modify to use authentication pool (pool defaults not updated)
system service-parameter-add identity ldap use_auth_pool=true

# list all parameters
system service-parameter-list

# apply the changes
system service-parameter-apply identity
```

Commands for Managing LDAP-backed Keystone

HCG 4.0 provides several commands for managing an LDAP-backed Keystone configuration.

To obtain command syntax information, use the **help** option. For example:

```
~(keystone_admin)$ system help service-parameter-add
usage: system service-parameter-add <service> <section> <name=value>
                                    [<name=value> ...]

Add a Service Parameter.

Positional arguments:
  <service>     Name of service [REQUIRED]
  <section>     Name of section [REQUIRED]
  <name=value>  Service Parameter attributes to add
```

system service-parameter-add

Adds a service parameter. For example:

```
~(keystone_admin)$ system service-parameter-add identity ldap \
parm1=value1 parm2=value2
+----------+--------------------------------------+
| Property | Value                                |
+----------+--------------------------------------+
| uuid     | 012c9b19-170e-4b91-9354-5a64bd4e02c4 |
| service  | identity                             |
| section  | ldap                                 |
| name     | parm1                                |
| value    | value1                               |
+----------+--------------------------------------+
+----------+--------------------------------------+
| Property | Value                                |
+----------+--------------------------------------+
| uuid     | 00292bee-2711-4bc9-86d8-400bc13955d6 |
| service  | identity                             |
| section  | ldap                                 |
| name     | parm2                                |
| value    | value2                               |
+----------+--------------------------------------+
```

system service-parameter-apply

Applies service parameters.

system service-parameter-delete

Deletes a service parameter.

system service-parameter-list

Lists service parameters.

```
+--------------------------------------+----------+---------+-------+--------+
| uuid                                 | service  | section | name  | value  |
+--------------------------------------+----------+---------+-------+--------+
| 012c9b19-170e-4b91-9354-5a64bd4e02c4 | identity | ldap    | parm1 | value1 |
| 00292bee-2711-4bc9-86d8-400bc13955d6 | identity | ldap    | parm2 | value2 |
+--------------------------------------+----------+---------+-------+--------+
```

system service-parameter-modify

Modifies service parameter attributes.

system service-parameter-show

Shows a service parameter. For example:

```
~(keystone_admin)$ system service-parameter-show \
012c9b19-170e-4b91-9354-5a64bd4e02c4
+----------+--------------------------------------+
| Property | Value                                |
+----------+--------------------------------------+
| uuid     | 012c9b19-170e-4b91-9354-5a64bd4e02c4 |
| service  | identity                             |
| group    | LDAP                                 |
| name     | parm1                                |
| value    | value1                               |
+----------+--------------------------------------+
```

For information about configuring an LDAP backend for Keystone, see Configuring an LDAP Identity Service for Keystone Users on page 181.

Establishing Keystone Credentials from a Linux Account

The preferred method for establishing OpenStack Keystone credentials is to log in to an LDAP account created using **ldapusersetup**.

For more information about **ldapusersetup**, see Creating LDAP Linux Accounts for OpenStack Users on page 173.

User accounts created using **ldapusersetup** have access to the OpenStack CLI as part of the shell. To list the available commands, type **?** at the command line:

```
user1@controller-0:~$ ?

awk         cinder  echo    glance  history   ls     neutron    pwd   source
cat         clear   env     grep    keystone  lsudo  nova       rm    system
cd          cp      exit    heat    ll        man    openstack  scp   vim
ceilometer  cut     export  help    lpath     env    passwd     sftp
```

When a user logs in to an account of this type, they are prompted to store Keystone credentials for the duration of the session:

```
Pre-store Keystone user credentials for this session? (y/N):y
```

This invokes a script to obtain the credentials. The user can invoke the same script at any time during the session as follows:

```
user1@controller-0:~$ source ~/lshell_env_setup
```

Any OpenStack credentials created by the script persist for the duration of the session. This includes credentials added by previous invocations of the script in the same session.

The Keystone Credentials Script

The Keystone credentials script offers the LDAP user name as the default Keystone user name:

```
Enter Keystone username [user1]:


Enter Keystone user domain name:
```

It requires the name of the tenant for which the user requires access:

```
Enter Project name:tenant1
```

NOTE: The Keystone user must be a member of the OpenStack tenant. This is configured using OpenStack.

```
Enter Project domain name:
```

It also requires the Keystone user password:

```
Enter Keystone password:
```

When the script is run during login, it sets the default **Keystone Region Name** and **Keystone Authentication URL**.

```
Selecting default Keystone Region Name: RegionOne
Selecting default Keystone Authentication URL: http://192.168.204.2:5000/v2.0/
To re-configure your environment run "source ~/lshell_env_setup" in your shell

Keystone credentials preloaded!
```

If the script is run from the shell after login, it provides an option to change the **Keystone Region Name** and **Keystone Authentication URL**.

Alternative Methods for Establishing Keystone Credentials

You can also establish Keystone credentials using the following methods:

- Download an OpenStack RC file (**openrc.sh**) from the Web administration interface, and use it to source the required environment. For more information, refer to http://docs.openstack.org.
- Add the required environment variables manually:

OS_USERNAME

the Keystone user name

OS_USER_DOMAIN_NAME

the default domain for the user

OS_PROJECT_NAME

the tenant name

OS_PROJECT_DOMAIN_NAME

the default domain for the project

OS_PASSWORD

a clear text representation of the Keystone password

OS_AUTH_URL

the Keystone Authentication URL

OS_IDENTITY_API_VERSION

the identity API version

OS_INTERFACE

the interface

OS_REGION_NAME

the Keystonre Region Name

For security and reliability, add all of the variables.

- Provide credentials as command-line options.

```
user1@controller-0:~$ system --os-username admin --os-password seeCaution host-list
```

⚠ **CAUTION:** HCG 4.0 does not recommend using the command-line option to provide OpenStack credentials. It creates a security risk, because the supplied credentials are visible in the command-line history.

Adding a Key Pair

Key pairs provide for secure login to guest images.

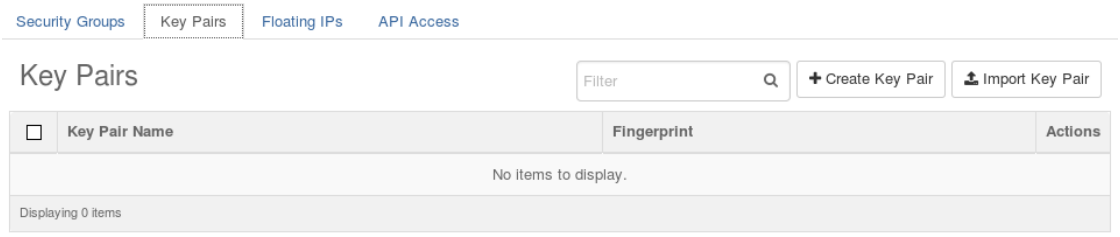
This exercise injects a key pair into the Nova database with the name **tenant1-controller-0**. This named key pair can be used to provide automatically authenticated SSH access to the virtual machines. You can use other available key pairs, or create new ones, as required.

Procedure

1. List the key pairs available from the system.

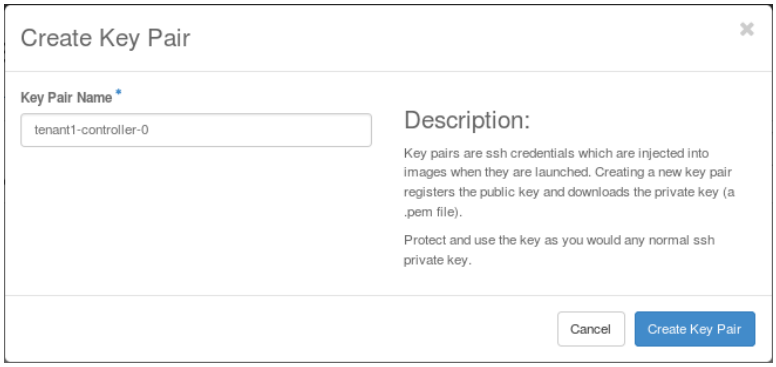
   Select **Project** > **Compute** > **Access & Security**.

   Select the **Key Pairs** tab. Because no key pairs have been defined yet, an empty list is displayed as follows:



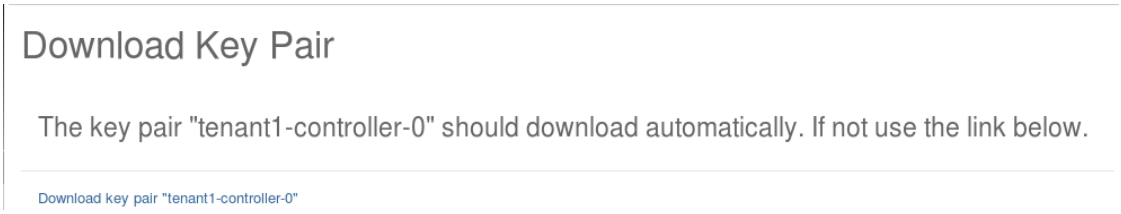
2. Create the key pair **tenant1-controller-0**.

   Click **Create Key Pair** to open the Create Key Pair window. Fill in the information as follows:



   Click **Create Key Pair** to create the authentication keys.

   The system gives you the opportunity to download the key pair to your workstation, as illustrated below:

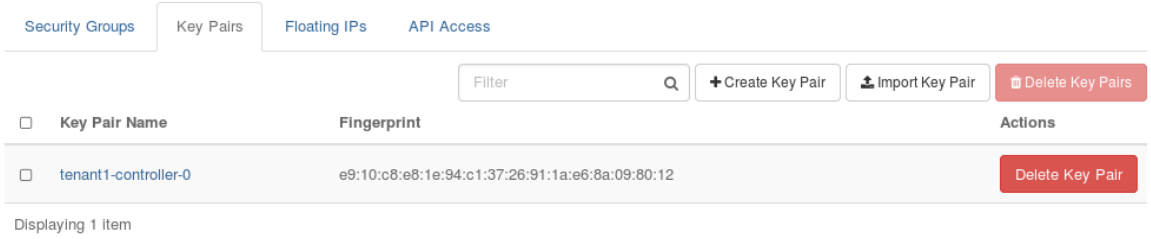


   Click on the download link to save a local copy of the authentication key pair. Use it as you would use any key pair for SSH authentication between two workstations.

   - Transfer the key pair to the workstation you plan to use to access the virtual machine over SSH.
   - Copy the public key to the virtual machine. You can use the **ssh-copy-id** command from a Linux workstation, or transfer the public key using a command such as **scp**.

   For more information, see the public document for SSH.

The key pair **tenant1-controller-0** is available now. It is listed as follows:



About Tenants (Projects) and Users

Tenants and users are system resources managed by the OpenStack Keystone service.

Tenants are the core resource structure on which all end user services are managed. They are isolated resource containers consisting of networks, storage volumes, images, virtual machines, authentication keys, and users.

When HCG 4.0 is deployed, two default tenants are created: **admin** and **services**. They are used to group resources to be associated with the **admin** user and the cloud services, respectively.

NOTE: Earlier versions of OpenStack used the term *project* instead of *tenant*. Because of this legacy terminology, the Web administration interface uses both terms, and some command-line tools use **--project_id** when a tenant ID is expected.

Users are system resources that can operate on one or more tenants, within the constraints of a particular role. For each user, the Keystone service maintains a list of (tenant, role) tuples, which are used to determine the tenants the user can operate on, and the role the user should play on each of them.

In the default installation of HCG 4.0, several users are already defined. Each of the OpenStack services, such as Nova and Neutron, exist as system users. They all operate on the default tenant **services**.

The Keystone **admin** user is associated with the **admin** tenant. This user has administrator privileges for creating, modifying, and deleting OpenStack resources, including creating other tenants and users.

Operator Command Logging

HCG 4.0 logs all operator commands.

The logs include the timestamp, tenant name (if applicable), user name, command executed, and command success or failure status.

These log files use a ***-api.log** filen ame convention and can be found under the **/var/log** directory.

Each OpenStack component that generates its own API log files (for example, Nova, Neutron, Cinder, and so forth) and each HCG 4.0-specific component and patching system follow this convention.

These log files can be examined locally on the Controllers by inspecting the ***-api.log** files under the **/var/log** directory. Logs can also be examined on a remote log server, if the remote logging feature is configured.

The one exception to this is **patching-api.log**. For patching robustness reasons, the HCG 4.0 patching system uses minimal system facilities and does not use syslog, therefore its logs do not appear on the remote log server.

For example, for the HCG 4.0 system command, whenever a REST API call is made that is either a:

- POST - usually means creating something
- PATCH - usually means partially updating (modifying) something
- PUT - usually means fully updating (modifying) something
- DELETE - usually means deleting something

HCG 4.0 logs these events into a new log file called **/var/log/sysinv-api.log**.

If the **sysinv** command only issues a GET REST call, it is not logged.

For example:

system event-list - is not logged because this performs a sysinv REST GET call

system event-show*xx* - is not logged because this performs a sysinv REST GET call

system modify description="A TEST" - is logged to **sysinv-api.log** because it issues a REST POST call

system snmp-comm-delete "TEST_COMMUNITY1" - is logged to **sysinv-api.log** because it issues a REST DELETE call

Operator Login/Authentication Logging

HCG 4.0 logs all operator login and authentication attempts.

For security purposes, all login attempts (success and failure) are logged.

This includes Horizon logins, SSH logins, and so forth, as well as internal local LDAP login attempts and internal database login attempts.

- The logs include timestamp, user name, remote IP Address, and the number of failed login attempts (if applicable).

These log files can be found under the **/var/log** directory, and include:

- **/var/log/auth.log**
- **/var/log/horizon.log**
- **/var/log/pmond.log**
- **/var/log/hostwd.log**
- **/var/log/sysinv.log**
- **/var/log/user.log**

You can examine these log files locally on the controllers by inspecting the files under the **/var/log** directory. Logs can also be examined on a remote log server, if the remote logging feature is configured.

Secure HTTPS External Connectivity

HCG 4.0 provides support for secure HTTPS external connections for REST API access and Web server access.

Enabling HTTPS Access (optional)

To enable secure HTTPS access for REST API applications and the Web server, a digital certificate is required during software installation. When secure HTTPS connectivity is chosen, HTTP is disabled.

For evaluation purposes, you have the option to select a self-signed certificate included with HCG 4.0. For actual deployment, it is strongly recommended that you use a CA-signed certificate. You must obtain the certificate and copy it to the controller host before starting the controller configuration script. You can update the certificate at any time after installation.

NOTE: If the self-signed certificate is in use, remote clients must be configured to accept the certificate without verifying it ("insecure" mode) in order to connect.

Installing a digital certificate

To install a CA-signed digital certificate, follow the procedure for installing and configuring the HCG 4.0. During this procedure, you must copy the certificate PEM file to the controller host before running the controller configuration script.

Updating a digital certificate

After you have installed a digital certificate, whether CA-signed or self-signed, you can update it by copying the new certificate to the active controller host, and then running the **https-certificate-install** utility as shown in the following example.

```
$ sudo /usr/sbin/https-certificate-install pem_file
```

Firewall Options

HCG 4.0 incorporates a firewall for the OAM network. During initial configuration, you can specify an additional file in order to augment or override the default rules.

For more information about specifying a firewall rules file during controller configuration, see *HCG 4.0 Installation: The Controller Configuration Script*.

The HCG 4.0 firewall uses the **Netfilter** framework to implement a firewall on the OAM network. If the system is configured to support an optional firewall rules file, you can introduce custom rules by adding entries in this file.

Two input chains are supported for custom rules: **INPUT-custom-pre**, for rules to be processed before the default rules, and **INPUT-custom-post**, for rules to be processed after the default rules.

A minimal set of rules is always applied before any custom rules, as follows:

- Non-OAM traffic is always accepted.
- Egress traffic is always accepted.
- Service manager (SM) traffic is always accepted.
- SSH traffic is always accepted.

For the default rules used by HCG 4.0, see *Helion OpenStack Carrier Grade 4.0 System Administration: Default Firewall Rules on page 11*. For more about custom rules, see *Helion OpenStack Carrier Grade 4.0 System Administration: Firewall Rules File Format on page 12*.

You can validate the file using the following command:

```
$ iptables-restore --noflush --test < filename
```

where *filename* is the path and name of the file.

CAUTION: You should validate the file before you run the configuration controller script. If the file is invalid, you must correct any errors and then start the script again from the beginning.

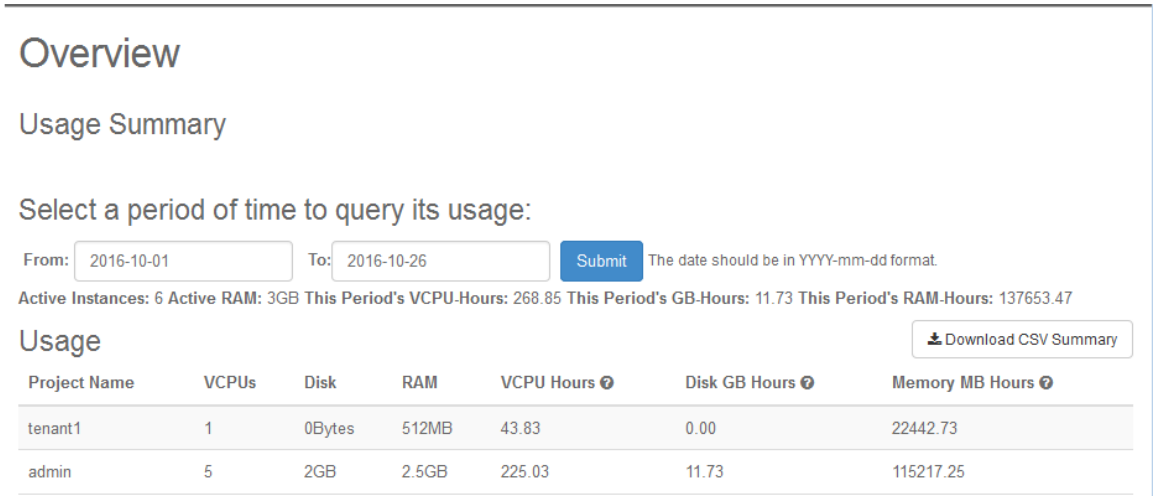
7

Resource Monitoring

The Overview Page

The Overview page appears when you log into the HCG 4.0 web administration interface as the administrator.

This page shows a resource usage summary for currently running instances.



The page shows the following information:

- the date range for which data is summarized
- the total **Active Instances**, **VCPU-Hours**, **GB-Hours**, and **RAM-Hours** instance usage for all projects
- instance usage statistics for each individual project

To change the date range, click the **From** or **To** field and then use the calendar that appears, or type the date using **YYYY-MM-DD** format.

You can obtain a comma-separated-values (CSV) report for further processing by clicking **Download CSV Summary** and then specifying a local path. The exact download behavior depends on your browser.

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 HCG 4.0 cluster extends Ceilometer with improved reports and new tools to facilitate offline analysis of the collected data.

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 HCG 4.0 improves on several aspects. They are described in the following sections.

Optimized Ceilometer Filters

The Ceilometer implementation in HCG 4.0 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.

CSV Performance Monitoring Backend

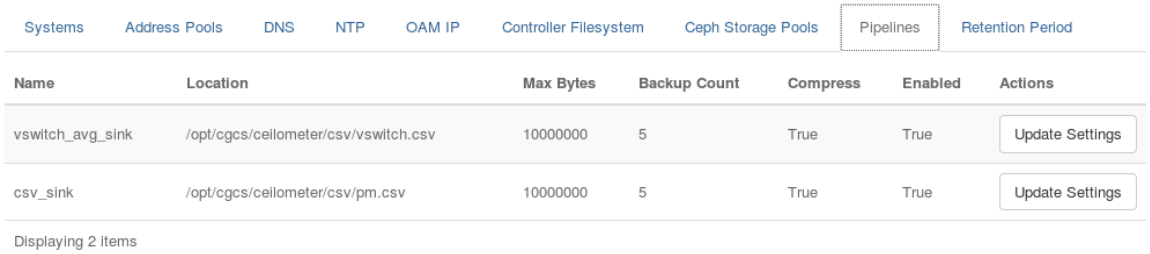
HCG 4.0 provides access to performance measurement samples in the form of comma-separated values (CSV) files.

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

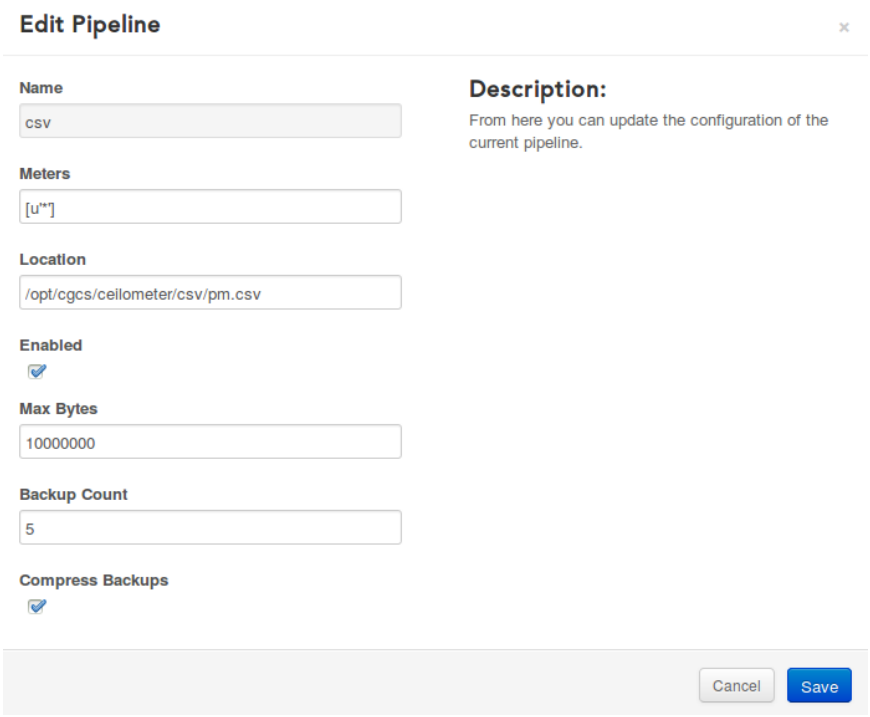
The CSV files are expected to be retrieved from the controllers using any suitable file transfer client application such as SFTP or SCP. This can be done manually by the system administrator, or automatically by an operations and support server (OSS/BSS) configured with the appropriate login credentials.

Recording of samples and management of CSV files is done through special Ceilometer pipelines available from the **Pipelines** tab available from **Admin** > **Platform** > **System Configuration**, 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.

Click the button **Update Settings** to configure the behavior of a pipeline. The Edit Pipeline window is presented as follows:



The following fields are available:

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.

You should use a path below **/opt/cgcs**. Otherwise, if the active controller fails, the **csv** files will not be available on the backup 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.

On-Line Ceilometer Reports

You can generate on-line Ceilometer reports.

On-line, on-demand, Ceilometer reports in HCG 4.0 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

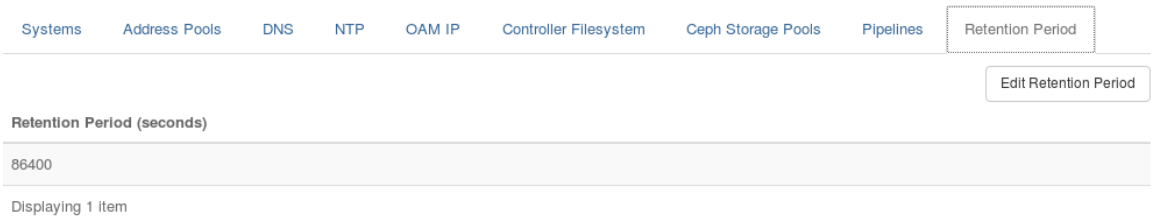
Additionally, all database queries are user-initiated, as opposed to event-initiated. This provides a different user workflow, whereby all required report parameters and filters are configured first, before the database query is executed.

To use on-line Ceilometer reports, see Querying Ceilometer Meters on page 200.

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.

Click the **Edit Retention Period** button in the **Retention Period** tab, available from **AdminPlatform** > **System Configuration**, to modify the current value. You must ensure that the configured value is equal or higher than the period over which you intend to gather statistics.



You can also control the retention period from the CLI. To view the current settings, use the following command.

```
~(keystone_admin)$ system pm-show
```

To change the retention period from the CLI, use the following command syntax.

```
~(keystone_admin)$ system pm-modify retention_secs=retention_period
```

For example:

```
~(keystone_admin)$ system pm-modify retention_secs=172800
```

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** is displayed for the controller nodes on the Host tab of the Host Inventory page. These alarms are resolved and cleared automatically after a few seconds.

Querying Ceilometer Meters

You can query Ceilometer meters using several approaches.

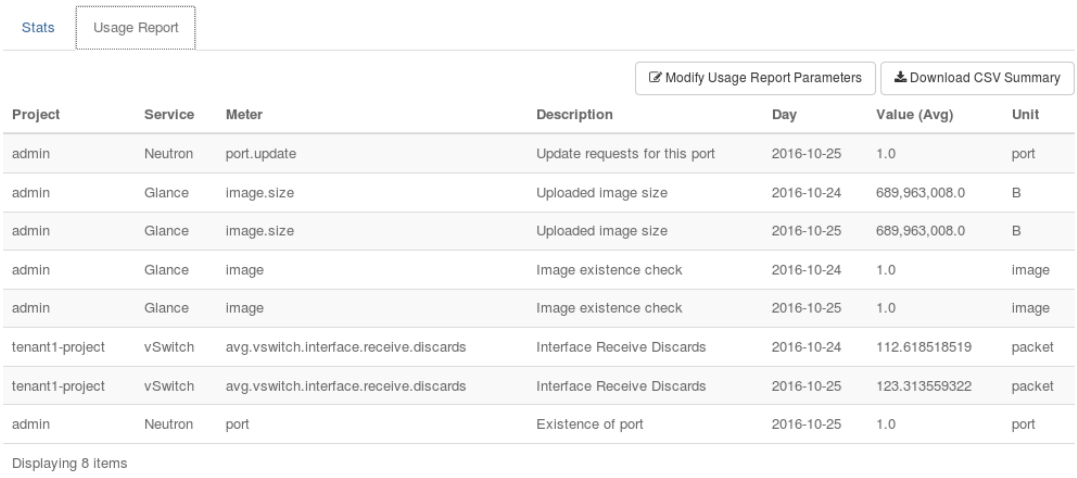
As an alternative to the web administration interface, you can use the CLI to make queries. See Querying Ceilometer Meters Using the CLI on page 201.

For additional information about Ceilometer meters, see Resource Usage on page 196.

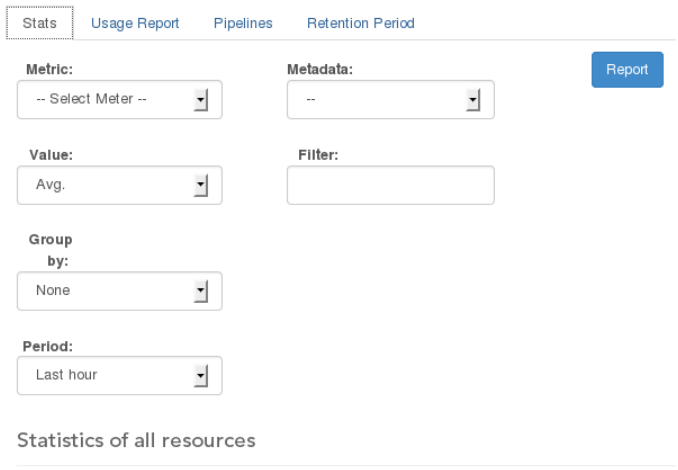
Procedure

1. From the menu pane, select **Admin** > **System** > **Resource Usage**.
2. Select the tab for the type of query you want to use.
   - To see statistics for a standard set of meters, select the **Usage Reports** tab.

NOTE: The data is refreshed when the tab is selected. Depending on system size and current loads, this may take a few seconds.



   - To obtain statistics for a specific meter, select the **Stats** tab.



The following fields are available for reporting a specific meter:

Metric

The Ceilometer meter you want to query. Meters are grouped by service, as follows:

- Compute (Nova)
- Network (Neutron)
- Image (Glance)
- Volume (Cinder)
- Switching (AVS)

For a list of supported meters, see Supported Performance Meters on page 204.

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. They include **last 15 minutes**, **last 30 minutes**, **last hour**, **last day**, **last week**, **last 15 days**, **last 30 days**, **last year**, and **other**. 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 meter. In this menu, you can select the specific attribute you want the report on.

Filter

Use this field to limit the report to show meter samples whose metadata attribute equals the specified value. The filter field is applied only when a specific metadata attribute is selected.

Querying Ceilometer Meters Using the CLI

If you prefer, you can use the CLI to query Ceilometer.

For web administration interface instructions, see Querying Ceilometer Meters on page 200.

To view a set of samples for a meter, use a command of the following form:

```
~(keystone_admin)$ ceilometer sample-list [-m name] [-l number] [-q query]
```

where

name

is the name of the Ceilometer meter

number

is the maximum number of samples to return

query

is a list of metadata filters to apply to the samples, in the form 'metadata_type=filter_value; metadata_type=filter_value; ...'

For example:

```
~(keystone_admin)$ ceilometer sample-list -m vcpu_util -l 10 \
-q 'metadata.display_name=clearwater-ip-pbx-1'
+--------------+-----------+-------+---------------+------+---------------------+
| Resource ID  | Name      | Type  | Volume        | Unit | Timestamp           |
+--------------+-----------+-------+---------------+------+---------------------+
| d9ae484c-... | vcpu_util | gauge | 20.4          | %    | 2015-11-18T14:39:31 |
| d9ae484c-... | vcpu_util | gauge | 20.7          | %    | 2015-11-18T14:39:01 |
| d9ae484c-... | vcpu_util | gauge | 21.0333333333 | %    | 2015-11-18T14:38:31 |
| d9ae484c-... | vcpu_util | gauge | 21.5333333333 | %    | 2015-11-18T14:38:01 |
| d9ae484c-... | vcpu_util | gauge | 20.2333333333 | %    | 2015-11-18T14:37:31 |
| d9ae484c-... | vcpu_util | gauge | 19.8          | %    | 2015-11-18T14:37:01 |
| d9ae484c-... | vcpu_util | gauge | 19.5333333333 | %    | 2015-11-18T14:36:31 |
| d9ae484c-... | vcpu_util | gauge | 19.6333333333 | %    | 2015-11-18T14:36:01 |
| d9ae484c-... | vcpu_util | gauge | 20.6666666667 | %    | 2015-11-18T14:35:31 |
| d9ae484c-... | vcpu_util | gauge | 19.4666666667 | %    | 2015-11-18T14:35:01 |
+--------------+-----------+-------+---------------+------+---------------------+
```

To list the types of meters, use the following command:

```
~(keystone_admin)$ ceilometer metertype-list
```

This command outputs the *type* and measurement *unit* for each meter.

Valid types include:

delta

These meters measure change over time, such as bandwidth.

cumulative

These meters increase over time, such as instance hours.

gauge

These meters measure discrete items such as image uploads and floating IP addresses, as well as fluctuating values such as disk I/O.

Valid units may be percentages, bytes, nanoseconds or packets, depending on the meter. For more information, see http://docs.openstack.org/admin-guide-cloud/telemetry-measurements.html.

For example:

```
~(keystone_admin)$ ceilometer metertype-list

+---------------------------------+-------------+-----------+
```

```
| Name                                | Type        | Unit      |
+-------------------------------------+-------------+-----------+
| avg.vswitch.engine.util             | delta       | %         |
| avg.vswitch.port.receive.bytes      | cumulative  | B         |
| avg.vswitch.port.receive.packets    | cumulative  | packet    |
| avg.vswitch.port.receive.util       | gauge       | %         |
| avg.vswitch.port.transmit.bytes     | cumulative  | B         |
| avg.vswitch.port.transmit.errors    | cumulative  | packet    |
| avg.vswitch.port.transmit.packets   | cumulative  | packet    |
| avg.vswitch.port.transmit.util      | gauge       | %         |
| cpu                                 | cumulative  | ns        |
| cpu_util                            | gauge       | %         |
| disk.allocation                     | gauge       | B         |
| disk.capacity                       | gauge       | B         |
| disk.device.allocation              | gauge       | B         |
| disk.device.capacity                | gauge       | B         |
...
```

For a list of supported meters, see Supported Performance Meters on page 204. To list the available meters and their resource IDs from the CLI, use the following command:

```
~(keystone_admin)$ ceilometer meter-list
```

To list the metadata associated with a meter, use a command of the following form:

```
~(keystone_admin)$ ceilometer resource-show resource_id
```

where *resource_id* is the resource ID of the metric.

To list current statistics for a meter, including the average, minimum, maximum, and summed values, use a command of the following form:

```
~(keystone_admin)$ ceilometer statistics -m meter -p period -q query \
-g field -a funcs
```

where

meter

is the name of the Ceilometer meter

period

is the period in seconds for which to include samples

query

is a list of metadata filters to apply to the samples, in the form 'metadata_type=filter_value; metadata_type=filter_value; ...'

field

is the grouping used when displaying the samples (for example, by tenant or by resource)

funcs

is a list of statistical functions to display, in the form '**func** [-**param**]; **func** [-**param**]; ...'

If this option is not specified, then **min**, **max**, **avg**, and **sum** are shown by default.

For example:

```
~(keystone_admin)$ ceilometer statistics -m vcpu_util -p 10 \
-q 'metadata.display_name=clearwater-ip-pbx-1'
+--------+---------------------+---------------------+------+---------------+
| Period | Period Start        | Period End          | Max  | Min           |
+--------+---------------------+---------------------+------+---------------+
| 0      | 2015-11-17T14:01:30 | 2015-11-18T14:41:01 | 64.1 | 11.8666666667 |
```

```
+--------+---------------------+---------------------+------+---------------+ ...

---------------+---------------+-------+----------+
 Avg           | Sum           | Count | Duration |
---------------+---------------+-------+----------+
 20.5642892608 | 60870.2962121 | 2960  | 88771.0  |
---------------+---------------+-------+----------+ ...

---------------------+---------------------+
 Duration Start      | Duration End        |
---------------------+---------------------+
 2015-11-17T14:01:30 | 2015-11-18T14:41:01 |
---------------------+---------------------+
```

For more information about Ceilometer statistics, refer to the public Openstack documentation.

Supported Performance Meters

HCG 4.0 includes performance meters for various OpenStack and platform services.

Nova Meters

Name	Type	Unit	Resource	Note
instance	Gauge	instance	inst ID	Duration of instance
instance:<type>	Gauge	instance	inst ID	Duration of instance <type> (openstack types)
memory	Gauge	MB	inst ID	Volume of RAM in MB
cpu	Cumulative	ns	inst ID	CPU time used
cpu_util	Gauge	%	inst ID	Average CPU utilisation
vcpus	Gauge	vcpu	inst ID	Number of VCPUs
disk.read.requests	Cumulative	request	inst ID	Number of read requests
disk.write.requests	Cumulative	request	inst ID	Number of write requests
disk.read.bytes	Cumulative	B	inst ID	Volume of read in B
disk.write.bytes	Cumulative	B	inst ID	Volume of write in B
disk.root.size	Gauge	GB	inst ID	Size of root disk in GB
disk.ephemeral.size	Gauge	GB	inst ID	Size of ephemeral disk in GB

Neutron Meters

Name	Type	Unit	Resource	Note
network	Gauge	network	netw ID	Duration of network

Name	Type	Unit	Resource	Note
network.create	Delta	network	netw ID	Creation requests for this network
network.update	Delta	network	netw ID	Update requests for this network
subnet	Gauge	subnet	subnt ID	Duration of subnet
subnet.create	Delta	subnet	subnt ID	Creation requests for this subnet
subnet.update	Delta	subnet	subnt ID	Update requests for this subnet
port	Gauge	port	port ID	Duration of port
port.create	Delta	port	port ID	Creation requests for this port
port.update	Delta	port	port ID	Update requests for this port
router	Gauge	router	rtr ID	Duration of router
router.create	Delta	router	rtr ID	Creation requests for this router
router.update	Delta	router	rtr ID	Update requests for this router
ip.floating	Gauge	ip	ip ID	Duration of floating ip
ip.floating.create	Delta	ip	ip ID	Creation requests for this floating ip
ip.floating.update	Delta	ip	ip ID	Update requests for this floating ip

Glance Meters

Name	Type	Unit	Resource	Note
image	Gauge	image	image ID	Image polling -> it (still) exists
image.size	Gauge	B	image ID	Uploaded image size
image.update	Delta	image	image ID	Number of update on the image
image.upload	Delta	image	image ID	Number of upload of the image
image.delete	Delta	image	image ID	Number of delete on the image
image.download	Delta	B	image ID	Image is downloaded
image.serve	Delta	B	image ID	Image is served out

Cinder Meters

Name	Type	Unit	Resource	Note
volume	Gauge	volume	vol ID	Duration of volume
volume.size	Gauge	GB	vol ID	Size of volume

AVS vSwitch Meters

Name	Type	Unit	Resource	Note
avg.vswitch.engine.util	gauge	%	node ID	average cpu utilization of vswitch DPDK engines
avg.vswitch.port.receive.bytes	cumulative	B	node.port ID	# of bytes received on a particular port (physical or virtual)
avg.vswitch.port.receive.packets	cumulative	packet	node.port ID	# of packets received on a particular port (physical or virtual)
avg.vswitch.port.receive.util	gauge	%	node.port ID	rx link utilization
avg.vswitch.port.transmit.bytes	cumulative	B	node.port ID	# of bytes transmitted on a particular port (physical or virtual)
avg.vswitch.port.transmit.packets	cumulative	packet	node.port ID	# of packets transmitted on a particular port (physical or virtual)
avg.vswitch.port.transmit.util	gauge	%	node.port ID	tx link utilization

Platform Meters

Name	Type	Unit	Resource	Note
platform.cpu.util	gauge	%	node ID	average cpu utilization of core dedicated to platform
platform.mem.util	gauge	%	node ID	average memory utilization of memory dedicated to platform
platform.fs.util	gauge	%	node ID	average filesystem utilization of local file system dedicated to platform

Intelligent Platform Management Interface (IPMI) Meters

NOTE: Sample meters are shown. The available meters depend on the hardware platform.

Name	Type	Unit	Resource	Note
hardware.ipmi.temperature	gauge	C	node ID	
hardware.ipmi.current	gauge	A	node ID	
hardware.ipmi.fan	gauge	RPM	node ID	
hardware.ipmi.voltage	gauge	V	node ID	
hardware.ipmi.node.temperature	gauge	C	node ID	
hardware.ipmi.node.outlet_temperature	gauge	C	node ID	
hardware.ipmi.node.power	gauge	W	node ID	
hardware.ipmi.node.airflow	gauge	CFM	node ID	
hardware.ipmi.node.cups	gauge	CUPS	node ID	
hardware.ipmi.node.cpu_util	gauge	%	node ID	
hardware.ipmi.node.mem_util	gauge	%	node ID	
hardware.ipmi.node.io_util	gauge	%	node ID	

Viewing Resource Usage for a Device

You can view PCI device usage from the web administration interface or the CLI.

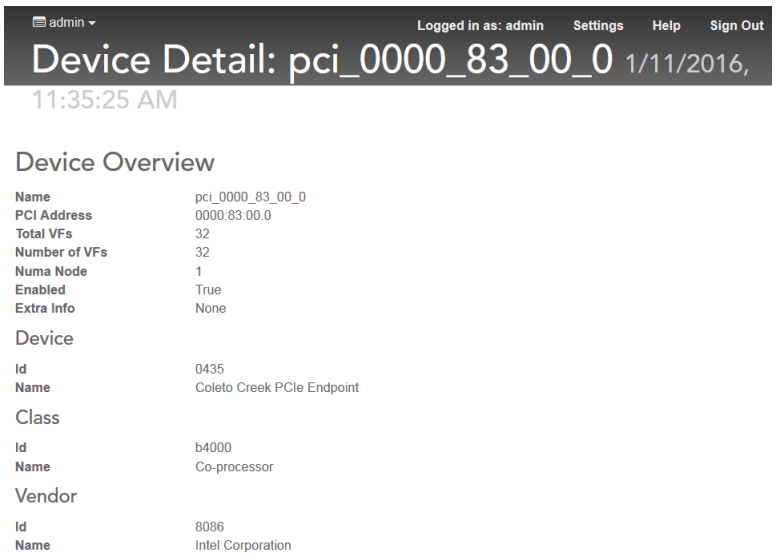
Procedure

1. Open the Host Inventory page.

   In the menu pane, select **Admin** > **Platform** > **Host Inventory**.

2. Select the Device Usage tab.

3. In the **Devices** list, click the **Name** of the device.



Details for the device are displayed, including usage across all compute nodes.

Viewing Resource Usage for PCI Interfaces

Information about PCI passthrough and SR-IOV usage for NICs is available on the Provider Network Overview page.

For more about the Provider Network Overview page, see Displaying Provider Network Information on page 21.

NOTE: For information about PCI passthrough or SR-IOV devices other than NICs, see Devices Tab on page 73.

To view information about PCI interface resources for a provider network from the CLI, use the following command:

```
~(keystone_admin)$ nova providernet-show providernet
```

where *providernet* is the UUID of the provider network.

For example:

```
~(keystone_admin)$ nova providernet-show a507bb89-8e78-48e4-8c8a-d8bac14fc097
+--------------------+--------------------------------------+
| Property           | Value                                |
+--------------------+--------------------------------------+
| id                 | a507bb89-8e78-48e4-8c8a-d8bac14fc097 |
| name               | group0-ext0                          |
| pci_pfs_configured | 1                                    |
| pci_pfs_used       | 1                                    |
| pci_vfs_configured | 0                                    |
| pci_vfs_used       | 0                                    |
+--------------------+--------------------------------------+
```

Where:

pci_pfs_configured

is the number of PCI passthrough interfaces attached to the provider network

pci_pfs_used

is the number of PCI passthrough interfaces allocated to instances

pci_vfs_configured

is the number of SR-IOV interfaces attached to the provider network

pci_vfs_used

is the number of SR-IOV interfaces allocated to instances

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 *Helion OpenStack Carrier Grade 4.0 Cloud Administration: 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 *Helion OpenStack Carrier Grade 4.0 Cloud Administration: 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. For details, see Processor Tab on page 60.

8

Fault Management

Fault Management

You can view the alarms and logs generated by HCG 4.0 in order to monitor and respond to fault conditions.

You can access active and historical alarms and customer logs using the CLI or the GUI. To use the CLI, see Viewing Active Alarms Using the CLI on page 216 and Viewing the Event Log Using the CLI on page 214.

Using the GUI, you can obtain fault management information in more than one way.

- The Fault Management page available from **Admin** > **Platform** > **Fault Management** in the left-hand pane provides comprehensive access to the following:

- **Active Alarms**—Alarms that are currently set, and require user action to clear them. For more about active alarms, see Viewing Active Alarms Using the CLI on page 216 and Deleting an Alarm on page 219.
- **Event Log**—The event log consolidates historical alarms that have been raised in the past, including those that have been cleared, as well as logs that do not require user action, but may provide useful information for fault management.

  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. Each log describes a single event. The logs are displayed in a list, along with summary information. For each individual log, you can view detailed information.

  Logs and historical alarms are held in a buffer, with older entries discarded as needed to release logging space.

  For more about the event log, which includes historical alarms and customer logs, see Viewing the Event Log Using the Web Interface on page 213 and Viewing the Event Log Using the CLI on page 214.

- The Provider Network Topology view provides real-time alarm information for provider networks and associated compute hosts and data interfaces. For more information, see The Provider Network Topology View on page 23.
- For advanced troubleshooting and analysis, you can configure a remote log server to collect logs from all hosts and present them centrally using an ELK stack. This includes system logs as well as customer logs. For more information, see Centralized Log Collection and Analysis on page 230.

The Global Alarm Banner

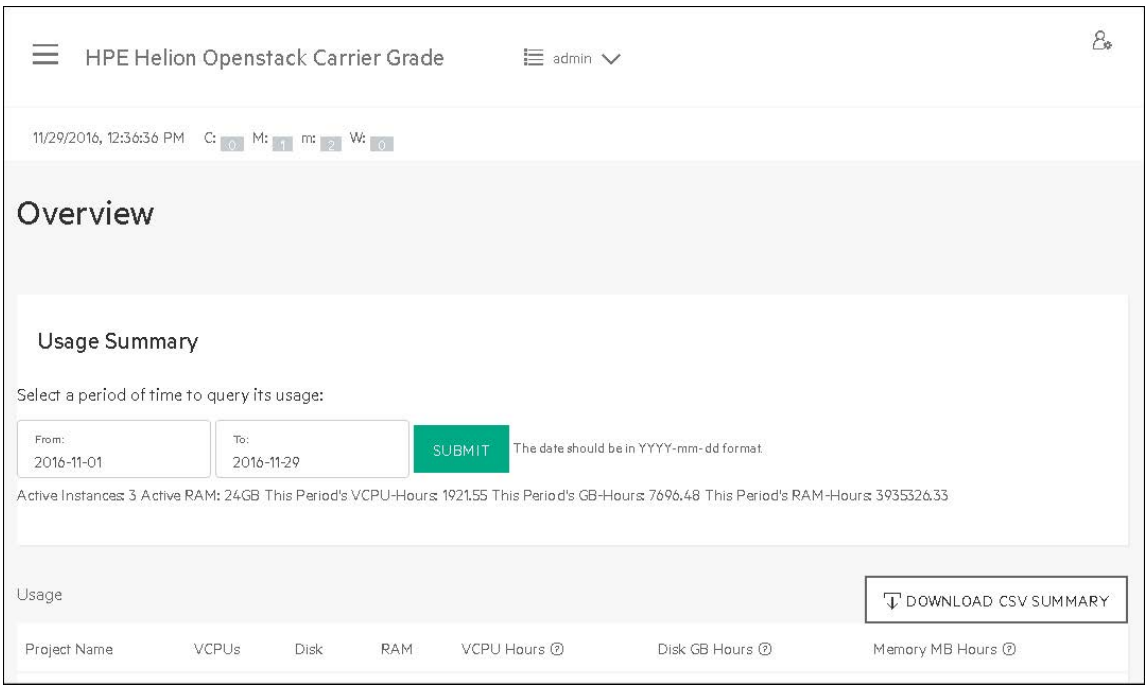
The HCG 4.0 web administration interface provides an active alarm counts banner in the page header at the top right of all screens.

The global alarm banner can be seen only by users with admin privileges.

The global alarm banner provides a color-coded snapshot of current active alarm counts for each alarm severity.

NOTE: Suppressed alarms are not shown. For more about suppressed alarms, see Events Suppression on page 219.

Clicking on the alarm banner opens the Fault Management page, where more detailed information about the alarms is provided.



Viewing the Event Log Using the Web Interface

The HCG 4.0 web administration interface provides a convenient way to work with historical alarms, events, and customer logs.

Procedure

1. Select **Admin** > **Platform** > **Fault Management** in the left pane.
2. Select **Event Log** at the top of the Fault Management window.

   The Event Logs window appears. By default, the Event Logs screen shows all events, including both historical set/clear alarms and logs.
3. Use the **All Events**, **Alarm Events**, and **Log Events** buttons at the top of the Event Logs window to select the information you want to view. You can also use the **Show Suppressed** and **Hide Suppressed** buttons to show and hide, respectively, any currently suppressed alarms.

   You can sort the entries by clicking on the column titles. For example, to sort the view of the entries by severity, click **Severity**; the entries are resorted and grouped by severity.

   You can also filter entries using the **Filter** text box. Type the filter string, and then click the magnifying-glass icon. The results include only those entries that contain the string.
4. Optional: Use the **Default Limit** drop-down list to select a new default limit on the number of items displayed per page of the table.

Viewing the Event Log Using the CLI

You can use CLI commands to work with historical alarms and logs in the event log.

Prerequisites

You must be logged in with administrative privileges.

To acquire Keystone **admin** credentials, use the following command:

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

- Use the **system event-list** command to view historical alarms and logs. By default, only unsuppressed events are shown. For more about event suppression, see Events Suppression on page 219

  The syntax of the command is:

  ```
  system event-list [-q <QUERY>] [-l <NUMBER>] [--alarms] [--logs] [--include-
  suppress]
  ```

  Optional arguments:

  -q <QUERY>, **--query <QUERY>** - key[op]data_type::value; list. data_type is optional, but if supplied must be string, integer, float, or boolean.

  -l <NUMBER>, **--limit <NUMBER>**- Maximum number of event logs to return.

  --alarms - Show alarms only.

  --logs - Show logs only.

  --include-suppress - Show suppressed alarms as well as unsuppressed alarms.

Examples

The default usage, shown here, views all unsuppressed alarms and logs, but uses the **-l** option to limit the output to five entries.

The output of the command is split in three parts below for presentation purposes only.

```
[wrsroot@controller-0 ~(keystone_admin)]$ system event-list -l 5
+--------------------+----------------------------+-------+--------------
| UUID               | Time Stamp                 | State | Event Log ID
+--------------------+----------------------------+-------+--------------
| 313c8279-0ec4-49...| 2016-03-08T18:01:28.912411 | log   | 200.022
| 7f2acb58-95af-42...| 2016-03-08T18:01:28.695433 | log   | 200.022
| eb0dfd57-77e1-42...| 2016-03-08T18:01:23.490504 | set   | 200.004
| 20cb1439-7f84-41...| 2016-03-08T18:01:23.474510 | set   | 200.005
| dd529673-5988-43...| 2016-03-08T18:01:21.255716 | set   | 200.005
+--------------------+----------------------------+-------+--------------

+--------------------------------------------------------------------------
| Reason Text
+--------------------------------------------------------------------------
| controller-1 is 'disabled-failed' to the system
| controller-1 is now 'disabled'
| controller-1 ... failure. Host is being auto recovered by Reboot.
| controller-1 ... critical 'Management Network' communication failure.
| controller-1 ... exceeded its lower alarming threshold.
+--------------------------------------------------------------------------

+-------------------------------------+----------------+
| Entity Instance ID                  | Severity       |
+-------------------------------------+----------------+
```

```
| host=controller-1.status=failed      | not-applicable |
| host=controller-1.state=disabled     | not-applicable |
| host=controller-1                    | critical       |
| host=controller-1.network=Management | critical       |
| host=controller-1.network=Management | major          |
+--------------------------------------+----------------+
[wrsroot@controller-0 ~(keystone_admin)]$
```

In the following example, the **system event-list** command shows alarms only; the **State** column indicates either **set** or **clear**.

The output of the command is split in three parts below for presentation purposes only.

```
[wrsroot@controller-0 ~(keystone_admin)]$ system event-list -l 5 --alarms
+--------------------+----------------------------+-------+--------------
| UUID               | Time Stamp                 | State | Event Log ID
+--------------------+----------------------------+-------+--------------
| eb0dfd57-77e1-42...| 2016-03-08T18:01:23.490504 | set   | 200.004
| 20cb1439-7f84-41...| 2016-03-08T18:01:23.474510 | set   | 200.005
| dd529673-5988-43...| 2016-03-08T18:01:21.255716 | set   | 200.005
| 33592561-520f-49...| 2016-03-08T18:01:09.433405 | set   | 400.002
| 92f743b4-8e3e-4d...| 2016-03-08T18:01:09.418902 | set   | 400.002
+--------------------+----------------------------+-------+--------------

+-----------------------------------------------------------------------------
| Reason Text
+-----------------------------------------------------------------------------
| controller-1 ... failure. Host is being auto recovered by Reboot.
| controller-1 ... 'Management Network' communication failure.
| controller-1 ... failures that have exceeded lower alarming threshold.
| Service group oam-services loss of redundancy; ...
| Service group controller-services loss of redundancy; ...
+-----------------------------------------------------------------------------

+-------------------------------------------------------------+----------+
| Entity Instance ID                                          | Severity |
+-------------------------------------------------------------+----------+
| host=controller-1                                           | critical |
| host=controller-1.network=Management                        | critical |
| host=controller-1.network=Management                        | major    |
| service_domain=controller.service_group=oam-services        | major    |
| service_domain=controller.service_group=controller-services | major    |
+-------------------------------------------------------------+----------+

[wrsroot@controller-0 ~(keystone_admin)]$
```

In this example, the **system event-list** command shows logs only; the **State** column indicates **log**.

The output of the command is split in three parts below for presentation purposes only.

```
[wrsroot@controller-0 ~(keystone_admin)]$ system event-list -l 5 --logs
+--------------------+----------------------------+-------+--------------
| UUID               | Time Stamp                 | State | Event Log ID
+--------------------+----------------------------+-------+--------------
| 980a6f11-4c1a-4f... | 2016-03-08T18:02:02.113072 | log   | 200.022
| 313c8279-0ec4-49... | 2016-03-08T18:01:28.912411 | log   | 200.022
| 7f2acb58-95af-42... | 2016-03-08T18:01:28.695433 | log   | 200.022
| 932e20eb-74a8-4e... | 2016-03-08T18:01:09.064913 | log   | 401.002
| a89a468c-0629-42... | 2016-03-08T18:01:08.831612 | log   | 401.002
+--------------------+----------------------------+-------+--------------

+-----------------------------------------------------------------------------
| Reason Text
+-----------------------------------------------------------------------------
| controller-1 is now 'offline'
| controller-1 is 'disabled-failed' to the system
| controller-1 is now 'disabled'
| Service group oam-services loss of redundancy; expected 1 standby...
| Service group controller-services loss of redundancy; expected 1 standby
+-----------------------------------------------------------------------------
```

```
+------------------------------------------------------------+----------------+
| Entity Instance ID                                         | Severity       |
+------------------------------------------------------------+----------------+
| host=controller-1.status=offline                           | not-applicable |
| host=controller-1.status=failed                            | not-applicable |
| host=controller-1.state=disabled                           | not-applicable |
| service_domain=controller.service_group=oam-services       | critical       |
| service_domain=controller.service_group=controller-services | critical       |
+------------------------------------------------------------+----------------+

[wrsroot@controller-0 ~(keystone_admin)]$
```

Viewing Active Alarms Using the Web Interface

The HCG 4.0 web administration interface provides a convenient way to work with active alarms.

- Select **Admin** > **Platform** > **Fault Management** in the left pane.

  The Active Alarms window appears by default when you select **Fault Management**.

  A color-coded summary count of active alarms is shown at the top of the screen, above the list of active alarms.

  You can sort the entries by clicking on the column titles. For example, to sort the view of the entries by severity, click **Severity**; the entries are resorted and grouped by severity.

  You can also filter entries using the **Filter** text box. Type the filter string, and then click the magnifying-glass icon. The results include only those entries that contain the string.

  You can use the **Show Suppressed** and **Hide Suppressed** buttons to show and hide, respectively, any currently suppressed alarms.

NOTE: For provider networks and compute host data interfaces, you can also use the Provider Network Topology view to monitor active alarms. For more information, see The Provider Network Topology View on page 23.

Viewing Active Alarms Using the CLI

You can use the CLI to find information about currently active system alarms.

Prerequisites

You must be logged in with administrative privileges.

To acquire Keystone **admin** credentials, use the following command:

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

You can view currently active alarms through the CLI using the commands:

- **system alarm-list [-q <QUERY>] --include_suppress**
- **system alarm-show**

Examples and usage information for each of these commands is given below.

Examples

system alarm-list

The command **system alarm-list** lists currently active alarms, as illustrated below (the output is split in two pieces for presentation purposes only).

This example lists a single critical alarm on host **controller-0** regarding running out of space on disk unit **/dev/sda3**. Each alarm object is listed with a unique UUID which you can use to obtain additional information.

```
~(keystone_admin)$ system alarm-list

+--------------+----------+--------------------+----------+---------------
| UUID         | Alarm ID | Entity Instance ID | Severity |  Time Stamp
+--------------+----------+--------------------+----------+---------------
| 4ab5698a-... | 100.104  | host=controller-0  | critical |  2014-06-25...
+--------------+----------+--------------------+----------+---------------

--+-------------------------------------------------------------+
  | Reason Text                                                 |
--+-------------------------------------------------------------+
  | /dev/sda3 severity critical threshold set (0.00 MB left) |
--+-------------------------------------------------------------+
```

You can use one of the following **--query** command filters to view specific subsets of alarms, or a particular alarm:

Query Filter	Comment
uuid=<uuid>	Query alarms by UUID, for example: `$ system alarm-list --query uuid=4ab5698a-19cb...`
alarm_id=<alarm id>	Query alarms by alarm ID, for example: `$ system alarm-list --query alarm_id=100.104`

alarm_type=<type>	Query alarms by type, for example:
	`$ system alarm-list --query \`
	`alarm_type=operational-violation`

entity_type_id=<type id>	Query alarms by entity type ID, for example:
	`$ system alarm-list --query \`
	`entity_type_id=system.host`

entity_instance_id=<instance id>	Query alarms by entity instance id, for example:
	`$ system alarm-list --query \`
	`entity_instance_id=host=compute-0`

Query Filter	Comment
severity=<severity>	Query alarms by severity type, for example: `$ system alarm-list --query severity=warning` The valid severity types are *critical*, *major*, *minor*, and *warning*.

Query command filters can be combined into a single expression separated by semicolons, as illustrated in the following example:

```
$ system alarm-list -q
'alarm_id=400.002;entity_instance_id=service_domain=controller.service_group=directo
ry-services'
```

You can also use the **--include_suppress** option. This option indicates that all active alarms should be displayed, including suppressed alarms. Suppressed alarms are displayed with their Alarm ID set to **S***(alarm-id)*

system alarm-show

The command **system alarm-show** presents additional information about a currently active alarm, as illustrated below:

```
~(keystone_admin)$ system alarm-show 4ab5698a-19cb-4c17-bd63-302173fef62c

+------------------------+------------------------------------------------+
| Property               | Value                                          |
+------------------------+------------------------------------------------+
| alarm_id               | 100.104                                        |
| alarm_state            | set                                            |
| alarm_type             | operational-violation                          |
| entity_instance_id     | system=hp380-1_4.host=controller-0             |
| entity_type_id         | system.host                                    |
| probable_cause         | threshold-crossed                              |
| proposed_repair_action | /dev/sda3 check usage                          |
| reason_text            | /dev/sda3 critical threshold set (0.00 MB left) |
| service_affecting      | False                                          |
| severity               | critical                                       |
| suppression            | True                                           |
| timestamp              | 2014-06-25T16:58:57.324613                     |
| uuid                   | 4ab5698a-19cb-4c17-bd63-302173fef62c           |
+------------------------+------------------------------------------------+
```

The pair of attributes **(alarm_id, entity_instance_id)** uniquely identifies an active alarm:

alarm_id

An ID identifying the particular alarm condition. Note that there are some alarm conditions, such as *administratively locked*, that can be raised by more than one entity-instance-id.

entity_instance_id

Type and instance information of the object raising the alarm. A period-separated list of (key, value) pairs, representing the containment structure of the overall entity instance. This structure is used for processing hierarchical clearing of alarms.

Deleting an Alarm

You can delete an alarm when it is not automatically cleared.

Manually deleting an alarm should not be done unless it is absolutely clear that there is no reason for the alarm to be active.

You can use the command **system alarm-delete** to manually delete an alarm that remains active for no apparent reason, which may happen in rare conditions. Alarms usually clear automatically when the trigger condition is corrected.

- To delete an alarm, use the **system alarm-delete** command as shown below:

```
~(keystone_admin)$ system alarm-delete 4ab5698a-19cb-4c17-bd63-302173fef62c
```

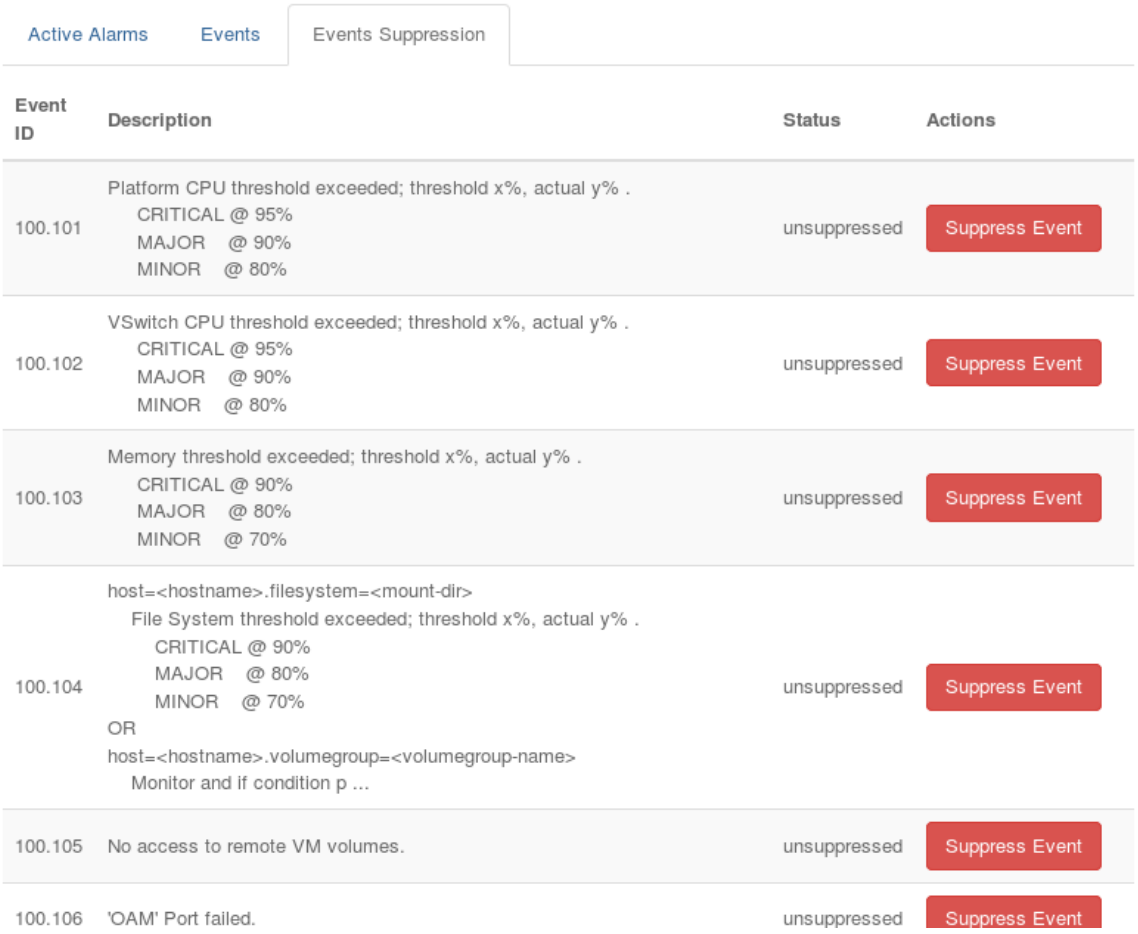
Events Suppression

HCG 4.0 provides the ability to suppress alarms.

All alarms are unsuppressed by default. A suppressed Alarm will not appear in the Active Alarm or Events displays, on Horizon, the CLI, or SNMP, and will not be included in the Active Alarm Counts. Suppressing an Alarm will result in the system NOT notifying the operator of this particular fault.

The Events Suppression tab on the Fault Management page, available from **Admin** > **Platform** > **Fault Management** in the left-hand pane, provides the suppression status of each event and functionality for suppressing or unsuppressing each event.

As shown below, the Events Suppression tab lists each event by ID, and provides a description of the event and a current status indicator. Each event can be suppressed using the **Suppress Event** button.



Suppressing and Unsuppressing Events

You can set events to a suppressed state and toggle them back to unsuppressed.

Procedure

1. Open the Events Suppression tab on the Fault Managementpage, available from **Admin** > **Platform** > **Fault Management** in the left-hand pane.

   The Events Suppression tab appears. It provides the status of each event and functionality for suppressing or unsuppressing each event, depending on the current status of the event.

2. Locate the event ID that you want to suppress.

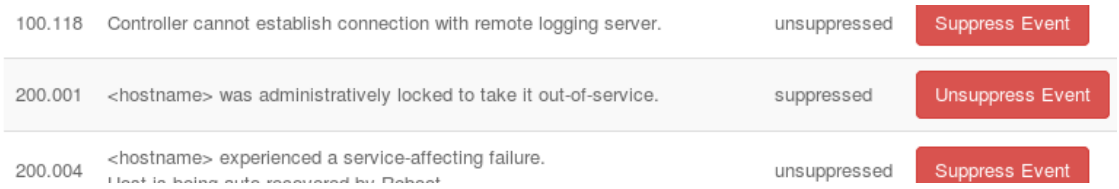
3. Click the **Suppress Event** button for that event.

   You are prompted to confirm that you want to suppress the event.

⚠ **CAUTION:** Suppressing an Alarm will result in the system *not* notifying the operator of this particular fault.

4. Click **Suppress Event** in the Confirm Suppress Event dialog box.

   The Events Suppression tab is refreshed to show the selected event ID with a status of Suppressed, as shown below. The **Suppress Event Suppress** button is replaced by **Unsuppress Event**, providing a way to toggle the event back to unsuppressed.



Viewing Suppressed Alarms Using the CLI

You can view a list of currently suppressed alarms using the CLI.

- Use the **system event-suppress-list** CLI command to view a list of all currently suppressed alarms.

  This command shows all alarm IDs along with their suppression status.

```
~(keystone_admin)$  system event-suppress-list \
[--nopaging] [--uuid] [--include-unsuppressed]
```

  where

  --nopaging

  disables paged output

  --uuid

  includes the alarm UUIDs in the output

  --include-unsuppressed

  includes unsuppressed alarm IDs in the output

For example:

```
[wrsroot@controller-0 ~(keystone_admin)] system event-suppress-list

+----------+-------------+
| Event ID | Status      |
+----------+-------------+
| 100.101  | suppressed  |
| 100.103  | suppressed  |
| 100.105  | suppressed  |

      ...
+----------+-------------+
```

Suppressing an Alarm Using the CLI

You can use the CLI to suppress alarms.

Procedure

Use the **system event-suppress** to suppress a single alarm or multiple alarms by ID.

```
~(keystone_admin)$ system event-suppress [--nowrap] --alarm id alarm_ id[,alarm-id] \
[--nopaging] [--uuid]
```

where

alarm-id

is the **Alarm ID** of an alarm.

--nowrap

disables output wrapping

--nopaging

disables paged output

--uuid

includes the alarm UUIDs in the output

An error message is generated in the case of an invalid <*alarm-id*>: **Alarm ID not found: <alarm-id>**.

If the specified number of Alarm IDs is greater than 1, and at least 1 is wrong, then the suppress command is not applied (none of the specified Alarm IDs are suppressed).

NOTE: Suppressing an Alarm will result in the system NOT notifying the operator of this particular fault.

Unsuppressing an Alarm Using the CLI

You can unsuppress an alarm using the CLI.

Procedure

Use the **system event-unsuppress** CLI command to unsuppress a currently suppressed alarm.

```
~(keystone_admin)$ system event-unsuppress [--nowrap] --alarm_id alarm-id[,alarm-id] \
[--nopaging] [--uuid]
```

where

alarm-id

is the **Alarm ID** of an alarm to unsuppress

--nowrap

disables output wrapping

--nopaging

disables paged output

--uuid

includes the alarm UUIDs in the output

Alarm(s) with the specified *alarm-id(s)* will be unsuppressed.

You can unsuppress all currently suppressed alarms using the following command:

```
~(keystone_admin)$ system event-unsuppress -all [--nopaging] [--uuid]
```

CLI Commands and Paged Output

There are some system CLI commands that perform paging, and you can use options to limit the paging or to disable it, which is useful for scripts.

CLI system commands that perform paging include:

- **system event-list**
- **system event-suppress**
- **system event-suppress-list**
- **system event-unsuppress**
- **system event-unsuppress-all**

To turn paging off, use the **--nopaging** option for the above commands. The **--nopaging** option is useful for bash script writers.

Examples

The following examples demonstrate the resulting behavior from the use and non-use of the paging options.

This produces a paged list of events.

```
$ system event-list
```

This produces a list of events without paging.

```
$ system event-list --nopaging
```

This produces a paged list of 50 events.

```
$ system event-list --limit 50
```

This will produce a list of 50 events without paging.

```
$ system event-list --limit 50 --nopaging
```

SNMP

HCG 4.0 can generate SNMP traps for HCG 4.0 Alarm Events and Customer Log Events.

This includes alarms based on hardware sensors monitored by board management modules, if present. For more information, see Sensors Tab on page 70.

About SNMP Support

Support for SNMP is implemented as follows:

- access is disabled by default, must be enabled manually from the command line interface
- available using the controller's node floating OAM IP address, over the standard SNMP UDP port 161
- supported version is SNMPv2c
- access is read-only for all SNMP communities
- all SNMP communities have access to the entire OID tree, there is no support for *VIEWS*
- supported SNMP operations are *GET*, *GETNEXT*, *GETBULK*, and *SNMPv2C-TRAP2*
- the SNMP *SET* operation is not supported

SNMPv2-MIB (RFC 3418)

Support for the basic standard MIB for SNMP entities is limited to the System and SNMP groups, as follows:

- System Group, **.iso.org.dod.internet.mgmt.mib-2.system**
- SNMP Group, **.iso.org.dod.internet.mgmt.mib-2.snmp**
- coldStart and warmStart Traps

The following system attributes are used in support of the SNMP implementation. They can be displayed using the **system show** command.

contact

A read-write system attribute used to populate the **sysContact** attribute of the SNMP System group. The contact value can be set with the following command:

```
~(keystone_admin)$ system modify contact="the-site-contact"
```

location

A read-write system attribute used to populate the **sysLocation** attribute of the SNMP System group. The location value can be set with the following command:

```
~(keystone_admin)$ system modify location="some-location"
```

name

A read-write system attribute used to populate the **sysName** attribute of the SNMP System group. The name value can be set with the following command:

```
~(keystone_admin)$ system modify name="the-system-name"
```

software_version

A read-only system attribute set automatically by the system. Its value is used to populate the **sysDescr** attribute of the SNMP System group.

The following SNMP attributes are used as follows:

sysObjectId

Set to **iso.org.dod.internet.private.enterprise.hpe.hcg** (1.3.6.1.4.1.1.2).

sysUpTime

Set to the up time of the active controller.

sysServices

Set to the nominal value of 72 to indicate that the host provides services at layers 1 to 7.

HCG 4.0 Enterprise MIBs

HCG 4.0 supports the HCG 4.0 *Enterprise Registration* and *Alarm* MIBs.

Enterprise Registration MIB, wrsEnterpriseReg.mib

Defines the HCG 4.0 hierarchy underneath the **iso(1).org(3).dod(6).internet(1).private(4).enterprise(1)**. This hierarchy is administered as follows:

- **.wrs(731)**, the IANA-registered enterprise code for HCG 4.0
- **.wrs(731).wrsCommon(1).wrs<Module>(1-...)**, defined in **wrsCommon<Module>.mib**.
- **.wrs(731).wrsProduct(2-...)**, defined in **wrs<Product>.mib**.

Alarm MIB, wrsAlarmMib.mib

Defines the common TRAP and ALARM MIBs for HCG 4.0 products. The definition includes *textual conventions*, an *active alarm table*, a *historical alarm table*, a *customer log table*, and *traps*.

Textual Conventions

Semantic statements used to simplify definitions in the active alarm table and traps components of the MIB.

Tables

See SNMP Event Table on page 228 for detailed descriptions.

Traps

See Traps on page 226 for detailed descriptions.

Enabling SNMP Support

In order to have a workable SNMP configuration you must use the command line interface on the active controller to:

1. Define at least one SNMP community string. See Adding an SNMP Community String on page 228 for details.
2. Configure at least one SNMP trap destination so that alarms and logs can be reported as they happen. For more information, see Configuring SNMP Trap Destinations on page 226.

Traps

HCG 4.0 supports SNMP traps. Traps send unsolicited information to monitoring software when significant events occur..

The following traps are defined.

- **wrsAlarmCritical**
- **wrsAlarmMajor**
- **wrsAlarmMinor**
- **wrsAlarmWarning**
- **wrsAlarmMessage**
- **wrsAlarmClear**
- **wrsAlarmHierarchicalClear**

NOTE: Customer Logs always result in **wrsAlarmMessage** traps.

For Critical, Major, Minor, Warning, and Message traps, all variables in the active alarm table are included as *varbinds*.

For the Clear trap, *varbinds* include only the *AlarmID*, *EntityInstanceID*, *DateAndTime*, and *ReasonText* variables.

For the HierarchicalClear trap, *varbinds* include only the *EntityInstanceID*, *DateAndTime*, and *ReasonText* variables.

For all alarms, the Notification Type is based on the severity of the trap or alarm. This is done to facilitate the interaction with most SNMP trap viewers which typically use the Notification Type to drive the coloring of traps, that is, red for critical, yellow for minor, and so on.

Configuring SNMP Trap Destinations

SNMP trap destinations are hosts configured in HCG 4.0 to receive unsolicited SNMP notifications.

Destination hosts are specified by IP address, or by host name if it can be properly resolved by HCG 4.0. Notifications are sent to the hosts using a designated community string so that they can be validated.

Procedure

1. Configure IP address 10.10.10.1 to receive SNMP notifications using the community string *commstr1*.

```
~(keystone_admin)$ system snmp-trapdest-add -c commstr1 --ip_address 10.10.10.1
+------------+----------------------------------------+
| Property   | Value                                  |
```

```
+------------+--------------------------------------+
| uuid       | c7b6774e-7f45-40f5-bcca-3668de2a186f |
| ip_address | 10.10.10.1                           |
| community  | commstr1                             |
| type       | snmpv2c_trap                         |
| port       | 162                                  |
| transport  | udp                                  |
+------------+--------------------------------------+
```

The following are attributes associated with the new community string:

uuid

The UUID associated with the trap destination object.

ip_address

The trap destination IP address.

community

The community string value to be associated with the notifications.

type

snmpv2c_trap, the only supported message type for SNMP traps.

port

The destination UDP port that SNMP notifications are sent to.

transport

The transport protocol used to send notifications.

2. List defined trap destinations.

```
~(keystone_admin)$ system snmp-trapdest-list
+------------+----------------+------+--------------+------------+
| IP Address  | SNMP Community | Port | Type         | Transport |
+-------------+----------------+------+--------------+------------+
| 10.10.10.1  | commstr1       | 162  | snmpv2c_trap | udp       |
+-------------+----------------+------+--------------+------------+
```

3. Query access details of a specific trap destination.

```
~(keystone_admin)$ system snmp-trapdest-show 10.10.10.1
+------------+--------------------------------------+
| Property   | Value                                |
+------------+--------------------------------------+
| uuid       | c7b6774e-7f45-40f5-bcca-3668de2a186f |
| ip_address | 10.10.10.1                           |
| community  | commstr1                             |
| type       | snmpv2c_trap                         |
| port       | 162                                  |
| transport  | udp                                  |
+------------+--------------------------------------+
```

4. Disable the sending of SNMP notifications to a specific IP address.

```
~(keystone_admin)$ system snmp-trapdest-delete 10.10.10.1
Deleted ip 10.10.10.1
```

SNMP Event Table

HCG 4.0 supports SNMP active and historical alarms, and customer logs, in an event table.

The event table contains historical alarms (*sets* and *clears*) alarms and customer logs. It does not contain active alarms. Each entry in the table includes the following variables:

- *UUID*
- *EventID*
- *State*
- *EntityInstanceID*
- *DateAndTime*
- *EventSeverity*
- *ReasonText*
- *EventType*
- *ProbableCause*
- *ProposedRepairAction*
- *ServiceAffecting*
- *SuppressionAllowed*

NOTE: The previous SNMP Historical Alarm Table and the SNMP Customer Log Table are still supported but marked as deprecated in the MIB.

Adding an SNMP Community String

To enable SNMP services you need to define one or more SNMP community strings using the command line interface.

No default community strings are defined on HCG 4.0 after the initial commissioning of the cluster. This means that no SNMP operations are enabled by default.

The following exercise illustrates the system commands available to manage and query SNMP community strings. It uses the string **commstr1** as an example.

CAUTION: For security, do not use the string **public**, or other community strings that could easily be guessed.

Prerequisites

All commands must be executed on the active controller's console, which can be accessed using the OAM floating IP address. You must acquire Keystone **admin** credentials in order to execute the commands.

Procedure

1. Add the SNMP community string *commstr1* to the system.

```
~(keystone_admin)$ system snmp-comm-add -c commstr1
+-----------+--------------------------------------+
| Property  | Value                                |
+-----------+--------------------------------------+
| access    | ro                                   |
| uuid      | eccf5729-e400-4305-82e2-bdf344eb868d |
| community | commstr1                             |
| view      | .1                                   |
+-----------+--------------------------------------+
```

   The following are attributes associated with the new community string:

   access

   The SNMP access type. In HCG 4.0 all community strings provide read-only access. uuid

   The UUID associated with the community string.

   community

   The community string value.

   view

   The is always the full MIB tree.

2. List available community strings.

```
~(keystone_admin)$ system snmp-comm-list
+----------------+--------------------+--------+
| SNMP community | View               | Access |
+----------------+--------------------+--------+
| commstr1       | .1                 | ro     |
+----------------+--------------------+--------+
```

3. Query details of a specific community string.

```
~(keystone_admin)$ system snmp-comm-show commstr1
+------------+--------------------------------------+
| Property   | Value                                |
+------------+--------------------------------------+
| access     | ro                                   |
| created_at | 2014-08-14T21:12:10.037637+00:00     |
| uuid       | eccf5729-e400-4305-82e2-bdf344eb868d |
| community  | commstr1                             |
| view       | .1                                   |
+------------+--------------------------------------+
```

4. Delete a community string.

```
~(keystone_admin)$ system snmp-comm-delete commstr1
Deleted community commstr1
```

Community strings in HCG 4.0 provide query access to any SNMP monitor workstation that can reach the controller's OAM address on UDP port 161.

You can verify SNMP access using any monitor tool. For example, the freely available command **snmpwalk** can be issued from any host to list the state of all SNMP Object Identifiers (OID):

```
$ snmpwalk -v 2c -c commstr1 10.10.10.100 > oids.txt
```

In this example, 10.10.10.100 is the HCG 4.0 OAM floating IP address. The output, which is a large file, is redirected to the file **oids.txt**.

Centralized Log Collection and Analysis

You can configure HCG 4.0 to send detailed system logs from all hosts to a remote log server for centralized review and analysis.

You can also set up your own dashboards for viewing log details.

When centralized logging is enabled, logs written to the **/var/log** directory on each host are also sent to a remote log server. System logs used for troubleshooting and advanced analysis are included, along with the customer logs normally accessed from the CLI or web administration interface. By centralizing the logs, advanced users can apply powerful searches and advanced visualizations to examine the behavior of the system.

Each host sends logs through the Active Controller to a remote log server over the OAM network using either TCP or UDP. For added security, you can optionally configure a TLS connection. At the log server, an ELK (Elasticsearch, Kibana, Logstash) stack collects and presents the information.

Logstash

collects the logs

Elasticsearch

provides a search engine

Kibana

provides web-based visualization

The ELK stack is a widely-used source log analytics engine, with ample documentation and tutorials on the Internet. The HCG 4.0 SDK includes custom searches and filters for use with a HCG 4.0 system.

To set up and use a log server, see *Helion OpenStack Carrier Grade 4.0 System Administration:* *Configuring Centralized Log Collection on page 230*.

Configuring Centralized Log Collection

To configure centralized log collection, you must set up a remote server as a log server using a HCG 4.0 SDK utility, and then enable remote logging on HCG 4.0 using the CLI.

For more information about the SDK, including an overview of its components and how to access them, see the *HCG 4.0 Software Development Kit*.

Procedure

1. Set up a server to act as the log server.

For more information, see Hardware and Software Requirements for a Remote Log Server on page 231.

2. Assign the log server an IP address accessible from the HCG 4.0 OAM network.
3. Run a script to configure the log server with an ELK stack and HCG 4.0 custom searches and filters.

   For more information, see Configuring the Remote Log Server on page 231.
4. Enable remote logging on the HCG 4.0.

   For more informaton, see Configuring Remote Logging on HCG 4.0 on page 233.

Hardware and Software Requirements for a Remote Log Server

For centralized log collection, a properly equipped and configured log server is required.

- The server must use a supported version of CentOS or Ubuntu.

  For specific supported OS versions, refer to the README file included with the Remote Log Server component of the HCG 4.0 SDK.
- The hardware must meet the minimum requirements for the operating system.
- The server must be configured with an ELK stack.

  For users unfamiliar with ELK, the HCG 4.0 SDK includes a utility for installing and configuring a basic ELK stack setup.
- The server must be assigned an IP address accessible from the HCG 4.0 OAM network.

.

Configuring the Remote Log Server

The HCG 4.0 SDK includes a script for configuring a server as a remote log server using an ELK stack. You can use this if you are unfamiliar with ELK, or do not already have an ELK installation.

The script installs a basic ELK stack for log collection and presentation, and configures it to receive logs from HCG 4.0 at a specified address and port.

For added security, you can enable TLS during installation, specifying a private key and a certificate installed on the remote log server.

NOTE: Currently the Remote Log Server certificate received by HCG 4.0 on negotiating a TLS connection is not authenticated, but is used for encryption.

For more information about using the SDK, see the *HCG 4.0 Software Development Kit*.

Prerequisites

For log server specifications, see Hardware and Software Requirements for a Remote Log Server on page 231.

You must set up a network interface with an appropriate IP address on the server.

Procedure

1. Ensure that the remote server can access the HCG 4.0 OAM network.
2. Extract the Remote Log Server **tar** file included with the SDK.

   ```
   $ tar xfv wrs-install-log-server-1.0.0.tgz
   ```

3. Change to the extracted directory.

   ```
   $ cd install-log-server
   ```

4. Run the script to configure the log server.

   The **install-log-server.sh** script installs an ELK stack on the server.

   ```
   $ ./install-log-server.sh -i ip-address [-p port] \
   [-u] [-t [-k privatekey -c certificate]]
   ```

   where

   ip-address

   is the listening IP address

   port

   is the listening port. The default value is 514.

   -u

   enables UDP connections on the remote logging server. This can be used along with the **-t** option to enable both UDP and TCP.

   -t

   enables TCP connections on the remote logging server. This can be used along with the **-u** option to enable both TCP and UDP.

   NOTE: The -t option can be used together with the **-k** and **-c** options to enable TLS.

   privatekey

   is the name of a private key file installed on the remote log server

   certificate

   is the name of a certificate file installed on the remote log server

   For example:

   ```
   $ ./install-log-server.sh -i 128.224.186.92
   ```

Postrequisites

To begin using the log server, you must enable remote logging on the THCG 4.0. For more information, see Configuring Remote Logging on HCG 4.0 on page 233.

Configuring Remote Logging on HCG 4.0

To begin sending logs from HCG 4.0 to a remote log server, you must enable remote logging on the system, and then unlock each host to make the configuration change take effect.

You must use the CLI to change the remote logging configuration. This operation is not supported using the web administration interface.

Prerequisites

A correctly configured remote log server is required. For more information, see Configuring the Remote Log Server on page 231.

Procedure

1. Log in to the active controller and become the Keystone admin user.

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

2. Lock the standby controller.

```
~(keystone_admin)$ system host-lock controller-1
```

3. Use the **system remotelogging-modify** command to enable remote logging.

   Use a command of the following form:

```
[~(keystone_admin)]$  system remotelogging-modify --ip_address  server_address \
--transport transport_mode --enabled state
```

   where

   server_address

   is the IP address of the remote log server

   transport_mode

   is the transport protocol to use. Valid values are **tcp**, **udp**, or **tls**.

   NOTE: Currently the Remote Log Server certificate received by HCG 4.0 on negotiating a TLS connection is not authenticated, but is used for encryption.

   state

   is **True** to enable logging, or **False** to disable logging

   For example:

```
[~(keystone_admin)]$  system remotelogging-modify --ip_address 128.224.186.92 \
--transport tcp --enabled True

+------------+--------------------------------------+
| Property   | Value                                |
+------------+--------------------------------------+
| uuid       | 36bccb60-d560-4f15-aadc-d626579225d3 |
| ip_address | 128.224.186.92                       |
| enabled    | True                                 |
| transport  | tcp                                  |
```

```
| port       | 514                                  |
| created_at | 2016-06-07T19:12:30.002272+00:00     |
| updated_at | None                                 |
+------------+--------------------------------------+
```

4. Unlock the standby controller.

```
[~(keystone_admin)]$  system host-unlock controller-1
```

5. Swact the controllers.

```
[~(keystone_admin)]$  system host-swact controller-0
```

6. Lock the new standby controller.

```
[~(keystone_admin)]$  system host-lock controller-0
[~(keystone_admin)]$  system host-unlock controller-0
```

7. Lock and unlock all other hosts.

CAUTION: Before locking a compute host, ensure that any hosted VMs are stopped or migrated.

```
[~(keystone_admin)]$  system host-lock compute-1

[~(keystone_admin)]$  system host-lock compute-0

[~(keystone_admin)]$  system host-unlock compute-1

[~(keystone_admin)]$  system host-unlock compute-0
```

Using the Remote Log Server

The remote log server uses ELK, a popular open-source log analytics engine that includes Kibana for web-based presentation and analysis.

More information about Kibana and ELK, including documentation and tutorials, is widely available on the Internet.

For more information about deploying a remote log server, see Centralized Log Collection and Analysis on page 230.

NOTE: If HCG 4.0 loses connectivity with the remote server, an alarm message is raised.

Procedure

1. Use a browser to open Kibana on the log server.

   Use the form **http://*ip_addr*:5601**, where *ip_addr* is the IP address of the remote log server.

2. Use the controls in Kibana to view or analyze logs from HCG 4.0.

   For help using Kibana, refer to the public documentation on the Internet.

A

Utilities for vSwitch

Utilities for vSwitch

You can query virtual switch (vSwitch) instances in HCG 4.0, and perform packet tracing on vSwitch interfaces.

In HCG 4.0, an accelerated virtual switch (AVS) runs on each compute host, providing Layer 2 switching for the virtual machines instantiated on the host. Up to 254 ports are supported for each host; this total includes physical, guest, and host ports.

You can use the **vshell** utility to query the status of each vSwitch and collect performance statistics. You can use the **vtrace** utility to perform packet trace operations.

Querying vSwitch

You can use the **vshell** command-line utility to query the internal state of the virtual switch on a compute host.

The **vshell** utility reports information for the vSwitch running on a compute host. This can be useful for debugging network-related issues.

You can run the utility from the active controller, or locally on the compute host. You must be logged in with root privileges.

To run **vshell**, use the following syntax:

```
$ sudo vshell [-H hostname] command
```

Where:

hostname

is the name of the host, if the utility is run from the controller.

command

is the vshell command to run.

Commonly Used vshell Commands

The most common commands are listed below.

For more information, use the following command:

```
$ sudo vshell help
```

NOTE: The sample outputs in this section have been truncated or otherwise modified to fit the available space.

engine-list

Lists details for the packet processing engine.

```
$ sudo vshell -H compute-1 engine-list
+---------+----+-------+-----------+-----------+-----------+
| uuid    | id | cpuid | socket-id | rxq-count | txq-count |
+---------+----+-------+-----------+-----------+-----------+
| dfcd... | 0  | 1     | 0         | 29        | 41        |
| ef55... | 1  | 2     | 0         | 28        | 41        |
+---------+----+-------+-----------+-----------+-----------+
```

port-list

Lists attributes for virtual and physical ports.

```
$ sudo vshell -H compute-1 port-list
+-------+----+-----------+-----------+-------------+------------+------+
| uuid  | id | type      | socket-id | admin-state | link-state | mtu  |
+-------+----+-----------+-----------+-------------+------------+- ----+
| 21... | 0  | physical  | 0         | up          | up         | 1600 |
| d9... | 1  | physical  | 0         | up          | up         | 1600 |
| fd... | 2  | avp-guest | 0         | up          | up         | 1500 |
| da... | 3  | avp-guest | 0         | up          | up         | 1500 |
+-------+----+-----------+-----------+-------------+------------+------+

-------------+--------------+--------------+
 mac-address | network-uuid | network-name |
-------------+- ------------+--------------+
 90:e2:ba... |              |              |
 90:e2:ba... |              |              |
 fa:16:3e... | 4326a83a-... | net-4326a83a |
 fa:16:3e... | 4c02316e-... | net-4c02316e |
-------------+--------------+--------------+
```

interface-list

Lists attributes for logical interfaces.

```
$ sudo vshell -H compute-1 interface-list
+-------+----------+----------+-----------+-------------+------+
| uuid  | type     | class    | name      | mac-address | mtu  |
+-------+----------+----------+-----------+-------------+------+
| c6... | ae       | provider | ae0       | 90:e2:ba... | 1600 |
| 26... | ethernet | provider | eth0      | 90:e2:ba... | 1600 |
| d3... | vlan     | provider | ae0.632   | 90:e2:ba... | 1500 |
| 56... | vnic     | tenant   | vnic3     | fa:16:3e... | 1500 |
| a8... | vxlan    | provider | vxlan0    | 00:00:00... | 1500 |
+-------+----------+----------+-----------+-------------+------+
```

```
--------------+----------------+-------+
 network-uuid | network-name   | dvr   |
--------------+----------------+-------+
              |                | False |
              |                | False |
 8e0c9ba9-... | net-8e0c9ba9   | False |
 4326a83a-... | net-4326a83a   | False |
 582528d0-... | net-582528d0   | False |
--------------+----------------+-------+
```

lldp-neighbour-list

lists the learned Link Layer Discovery Protocol (LLDP) neighbors of physical ports.

```
$ sudo vshell -H compute-1 lldp-neighbour-list
+---------+-------------+----------------+-------------+--------+
| port-id | remote-port | remote-address | mac-address | rx-ttl |
+---------+-------------+----------------+-------------+--------+
| 0       | xe40        |                | 00:08:a2... | 120    |
| 1       | xe39        |                | 00:08:a2... | 120    |
+---------+-------------+----------------+-------------+--------+

-------------+--------------------+------------------+
 system-name | system-description | port-description |
-------------+--------------------+------------------+
 yow-cgcs... | yow-cgcs-quanta-1  | yow-cgcs-iron... |
 yow-cgcs... | yow-cgcs-quanta-1  | yow-cgcs-iron... |
-------------+--------------------+------------------+
```

network-table-list

Lists the learned and static MAC addresses of logical interfaces and network segments.

```
$ sudo vshell -H compute-1 network-table-list
+-------------+---------+----------------+---------------+--------------+
| mac-address | type    | interface-name | network-uuid  | network-name |
+-------------+---------+----------------+---------------+--------------+
| fa:16:3e... | dynamic | ae0.664        | 4326a83a-4... | net-4326a83a |
| fa:16:3e... | dynamic | ae0.632        | 8e0c9ba9-b... | net-8e0c9ba9 |
+-------------+---------+----------------+---------------+--------------+

-------------+-------------+
 created-age | timeout-age |
-------------+-------------+
 243552      | 2           |
 243656      | 5           |
-------------+-------------+
```

address-list

Lists IPv4 and IPv6 network addresses assigned to logical interfaces.

```
$ sudo vshell -H compute-1 address-list
+---------+----------------+----------------+----------------+--------------------+
| address | interface-uuid | interface-name | valid-lifetime | preferred-lifetime |
+---------+----------------+----------------+----------------+--------------------+
| 192.... | c67943b7-d1... | ae0            | infinity       | infinity           |
| fd00... | c67943b7-d1... | ae0            | infinity       | infinity           |
| fe80... | 1e93938d-4b... | eth1           | infinity       | infinity           |
| fe80... | 0198434f-f8... | ae0.680        | infinity       | infinity           |
+---------+----------------+----------------+----------------+--------------------+

-----------+----------+-------------+
 permanent | autoconf | floating-ip |
-----------+----------+-------------+
 True      | False    | False       |
 True      | False    | False       |
 False     | False    | False       |
 False     | False    | False       |
-----------+----------+-------------+
```

route-list

Lists the configured IPv4 and IPv6 network routes of virtual routers

```
$ sudo vshell -H compute-1 route-list
```

```
+--------+------------------+----------+----------------+----------------+
| router | prefix           | type     | interface-uuid | interface-name |
+--------+------------------+----------+----------------+----------------+
| 6b1... | 0.0.0.0/0        | external | c67943b7-d1... | ae0            |
| 6b1... | 192.168.60.64/27 | prefix   | c67943b7-d1... | ae0            |
| 6b1... | ::/0             | global   | c67943b7-d1... | ae0            |
| 6b1... | fd00:0:0:5::/64  | prefix   | c67943b7-d1... | ae0            |
+--------+------------------+----------+----------------+----------------+

---------------+--------+----------+-------------+-------------+
 gateway       | weight | lifetime | created-age | timeout-age |
---------------+--------+----------+-------------+-------------+
 192.168.60.65 | 1      | infinity | None        | None        |
 None          | 255    | infinity | None        | None        |
 fd00:0:0:5::1 | 1      | infinity | None        | None        |
 None          | 255    | infinity | None        | None        |
---------------+--------+----------+-------------+-------------+
```

ping

Initiate an ICMP echo request to a far-end IP address for connectivity testing

```
$ sudo vshell -H compute-1 ping ip-address source-interface
```

where

ip-address

is the far-end IP address

source-interface

is the UUID of the vSwitch interface to use

statistic-group-list

Lists available statistic groups. You can use these groups to enable or disable statistics collection for network-related activity. For performance reasons, the groups are disabled by default.

```
$ sudo vshell -H compute-1 statistic-group-list
+-----------+----------+
| name      | state    |
+-----------+----------+
| bridge    | disabled |
| dvr       | disabled |
| engine    | disabled |
| filter    | disabled |
| interface | disabled |
| ip        | disabled |
| layer2    | disabled |
| nat       | disabled |
| snat      | disabled |
| udp       | disabled |
| vxlan     | disabled |
+-----------+----------+
```

statistic-group-enable

Enables the statistic group specified by *groupname*. The following example enables the **engine** group:

```
$ sudo vshell -H compute-1 statistic-group-enable engine
```

⚠ **CAUTION:** Real-time statistics collection can affect system performance. Always disable statistics collection when not in use.

statistic-group-disable

Disables the statistic group specified by *groupname*. The following example disables the **engine** group:

```
$ sudo vshell -H compute-1 statistic-group-disable engine
```

engine-stats-list

Displays packet processing and CPU utilization statistics for the packet processing engine. To collect fresh statistics, enable the **engine** statistic group.

```
$ sudo vshell -H compute-1 statistic-group-enable engine
$ sudo vshell -H compute-1 engine-stats-list
+-------+----+-------+------------+------------+-------------+
| uuid  | id | cpuid | rx-packets | tx-packets | tx-disabled |
+-------+----+-------+------------+------------+-------------+
| df... | 0  | 1     | 2536       | 7911       | 0           |
| ef... | 1  | 2     | 1446       | 5819       | 0           |
+-------+----+-------+------------+------------+-------------+

-------------+------------+------------+-------+
 tx-overflow | rx-discard | tx-discard | usage |
-------------+------------+------------+-------+
 0           | 0          | 0          | 0.00% |
 0           | 0          | 0          | 0.00% |
-------------+------------+------------+-------+
```

For best performance, disable the group when you are finished.

```
$ sudo vshell -H compute-1 statistic-group-disable engine
```

port-stat-list

Displays packet processing statistics by port. For this list, there is no corresponding statistic group. Collection is always enabled.

```
sudo vshell -H compute-1 port-stats-list
+-------+----+-----------+------------+------------+----------+----------+
| uuid  | id | type      | rx-packets | tx-packets | rx-bytes | tx-bytes |
+-------+----+-----------+------------+------------+----------+----------+
| 21... | 0  | physical  | 423017     | 154532     | 85008801 | 36865698 |
| fd... | 2  | avp-guest | 16444      | 101988     | 2147791  | 25666266 |
+-------+----+-----------+------------+------------+----------+----------+

-----------+-----------+-----------+
 tx-errors | rx-errors | rx-nombuf |
-----------+-----------+-----------+
 0         | 0         | 0         |
 0         | 0         | 0         |
-----------+-----------+-----------+
```

port-queue-stats-list

Displays packet processing information for all queues on a port. It is possible that the total tx count for all queues on a port will not match the tx count reported by **port-stat-list** if activity occurs in the interval between running these commands.

```
sudo vshell -H compute-1 port-queue-stats-list
+--------------------------------------+----+-----+-------+---------+----------
+--------+--------+
| uuid                                 | id | dir | queue | packets | bytes    |
```

```
errors | nombuf |
+--------------------------------------+----+-----+-------+---------+----------
+--------+--------+
… …
| c9ee588c-6f04-434f-bc52-46028b38f2ad | 4  | rx  | 0     | 3       | 230      |
0      | 0      |
| c9ee588c-6f04-434f-bc52-46028b38f2ad | 4  | rx  | 1     | 0       | 0        |
0      | 0      |
| c9ee588c-6f04-434f-bc52-46028b38f2ad | 4  | tx  | 0     | 10      | 768      |
0      | 0      |
| c9ee588c-6f04-434f-bc52-46028b38f2ad | 4  | tx  | 1     | 12      | 852      |
0      | 0      |
| c97b5faf-4273-44cc-8a87-d4c8622885aa | 5  | rx  | 0     | 3       | 230      |
0      | 0      |
| c97b5faf-4273-44cc-8a87-d4c8622885aa | 5  | rx  | 1     | 16      | 3536     |
0      | 0      |
| c97b5faf-4273-44cc-8a87-d4c8622885aa | 5  | tx  | 0     | 0       | 0        |
0      | 0      |
| c97b5faf-4273-44cc-8a87-d4c8622885aa | 5  | tx  | 1     | 16414   | 4867024  |
0      | 0      |
```

interface-stats-list

Displays packet processing statistics by interface. To collect fresh statistics, enable the **interface** statistic group.

```
$ sudo vshell -H compute-1 statistic-group-enable interface
$ sudo vshell -H compute-1 interface-stats-list
+-------+----------+-----------+------------+------------+----------+----------+
| uuid  | type     | name      | rx-packets | tx-packets | rx-bytes | tx-bytes |
+-------+----------+-----------+------------+------------+----------+----------+
| c6... | ae       | ae0       | 0          | 0          | 0        | 0        |
| 26... | ethernet | eth0      | 0          | 0          | 0        | 0        |
| d3... | vlan     | ae0.632   | 0          | 0          | 0        | 0        |
| 56... | vnic     | vnic3     | 0          | 0          | 0        | 0        |
| a8... | vxlan    | vxlan0    | 0          | 0          | 0        | 0        |
+-------+----------+-----------+------------+------------+----------+----------+

-----------+-----------+-------------+-------------+-----------+------------+
 tx-errors | rx-errors | tx-discards | rx-discards | rx-floods | rx-no-vlan |
-----------+-----------+-------------+-------------+-----------+------------+
 0         | 0         | 0           | 0           | 0         | 0          |
 0         | 0         | 0           | 0           | 0         | 0          |
 0         | 0         | 0           | 0           | 0         | 0          |
 0         | 0         | 0           | 0           | 0         | 0          |
 0         | 0         | 0           | 0           | 0         | 0          |
-----------+-----------+-------------+-------------+-----------+------------+
```

For best performance, disable the group when you are finished.

```
$ sudo vshell -H compute-1 statistic-group-disable interface
```

ip-stats-list

Displays packet processing statistics for the IP stack. To collect fresh statistics, enable the **ip** statistic group.

```
$ sudo vshell -H compute-1 statistic-group-enable ip
$ sudo vshell -H compute-1 ip-stats-list
+--------+-------+----------+--------------+--------------+
| family | cpuid | rx-total | rx-broadcast | rx-multicast |
+--------+-------+----------+--------------+--------------+
| ipv4   | 0     | 0        | 0            | 0            |
| ipv4   | 1     | 0        | 0            | 0            |
| ipv4   | 2     | 0        | 0            | 0            |
| ipv6   | 0     | 0        | 0            | 0            |
| ipv6   | 1     | 0        | 0            | 0            |
| ipv6   | 2     | 0        | 0            | 0            |
+--------+-------+----------+--------------+--------------+

----------+-------------+-------------+-----------+
```

```
 tx-total | tx-broadcast | tx-multicast | fwd-total |
----------+--------------+--------------+-----------+
 0        | 0            | 0            | 0         |
 0        | 0            | 0            | 0         |
 0        | 0            | 0            | 0         |
 0        | 0            | 0            | 0         |
 0        | 0            | 0            | 0         |
 0        | 0            | 0            | 0         |
----------+--------------+--------------+-----------+

---------------+---------------+--------------+---------------+-----------------+
 rx-reassemble | tx-reassemble | tx-fragments | icmp-required | icmp-throttled |
---------------+---------------+--------------+---------------+-----------------+
 0             | 0             | 0            | 0             | 0               |
 0             | 0             | 0            | 0             | 0               |
 0             | 0             | 0            | 0             | 0               |
 0             | 0             | 0            | 0             | 0               |
 0             | 0             | 0            | 0             | 0               |
 0             | 0             | 0            | 0             | 0               |
---------------+---------------+--------------+---------------+-----------------+
```

For best performance, disable the group when you are finished.

```
$ sudo vshell -H compute-1 statistic-group-disable ip
```

memory-stats-list

Displays memory statistics by interface.

```
$  sudo vshell memory-stats-list
+-----------+----------------------+----------------------+------------------
+-----------------+---------------+------------+
| socket-id | physical-total-bytes | physical-free-bytes | heap-total-bytes | heap-
free-bytes | physical-used | total-used |
+-----------+----------------------+----------------------+------------------
+-----------------+---------------+------------+
| 0         | 1073741824           | 397485952           | 170131264        |
12954304        | 62.98%        | 61.77%     |
| 1         | 1073741824           | 568585856           | 11534272         |
6995584         | 47.05%        | 46.39%     |
+-----------+----------------------+----------------------+------------------
+-----------------+---------------+------------+
```

Performing Packet Tracing on vSwitch Interfaces

You can use the **vtrace** command to perform packet tracing on a vSwitch logical interface.

The **vtrace** command initiates a packet-trace capture on a logical interface. To use it, you must log on with root privileges to the host running the vSwitch instance.

⚠ **CAUTION:** This command can cause significant packet loss on the trace port. Avoid using it on live systems with high rates of traffic.

When **vtrace** is used, all transmit and receive packets passing through the logical interface are mirrored to a dynamically created Linux host interface. The utility uses the vSwitch packet tracing API to enable tracing, and invokes **tcpdump** on the host interface. You can use any **tcpdump** option except **-i** to filter and analyze the captured data.

To initiate a packet trace, use the following command:

```
$ sudo vtrace interface-uuid tcpdump-options filter-expression
```

where

interface-uuid

is the UUID of the logical interface. You can obtain this using the **vshell interface-list** command.

tcpdump-options

are the options for the packet trace. For details, refer to the public documentation for **tcpdump**.

NOTE: Do not use the **-i** option.

filter-expression

is an expression for filtering packet trace results. For details, refer to the public documentation for **tcpdump**.

B

HCG 4.0 Alarm Messages

Alarm Messages

The system inventory and maintenance service reports system changes with different degrees of severity. Use the reported alarms to monitor the overall health of the system.

For more information, see Fault Management on page 211.

In the following tables, the severity of the alarms is represented by one or more letters, as follows:

- C: Critical
- M: Major
- m: Minor
- W: Warning

A slash-separated list of letters is used when the alarm can be triggered with one of several severity levels.

Table 5 **Alarm Messages**

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
100.101	Platform CPU threshold exceeded; threshold x %, actual y% .	C/M/m	Monitor and if condition persists, contact next level of support.
	host=<*hostname*>		
100.102	VSwitch CPU threshold exceeded; threshold x %, actual y% .	C/M/m	Monitor and if condition persists, contact next level of support.

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
	host=<*hostname*>		
100.103	Memory threshold exceeded; threshold x%, actual y% .	C/M/m	Monitor and if condition persists, contact next level of support; may require additional memory on Host.
	host=<*hostname*>		
100.104	File System threshold exceeded; threshold x%, actual y%	C/M/m	Monitor and if condition persists, contact next level of support.
	host=<*hostname*>.filesystem=<*mount-dir*>		
	File System threshold exceeded; threshold x%, actual y%	C/M/m	Monitor and if condition persists, consider adding additional physical volumes to the volume group.
	host=<*hostname*>.volumegroup=<*volumegroup-name*>		
100.105	No access to remote VM volumes.	M	Check Management and Infrastructure Networks and Controller or Storage Nodes.
	host=<*hostname*>		
100.106	'OAM' Port failed.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.port=<*port-name*>		
100.107	OAM' Interface degraded. or 'OAM' Interface failed.	C or M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.interface=<*if-name*>		
100.108	'MGMT' Port failed.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.port=<*port-name*>		
100.109	'MGMT' Interface degraded. or 'MGMT' Interface failed.	C or M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.interface=<*if-name*>		

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
100.110	'INFRA' Port failed.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.port=<*port-name*>		
100.111	'INFRA' Interface degraded. or 'INFRA' Interface failed.	C or M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.interface=<*if-name*>		
100.112	'DATA-VRS' Port down.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.port=<*port-name*>		
100.113	'DATA-VRS' Interface degraded. or 'DATA-VRS' Interface down.	M or C	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.interface=<*if-name*>		
100.114	NTP configuration does not contain any valid or reachable NTP servers.	M	Monitor and if condition persists, contact next level of support.
	host=<*hostname*>.ntp		
	NTP address <*IP address*> is not a valid or a reachable NTP server.	m	
	host=<*hostname*>.ntp=<*IP address*>		
100.115	VSwitch Memory Usage, processor <processor> threshold exceeded; threshold x%, actual y%	C, M, m	Monitor and if condition persists, contact next level of support
	host=<hostname>.processor=<processor>		
100.116	Cinder LVM Thinpool Usage threshold exceeded; threshold x%, actual y% .	C, M, m	Monitor and if condition persists, contact next level of support.
	host=<hostname>.volumegroup=<volumegroup>		
100.117	Nova LVM Thinpool Usage threshold exceeded; threshold x%, actual y% .	C, M, m	Monitor and if condition persists, contact next level of support.
	host=<hostname>.volumegroup=<volumegroup>		
100.118	Controller cannot establish connection with remote logging server.	m	Ensure Remote Log Server IP is reachable from Controller through

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
			OAM interface; otherwise contact next level of support
	host=<hostname>		
200.001	<*hostname*> was administratively locked to take it out-of-service.	W	Administratively unlock Host to bring it back in-service.
	host=<*hostname*>		
200.004	<*hostname*> experienced a service-affecting failure. Host is being auto recovered by Reboot.	C	If auto-recovery is consistently unable to recover host to the unlocked-enabled state contact next level of support or lock and replace failing host.
	host=<*hostname*>		
200.005	Degrade: <*hostname*> is experiencing an intermittent 'Management Network' communication failures that have exceeded its lower alarming threshold.	M	Check 'Management Network' connectivity and support for multicast messaging. If problem consistently occurs after that and Host is reset, then contact next level of support or lock and replace failing host.
	Failure: <*hostname*> is experiencing a persistent Critical 'Management Network' communication failure.	C	
	host=<*hostname*>		
200.006	Main Process Monitor Daemon Failure (Major) <*hostname*> 'Process Monitor' (pmond) process is not running or functioning properly. The system is trying to recover this process. Monitored Process Failure (Critical/Major/Minor) Critical: <*hostname*> Critical '<*processname*>' process has failed and could not be auto-recovered gracefully. Auto-recovery progression by host reboot is required and in progress. Major: <*hostname*> is degraded due to the failure of its '<*processname*>' process. Auto recovery of this Major process is in progress. Minor: <*hostname*> '<*processname*>' process has failed. Auto recovery of this Minor process is in progress.	C/M/m	If this alarm does not automatically clear after some time and continues to be asserted after Host is locked and unlocked then contact next level of support for root cause analysis and recovery. If problem consistently occurs after Host is locked and unlocked then contact next level of support for root cause analysys and recovery.

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
	or <*hostname*> '<*processname*>' process has failed. Manual recovery is required.		
	host=<*hostname*>.process=<*processname*>		
200.007	Critical: (with host degrade): Host is degraded due to a 'Critical' out-of-tolerance reading from the '<*sensorname*>' sensor Minor: (with host degrade) Host is degraded due to a 'Major' out-of-tolerance reading from the '<*sensorname*>' sensor Minor: Host is reporting a 'Minor' out-of-tolerance reading from the '<*sensorname*>' sensor	C/M/m	If problem consistently occurs after Host is power cycled and or reset, contact next level of support or lock and replace failing host.
	host=<*hostname*>.sensor=<*sensorname*>		
200.009	Degrade: <*hostname*> is experiencing an intermittent 'Infrastructure Network' communication failures that have exceeded its lower alarming threshold.	M	Check 'Infrastructure Network' connectivity and support for multicast messaging. If problem consistently occurs after that and Host is reset, then contact next level of support or lock and replace failing host.
	Failure: <*hostname*> is experiencing a persistent Critical 'Infrastructure Network' communication failure.	C	
	host=<*hostname*>		
200.010	<*hostname*> access to board management module has failed.	W	Check Host's board management configuration and connectivity.
	host=<*hostname*>		
200.011	<*hostname*> experienced a configuration failure during initialization. Host is being re-configured by Reboot.	C	If auto-recovery is consistently unable to recover host to the unlocked-enabled state contact next level of support or lock and replace failing host.
	host=<*hostname*>		
200.012	<*hostname*> controller function has in-service failure while compute services remain healthy.	M	Lock and then Unlock host to recover. Avoid using 'Force Lock' action as that will impact compute

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
			services running on this host. If lock action fails then contact next level of support to investigate and recover.
	host=<*hostname*>		
200.013	<*hostname*> compute service of the only available controller is not poperational. Auto-recovery is disabled. Degrading host instead.	M	Enable second controller and Switch Activity (Swact) over to it as soon as possible. Then Lock and Unlock host to recover its local compute service.
	host=<*hostname*>		
200.014	The Hardware Monitor was unable to load, configure and monitor one or more hardware sensors.	m	Check Board Management Controller provisioning. Try reprovisioning the BMC. If problem persists try power cycling the host and then the entire server including the BMC power. If problem persists then contact next level of support.
	host=<*hostname*>		
200.015	Unable to read one or more sensor groups from this host's board management controller	M	Check board management connectivity and try rebooting the board management controller. If problem persists contact next level of support or lock and replace failing host.
	host=<*hostname*>		
210.001	System Backup in progress.	m	No action required.
	host=controller		
250.001	<*hostname*> Configuration is out-of-date.	M	Administratively lock and unlock <*hostname*> to update config.
	host=<*hostname*>		
250.002	<*hostname*> Ceph cache tiering configuration is out-of-date.	M	Apply Ceph service parameter settings.
	clustert=<*dist-fs-uuid*>		
250.010	<*hostname*> Configuration action is required to provision compute function.	M	<*hostname*> action required. Configure data intefaces and then perform system compute-config-complete.

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
	host=<*hostname*>		
270.001	Host <*host_name*> compute services failure[, reason = <*reason_text*>]	C	Wait for host services recovery to complete; if problem persists contact next level of support
	host=<*host_name*>.services=compute		
300.001	'Data' Port failed.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.port=<*port-uuid*>		
300.002	'Data' Interface degraded. or 'Data' Interface failed.	M/C	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.interface=<*if-uuid*>		
300.003	Networking Agent not responding.	M	If condition persists, attempt to clear issue by administratively locking and unlocking the Host.
	host=<*hostname*>.agent=<*agent-uuid*>		
300.004	No enabled compute host with connectivity to provider network.	M	Enable compute hosts with required provider network connectivity.
	host=<*hostname*>.providernet=<*pnet-uuid*>		
300.005	Communication failure detected over provider network x% for ranges y% on host z%. or Communication failure detected over provider network x% on host z%.	M	Check neighbour switch port VLAN assignments.
	providernet=<*pnet-uuid*>.host=<*hostname*>		
300.010	ML2 Driver Agent non-reachable or ML2 Driver Agent reachable but non-responsive or ML2 Driver Agent authentication failure or ML2 Driver Agent is unable to sync Neutron database	M	Monitor and if condition persists, contact next level of support.

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
	host=<*hostname*>.ml2driver=<*driver*>		
300.012	Openflow Controller connection failed.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.openflow-controller=<*uri*>		
300.013	No active Openflow controller connections found for this network. or One or more Openflow controller connections in disconnected state for this network.	C, M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.openflow-network=<*name*>		
300.014	OVSDB Manager connection failed.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.sdn-controller=<*uuid*>		
300.015	No active OVSDB connections found.	C	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>		
400.001	Service group failure; <*list of affected services*>. or Service group degraded; <*list of affected services*>. or Service group Warning; <*list of affected services*>.	C/M/m	Contact next level of support.
	service_domain=<*domain_name*>.service_group=<*group_name*>.host=<*hostname*>		
400.002	Service group loss of redundancy; expected <*num*> standby member<*s*> but only <*num*> standby member<*s*> available. or Service group loss of redundancy; expected <*num*> standby member<*s*> but only <*num*> standby member<*s*> available. or	M	Bring a controller node back in to service, otherwise contact next level of support.

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
	Service group loss of redundancy; expected <*num*> active member<*s*> but no active members available. or Service group loss of redundancy; expected <*num*> active member<*s*> but only <*num*> active member<*s*> available.		
	service_domain=<*domain_name*>.service_group=<*group_name*>		
400.003	License key has expired or is invalid; a valid license key is required for operation. or Evaluation license key will expire on <*date*>; there are <*num_days*> days remaining in this evaluation. or Evaluation license key will expire on <*date*>; there is only 1 day remaining in this evaluation.	C	Contact next level of support to obtain a new license key.
	host=<*hostname*>		
400.004	Service group software modification detected; <*list of affected files*>.	M	Contact next level of support.
	host=<*hostname*>		
400.005	Communication failure detected with peer over port <*linux-ifname*>. or Communication failure detected with peer over port <*linux-ifname*> within the last 30 seconds.	M	Check cabling and far-end port configuration and status on adjacent equipment.
	host=<*hostname*>.network=<*mgmt* | *oam* | *infra*>		
700.001	Instance <*instance_name*> owned by <*tenant_name*> has failed on host <*host_name*> Instance <*instance_name*> owned by <*tenant_name*> has failed to schedule	C	The system will attempt recovery; no repair action required
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.002	Instance <*instance_name*> owned by <*tenant_name*> is paused on host <*host_name*>	C	Unpause the instance
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
700.003	Instance <*instance_name*> owned by <*tenant_name*> is suspended on host <*host_name*>	C	Resume the instance
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.004	Instance <*instance_name*> owned by <*tenant_name*> is stopped on host <*host_name*>	C	Start the instance
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.005	Instance <*instance_name*> owned by <*tenant_name*> is rebooting on host <*host_name*>	C	Wait for reboot to complete; if problem persists contact next level of support
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.006	Instance <*instance_name*> owned by <*tenant_name*> is rebuilding on host <*host_name*>	C	Wait for rebuild to complete; if problem persists contact next level of support
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.007	Instance <*instance_name*> owned by <*tenant_name*> is evacuating from host <*host_name*>	C	Wait for evacuate to complete; if problem persists contact next level of support
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.008	Instance <*instance_name*> owned by <*tenant_name*> is live migrating from host <*host_name*>	W	Wait for live migration to complete; if problem persists contact next level of support
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.009	Instance <*instance_name*> owned by <*tenant_name*> is cold migrating from host <*host_name*>	C	Wait for cold migration to complete; if problem persists contact next level of support
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.010	Instance <*instance_name*> owned by <*tenant_name*> has been cold-migrated to host <*host_name*> waiting for confirmation	C	Confirm or revert cold-migrate of instance
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.011	Instance <*instance_name*> owned by <*tenant_name*> is reverting cold migrate to host <*host_name*>	C	Wait for cold migration revert to complete; if problem persists contact next level of support"
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
700.012	Instance <*instance_name*> owned by <*tenant_name*> is resizing on host <*host_name*>	C	Wait for resize to complete; if problem persists contact next level of support
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.013	Instance <*instance_name*> owned by <*tenant_name*> has been resized on host <*host_name*> waiting for confirmation	C	Confirm or revert resize of instance
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.014	Instance <*instance_name*> owned by <*tenant_name*> is reverting resize on host <*host_name*>	C	Wait for resize revert to complete; if problem persists contact next level of support"
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.015	Guest Heartbeat not established for instance <*instance_name*> owned by <*tenant_name*> on host <*host_name*>	M	Verify that the instance is running the Guest-Client daemon, or disabsle Guest Heartbeat for the instance if no longer needed, otherwise contact next level of support.
	tenant=<*tenant-uuid*>.instance=<*instance-uuid*>		
700.016	Multi-Node Recovery Mode	m	Wait for the system to exit out of this mode.
	subsystem=vim		
700.017	Server group <*server_group_name*> <*policy*> policy was not satisfied	M	Migrate instances in an attempt to satisfy the policy; if problem persists contact next level of support.
	server-group<*server-group-uuid*>		
800.001	Storage Alarm Condition: 1 mons down, quorum 1,2 controller-1,storage-0	C/M	If problem persists, contact next level of support.
	cluster=<*dist-fs-uuid*>		
800.002	Image storage media is full: There is not enough disk space on the image storage media. or Instance <instance name> snapshot failed: There is not enough disk space on the image storage media. or	W	If problem persists, contact next level of support.

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
	Supplied <attrs> (<supplied>) and <attrs> generated from uploaded image (<actual>) did not match. Setting image status to 'killed'. or Error in store configuration. Adding images to store is disabled. or Forbidden upload attempt: <exception> or Insufficient permissions on image storage media: <exception> or Denying attempt to upload image larger than <size> bytes. or Denying attempt to upload image because it exceeds the quota: <exception> or Received HTTP error while uploading image <image_id> or Client disconnected before sending all data to backend or Failed to upload image <image_id>		
	image=<*image-uuid*>, instance=<*instance-uuid*> or image=<*tenant-uuid*>, instance=<*instance-uuid*>		
800.003	Storage Alarm Condition: total ceph cluster size greater than sum of individual pool quotas	m	Update ceph storage pool quotas to use all available cluster space.
	cluster=<*dist-fs-uuid*>		
800.010	Potential data loss. No available OSDs in storage replication group.	C	Ensure storage hosts from replication group are unlocked and available. Check if OSDs of each storage host are up and running. If problem persists contact next level of support.
	cluster=<*dist-fs-uuid*>.peergroup=<*group-x*>		
800.011	Loss of replication in peergroup.	M	Ensure storage hosts from replication group are unlocked

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
			and available. Check if OSDs of each storage host are up and running. If problem persists contact next level of support.
	cluster=<*dist-fs-uuid*>.peergroup=<*group-x*>		
800.100	Storage Alarm Condition: Cinder I/O Congestion is above normal range and is building	M	Reduce the I/O load on the Cinder LVM backend. Use Cinder QoS mechanisms on high usage volumes.
	cinder_io_monitor		
800.101	Storage Alarm Condition: Cinder I/O Congestion is high and impacting guest performance	C	Reduce the I/O load on the Cinder LVM backend. Cinder actions may fail until congestion is reduced. Use Cinder QoS mechanisms on high usage volumes.
	cinder_io_monitor		
900.001	Patching operation in progress.	m	Complete reboots of affected hosts.
	host=controller		
900.002	Obsolete patch in system.	W	Remove and delete obsolete patches.
	host=controller		
900.003	Patch host install failure.	M	Undo patching operation.
	host=<*hostname*>		
900.004	Host version mismatch.	M	Reinstall host to update applied load.
	host=<*hostname*>		
900.005	System Upgrade in progress.	m	No action required.
	host=controller		
900.101	Software update auto-apply in progress.	M	ait for software update auto-apply to complete; if problem persists contact next level of support.
	sw-update		
900.102	Software update auto-apply aborting.	M	Wait for software update auto-apply abort to complete; if problem persists contact next level of support.

Alarm ID	Description	Severity	Proposed Repair Action
	Entity Instance ID		
	host=<*hostname*>		
900.103	Software update auto-apply failed.	M	Attempt to apply software updates manually; if problem persists contact next level of support.
	host=<*hostname*>		