Technical white paper

HP Helion CloudSystem 8.1 networking configuration and troubleshooting

Table of contents

Executive summary ........................................................................................................................................... 3
Overview of HP Helion CloudSystem 8.1 networking ................................................................................. 3
Overview of HP Helion CloudSystem 8.1 network topology ..................................................................... 6
Network definitions ....................................................................................................................................... 6
Required networks ........................................................................................................................................ 7
Sample network configuration of ESXi based environments using HP OneView ................................. 9
HP 5900 Series Network Switch configuration ....................................................................................... 11
vCenter/vSphere Network Switch configuration ......................................................................................... 15
ESXi Management Servers configuration ................................................................................................. 15
OneView configuration ............................................................................................................................ 21
ESXi compute nodes configuration ........................................................................................................ 40
Important steps during Helion CloudSystem 8.1 installation ................................................................... 47
Sample network configuration of KVM based environments using HP Virtual Connect Manager ....... 47
HP 5900 Series Network Switch configuration ....................................................................................... 50
KVM Management Server configuration ................................................................................................. 52
VCM configuration ..................................................................................................................................... 56
KVM compute nodes configuration ........................................................................................................ 62
Important steps during the Helion CloudSystem 8.1 installation ............................................................ 64
Network operations in Helion CloudSystem ............................................................................................. 65
Provider Networks ...................................................................................................................................... 65
Private Networks ......................................................................................................................................... 65
External Network ......................................................................................................................................... 66
Routers ......................................................................................................................................................... 66
Security Groups ........................................................................................................................................ 66
Role of network nodes ............................................................................................................................ 67
Troubleshooting Helion CloudSystem network issues ............................................................................. 70
KVM compute node does not appear in CloudSystem Console for activation ........................................ 70
Common networking configuration issues ............................................................................................... 71
Common Helion CloudSystem networking issues .................................................................................. 71
Executive summary

This white paper will demonstrate how to configure and troubleshoot end-to-end networking configurations in HP Helion CloudSystem 8.1 environments. The document describes sample configurations using HP OneView in VMware® vSphere® based environments and using HP Virtual Connect Manager in KVM (for Kernel-based Virtual Machine) based environments. The document also describes the common networking operations in HP Helion CloudSystem 8.1 environments including the role of the network node appliances.

Target audience: This document is intended for experienced system administrators with a working knowledge of the following concepts:

- Top of Rack (ToR) switches for networking
- Command Line Interface (CLI) commands for Microsoft® Windows® and Linux®
- VMware vCenter Server functionality, if using ESXi hypervisors and compute nodes
- VMware Distributed and Standard vSwitches, if using ESXi hypervisors and compute nodes
- Red Hat® KVM hypervisor configuration and use, if using KVM hypervisors and compute nodes
- Secure shell (ssh) and secure copy (scp) commands, if using KVM hypervisors and compute nodes
- Experience with OpenStack® technologies such as Nova, Glance, Keystone and Neutron

Overview of HP Helion CloudSystem 8.1 networking

HP Helion CloudSystem 8.1 operates in converged infrastructure environments and provides a software-defined approach to managing the cloud. HP Helion CloudSystem 8.1 consists of two offerings:

**HP Helion CloudSystem Foundation** is based on the HP Helion distribution of OpenStack Cloud Software. It integrates hardware and software to deliver core Infrastructure-as-a-Service (IaaS) provisioning and lifecycle management of compute, network and storage resources. You can manage HP Helion CloudSystem Foundation from an administrative console, self-service portal, Command Line Interfaces (CLIs), and OpenStack APIs. It provides an appliance-based deployment console to simplify installation and maintenance, and an embedded version of HP Operations Orchestration (OO) for automating administrative processes.

Figure 1. HP Helion CloudSystem Foundation
**HP Helion CloudSystem Enterprise** expands on HP Helion CloudSystem Foundation to integrate servers, storage, networking, security, and management to automate the lifecycle for hybrid service delivery. Template Architects can use Helion CloudSystem Enterprise to create infrastructure templates and offer them as services in a Marketplace Portal. The Marketplace Portal users request services from a catalog and manage their subscriptions. When a service is requested, Helion CloudSystem Enterprise automatically provisions the servers, storage, and networking. Helion CloudSystem Enterprise also includes an enhanced set of Operations Orchestration workflows.

*Figure 2. HP Helion CloudSystem Enterprise*
Figure 3 describes the HP Helion CloudSystem architecture.

**Figure 3.** HP Helion CloudSystem architecture
Overview of HP Helion CloudSystem 8.1 network topology

Networks are organized into two trunks, the Management Trunk and the Cloud Data Trunk. The Management Trunk contains all infrastructure networks that connect the virtual appliances, vCenter Server and the HP 3PAR StoreServ storage system. The Cloud Data Trunk contains the networks that connect provisioned virtual machines to the Helion CloudSystem Provider and Private Networks.

Figure 4. Helion CloudSystem appliances and network infrastructure

Network definitions

Management Trunk
The Management Trunk contains the following networks:

Data Center Management Network: This network provides access to the CloudSystem Console, which is the management interface for the Foundation base appliance. REST API calls are made from this network. The Helion CloudSystem Foundation base appliance and the Helion CloudSystem Enterprise appliance access vCenter Server over this network. The Helion CloudSystem Foundation base appliance also communicates with HP 3PAR StoreServ over this network. This network is used by the Cloud Administrators to manage the environment.

When using the ESXi management servers with ESXi compute nodes configuration:

- The Helion CloudSystem Foundation base appliance uses this network to access the vCenter Server that is managing the management hypervisor.
- The vCenter proxy appliance uses this network to access the vCenter Server that is managing ESXi compute clusters. This can be a separate vCenter Server or the same vCenter Server used by the Helion CloudSystem Foundation base appliance.
- The Helion CloudSystem Enterprise appliance also uses this network to access the vCenter Server. Helion CloudSystem Enterprise can be configured to use a third vCenter Server, or it can access one of the two existing vCenter Servers.

Cloud Management Network: This Private Network for the cloud is typically a VLAN, but could also be a physical network. The Helion CloudSystem Foundation base appliance runs a DHCP server for this network.

Important
The Cloud Management Network should be a dedicated Private Network for Helion CloudSystem Management use only. Some of the content transmitted between compute nodes and the cloud controller are unencrypted. Network isolation should be used to prevent unwanted exposure to sensitive data.
**Consumer Access Network:** This network gives cloud users a separate access point for the CloudSystem Portal and the Helion CloudSystem Enterprise appliance, where the other administrative servers are not accessible. In the OpenStack Keystone endpoint catalog, the public URL is on this network. The Consumer Access Network allows you to access the consoles of KVM virtual machine instances from the CloudSystem Portal. If you connect to the CloudSystem Portal using the Data Center Management Network, you cannot access KVM consoles. **This network will be used by Cloud users to access CloudSystem and CSA Marketplace portals.**

**External Network:** This network is automatically connected to the network node appliances after Cloud Networking settings are saved during the CloudSystem Console first time setup. A subnet in the External Network must be defined in the CloudSystem Portal before using this network.

Virtual machines are not connected directly to this network. Internal provider or Private Networks connect directly to a virtual machine, then a virtual router is used to connect the Private and External Networks. A networking service routes outgoing traffic to the External Network. When the External Network subnet assigns Floating IPs to virtual machines, users on the External Network can then access the virtual machines.

**Cloud Data Trunk**
This network trunk must be configured as a group of VLANs. It hosts the VLANs that OpenStack networking makes available to users. CloudSystem uses specific VLANs on this trunk as Private Networks. All compute nodes in the cloud must be connected to this network.

The Cloud Data Trunk contains the following production networks.

- **Provider Network:** A Provider Network is a data center network routed through the existing data center infrastructure. Adding a Provider Network allows you to add an existing data center network to any number of virtual machine instances in the cloud. These networks are configured from the CloudSystem Console.

- **Private Networks:** Private Networks are created from a pool of VLANs. The cloud administrator configures this pool in the CloudSystem Console. Then, when the cloud administrator switches to the CloudSystem Portal and creates a Private Network, the OpenStack Neutron networking service assigns a VLAN from the pool. OpenStack Neutron networking manages all aspects of this network, including external routing.

---

**Important**
All of the networks described above must be distinct networks.

---

**Required networks**
Table 1 describes the required networks, their purpose and specifies which virtual appliances and compute nodes use these networks.

**Table 1. Required Networks**

<table>
<thead>
<tr>
<th>Network</th>
<th>Number</th>
<th>Purpose</th>
<th>Connected To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Management</td>
<td>1</td>
<td>This network connects virtual appliances to HP 3PAR, VMware vCenter Server, VMware vCloud Networking and Security (vCNS) and compute enclosures. Only administrators have access to this network. In the OpenStack Keystone endpoint catalog, the admin URL is on this network.</td>
<td>Foundation base appliance vCenter proxy appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enterprise appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VMware vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Compute nodes</td>
</tr>
<tr>
<td>Cloud Management Network</td>
<td>1</td>
<td>This network is a dedicated Private Network for cloud management. The Foundation base appliance runs a DHCP server for this network.</td>
<td>Foundation base appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SDN appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network node appliances</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vCenter proxy appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KVM compute nodes</td>
</tr>
<tr>
<td>Network</td>
<td>Number</td>
<td>Purpose</td>
<td>Connected To</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Consumer Access Network</td>
<td>1</td>
<td>This network is a distinct VLAN that gives cloud users a separate access point for the CloudSystem Portal and the Enterprise appliance, where they cannot access administrative-only servers. In the OpenStack Keystone endpoint catalog, the public URL is on this network. <strong>NOTE:</strong> Use this network to launch a console for KVM instances in the CloudSystem Portal.</td>
<td>Foundation base appliance Enterprise appliance</td>
</tr>
<tr>
<td>External Network</td>
<td>1</td>
<td>This network is a distinct VLAN that allows cloud end users to attach public (floating) IP addresses to their provisioned virtual machine instances.</td>
<td>Network node appliances</td>
</tr>
<tr>
<td>Provider Networks and/or Private Networks</td>
<td>At least 1</td>
<td>A Provider Network is a data center network routed through the existing data center infrastructure. A Private Network is created from a pool of VLANs. Both networks support instance communication.</td>
<td>Network node appliances Compute nodes</td>
</tr>
</tbody>
</table>

It is important to understand the relationship between the CloudSystem components, the Data Center Management Network and the Consumer Access Network.

Table 2 describes what CloudSystem components can be accessed from each of these networks.

**Table 2.** CloudSystem connections to the Data Center Management Network and the Consumer Access Network

<table>
<thead>
<tr>
<th>CloudSystem Component</th>
<th>Data Center Management Network</th>
<th>Consumer Access Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudSystem Portal</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CloudSystem Console</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual Machine Console</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>HP CSA Management Console</td>
<td>Yes</td>
<td>Yes (can be blocked with external URL firewall filtering)</td>
</tr>
<tr>
<td>CSA Marketplace Portal</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>HP OO (on Foundation appliance)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>csadmin</td>
<td>Yes (access via adminURL endpoint)</td>
<td>Yes (access via PublicURL endpoint)</td>
</tr>
<tr>
<td>OpenStack Clients</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SAN Fabric</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Sample network configuration of ESXi based environments using HP OneView

The ESXi based environment is configured in a two-node ESXi cluster comprised of two HP ProLiant DL360p Gen8 servers for the management cluster and an HP BladeSystem c7000 enclosure with HP ProLiant BL460c Gen8 servers for the computer nodes.

Environment details

• Management Servers configuration:
  Two DL360p Gen8 servers configured as Helion CloudSystem Management cluster nodes. Each server has a Dual Port 10Gb NIC and a four port 1Gb NIC. These network ports are used as below:
  – 4x 1Gb NIC used for the Management Trunk
  – 2x 10Gb NIC used for Cloud Data Trunk

• Compute nodes configuration:
  Total 16x BL460c Gen8 blades as compute nodes hosted in a single c7000 Enclosure. The c7000 Enclosure has 2 I/O Interconnect Bays installed in Bays 1 and 2 of type HP VC FlexFabric 10Gb/24-Port Module.
  Bays 1 and 2 are used for both Network traffic and SAN traffic.
  In Interconnect Bays 1 and 2, Uplink Ports X5 and X6 are connected to an HP 5900 series Top of Rack Switch, Uplink Ports X1 to X4 are connected to SAN Switches and Uplink Ports X7 and X8 are used as Stacking Links.
  Each compute node is presented with 2x 10Gb ports. These network ports are used as below:
  – 2x 0.5Gb NIC used for the Management Trunk (LOM 1:1a and LOM 1:2a)
  – 2x 2Gb NIC used for the ESXi HA (LOM 1:1c and LOM 1:2c)
  – 2x 3.5Gb NIC used for Cloud Data Trunk (LOM 1:1d and LOM 1:2d)
  – LOM 1:1b and LOM 1:2b are used for SAN

Important
The VLAN IDs and network device names which were used in this sample configuration are specific to this environment.

In this configuration Active/Active network paths were being used for high availability. To achieve this:

• In the ToR switches, network bonding is configured.
• In OneView, two definitions for each network are created with one path being the “A” path and the other the “B” path. These “A” and “B” paths are then bound to their corresponding “A” and “B” interconnects.
• Network teaming is configured for the vSwitches on the ESXi hosts.

Figure 5 and Figure 6 illustrate the physical and logical networking configuration used in this sample configuration.
Figure 5. Physical Network configuration – ESXi Environment
**HP 5900 Series Network Switch configuration**

Table 3 provides the details about the physical network connections to the HP 5900 network switch from both the Management Servers and the c7000 enclosure. It also provides details about the VLANs which need to be configured on the network switch.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Physical NIC</th>
<th>Connected Network Switch Port</th>
<th>Bridge Aggregate</th>
<th>Uplink Set Name</th>
<th>Network Trunk</th>
<th>VLAN IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Server 1</td>
<td>10Gb Port 1 (vmnic0)</td>
<td>Port 11</td>
<td>11</td>
<td>NA</td>
<td>Cloud Data Trunk</td>
<td>300-310</td>
</tr>
<tr>
<td></td>
<td>10Gb Port 2 (vmnic1)</td>
<td>Port 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1Gb Port 1 (vmnic2)</td>
<td>Port 19</td>
<td>10</td>
<td>NA</td>
<td>Management</td>
<td>61, 100, 104, 105, 201, 211</td>
</tr>
<tr>
<td></td>
<td>1Gb Port 2 (vmnic3)</td>
<td>Port 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1Gb Port 3 (vmnic4)</td>
<td>Port 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1Gb Port 4 (vmnic5)</td>
<td>Port 17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To configure the 5900 ToR switch, refer to the information in Table 3 and complete the following steps:

1. Management Server 1 Configuration
   A. Use SSH to log into the switch and supply the appropriate username and password.
   B. Configure Bridge-Aggregation 10 as a static Link-Aggregation. The commands needed are shown below in bold.

   ```
   <snetsw> system-view
   System View: return to User View with Ctrl+Z.
   [snetsw] interface Bridge-Aggregation 10
   [snetsw-Bridge-Aggregation10] description vSwitch0 from management system 1
   [snetsw-Bridge-Aggregation10] quit
   
   C. Insert the ports for vmnic2, vmnic3, vmnic4, and vmnic5 into Bridge-Aggregation 10.
   [snetsw] interface range Ten-GigabitEthernet 1/0/17 to Ten-GigabitEthernet 1/0/20
   [snetsw-if-range] port link-aggregation group 10
   [snetsw-if-range] quit
   
   D. Configure Bridge-Aggregation 10 to pass VLANs 61, 100, 104, 105, 201, 211 as tagged networks.
   [snetsw] interface Bridge-Aggregation 10
   [snetsw-Bridge-Aggregation10] port link-type trunk
   [snetsw-Bridge-Aggregation10] port trunk permit vlan 61 100 104 105 201 211
   [snetsw-Bridge-Aggregation10] quit
   ```
E. Configure Bridge-Aggregation 11 as a static Link-Aggregation.

```
[snetsw] interface Bridge-Aggregation 11
[snetsw-Bridge-Aggregation11] description vSwitch1 from management system 1
[snetsw-Bridge-Aggregation11] quit
```

F. Insert the ports for vmnic0, vmnic1 into Bridge-Aggregation 11.

```
[snetsw] interface range Ten-GigabitEthernet 1/0/11 to Ten-GigabitEthernet 1/0/12
[snetsw-if-range] port link-aggregation group 11
[snetsw-if-range] quit
```

G. Configure Bridge-Aggregation 11 to pass VLANs 300 to 310 as tagged networks.

```
[snetsw] interface Bridge-Aggregation 11
[snetsw-Bridge-Aggregation11] port link-type trunk
[snetsw-Bridge-Aggregation11] port trunk permit vlan 300 to 310
[snetsw-Bridge-Aggregation11] quit
```

H. Save the configuration.

```
[snetsw] save
```

2. Management Server 2 Configuration

A. Use SSH and log into the switch and supply the appropriate username and password.

B. Configure Bridge-Aggregation 12 as a static Link-Aggregation. The commands needed are in bold.

```
<snetsw> system-view
System View: return to User View with Ctrl+Z.
[snetsw] interface Bridge-Aggregation 12
[snetsw-Bridge-Aggregation12] description vSwitch0 from management system 2
[snetsw-Bridge-Aggregation12] quit
```

C. Insert the ports for vmnic2, vmnic3, vmnic4, and vmnic5 into Bridge-Aggregation 12.

```
[snetsw] interface range Ten-GigabitEthernet 1/0/33 to Ten-GigabitEthernet 1/0/36
[snetsw-if-range] port link-aggregation group 12
[snetsw-if-range] quit
```

D. Configure Bridge-Aggregation 12 to pass VLANs 61,100,104,105,201,211 as tagged networks.

```
[snetsw] interface Bridge-Aggregation 12
[snetsw-Bridge-Aggregation12] port link-type trunk
[snetsw-Bridge-Aggregation12] port trunk permit vlan 61 100 104 105 201 211
[snetsw-Bridge-Aggregation12] quit
```

E. Configure Bridge-Aggregation 13 as a static Link-Aggregation.

```
[snetsw] interface Bridge-Aggregation 13
[snetsw-Bridge-Aggregation13] description vSwitch1 from management system 2
[snetsw-Bridge-Aggregation13] quit
```

F. Insert the ports for vmnic0, vmnic1 into Bridge-Aggregation 13

```
[snetsw] interface range Ten-GigabitEthernet 1/0/29 to Ten-GigabitEthernet 1/0/30
[snetsw-if-range] port link-aggregation group 13
[snetsw-if-range] quit
```
G. Configure Bridge-Aggregation 13 to pass VLANs 300 to 310 as tagged networks.

   [snetsw] interface Bridge-Aggregation 13
   [snetsw-Bridge-Aggregation13] port link-type trunk
   [snetsw-Bridge-Aggregation13] port trunk permit vlan 300 to 310
   [snetsw-Bridge-Aggregation13] quit

H. Save the configuration.
   [snetsw] save

3. Compute nodes configuration (Virtual Connect Modules of c7000 enclosure)

A. Use SSH to log into the switch and supply the appropriate username and password.

B. Configure Bridge-Aggregation 6 as a static LACP Link-Aggregation as required for Virtual Connect. The commands needed are in **bold**.

   `<snetsw>` system-view
   System View: return to User View with Ctrl+Z.
   [snetsw] interface Bridge-Aggregation 6
   [snetsw-Bridge-Aggregation6] description Interconnect 1 ports X5 and X6
   [snetsw-Bridge-Aggregation6] link-aggregation mode dynamic
   [snetsw-Bridge-Aggregation6] quit

C. Insert the Interconnect 1 X5 and X6 into Bridge-Aggregation 6.

   [snetsw-if-range] port link-aggregation group 6
   [snetsw-if-range] quit

D. Configure Bridge-Aggregation 6 to pass VLANs 100, 104, 105, and 300-310 as tagged networks.

   [snetsw] interface Bridge-Aggregation 6
   [snetsw-Bridge-Aggregation6] port link-type trunk
   [snetsw-Bridge-Aggregation6] port trunk permit vlan 100 104 105 300 to 310
   [snetsw-Bridge-Aggregation6] quit

E. Configure Bridge-Aggregation 7 as a static LACP Link-Aggregation as required for Virtual Connect.

   [snetsw] interface Bridge-Aggregation 7
   [snetsw-Bridge-Aggregation7] description Interconnect 2 ports X5 and X6
   [snetsw-Bridge-Aggregation7] link-aggregation mode dynamic
   [snetsw-Bridge-Aggregation7] quit

F. Insert the Interconnect 2 X5 and X6 into Bridge-Aggregation 7.

   [snetsw-if-range] port link-aggregation group 7
   [snetsw-if-range] quit

G. Configure Bridge-Aggregation 7 to pass VLANs 100, 104, 105 and 300-310 as tagged networks.

   [snetsw] interface Bridge-Aggregation 7
   [snetsw-Bridge-Aggregation7] port link-type trunk
   [snetsw-Bridge-Aggregation7] port trunk permit vlan 100 104 105 300 to 310
   [snetsw-Bridge-Aggregation7] quit
H. Save the configuration.
   
   [snetsw] save

**vCenter/vSphere Network Switch configuration**

HP Helion CloudSystem supports both Standard vSwitch and Distributed vSwitch types. To use Neutron security group rules, it is required to use Distributed vSwitch.

Choose the vSwitch type, either Standard or Distributed vSwitch based on available vCenter Server licenses and the desired features. CloudSystem supports the following:

- **Standard vSwitches**: Security groups are not functional with Standard vSwitches.
- **Distributed vSwitches**: Basic networking is provided without security groups. Install vCNS/App Firewall to enable security groups. vCNS/App Firewall is set up only when using Distributed vSwitches.

**Note**

To configure the distributed virtual switches a VMware vSphere 5 Enterprise Plus license is required. For more information refer the HP CloudSystem: Using VMware ESXi Clusters as Compute Nodes white paper from the Enterprise Information Library.

**ESXi Management Servers configuration**

Table 4 describes the network configuration required on the Management servers. Use the information in Table 4 to create the vSwitches and Port Groups required for the Helion CloudSystem Software.

**Table 4. Network configuration of ESXi Management Servers**

<table>
<thead>
<tr>
<th>vSwitch Name</th>
<th>Physical NIC of vSwitch</th>
<th>vSwitch Port Group</th>
<th>Network Type</th>
<th>VLAN ID</th>
<th>Network Trunk</th>
<th>vSwitch connection Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSwitch0</td>
<td>vmnic2</td>
<td>CS8-dc-mgmt</td>
<td>Data Center Management Network</td>
<td>100</td>
<td>Management</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>vmnic3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSwitch0</td>
<td>vmnic2</td>
<td>CS8-cmn-mgmt</td>
<td>Cloud Management Network</td>
<td>201</td>
<td>Management</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>vmnic3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSwitch0</td>
<td>vmnic2</td>
<td>CS8-can-mgmt</td>
<td>Consumer Access Network</td>
<td>211</td>
<td>Management</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>vmnic3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSwitch0</td>
<td>vmnic2</td>
<td>CS8-External</td>
<td>External Network</td>
<td>61</td>
<td>Management</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>vmnic3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSwitch0</td>
<td>vmnic2</td>
<td>vmkcompMigration</td>
<td>VMware Migration Network</td>
<td>104</td>
<td>Management</td>
<td>VM Kernel</td>
</tr>
<tr>
<td></td>
<td>vmnic3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSwitch0</td>
<td>vmnic2</td>
<td>vmkcompHA</td>
<td>VMware HA Network</td>
<td>105</td>
<td>Management</td>
<td>VM Kernel</td>
</tr>
<tr>
<td></td>
<td>vmnic3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vmnic5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSwitch0</td>
<td>vmnic0</td>
<td>CS8CloudDataMgmt</td>
<td>Provide and Private Networks</td>
<td>ALL(4095)</td>
<td>Cloud Data Trunk</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>vmnic1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

15
Technical white paper | HP Helion CloudSystem 8.1 networking configuration and troubleshooting

**Note**
Ensure the name of vSwitches and Port groups are the same on both of the Management Servers.

**Management Network Trunk configuration**
For each of the DL360p Gen8 servers that make up the Helion CloudSystem management cluster nodes, perform the following steps to configure vSwitch0 (Management Trunk).

1. Identify the network adapters on the Management node. The following steps assume the ESXi Management network is configured and the node is added to the vCenter server used to manage the ESXi Management cluster nodes.
   - **A.** Log in to the vCenter which is managing the ESXi Management cluster. Select ‘Hosts and Clusters’ under Inventory and select the Management Server. Select the Configuration tab and then the **Hardware → Network Adapters** view to get the list of network adapters in the system. An example of this is shown in Figure 7.
   
   **Figure 7.** Network Adapters in ESXi Host

   ![Network Adapters in ESXi Host](image)

   B. The Management node in Figure 7 shows the server has 2x 10Gb and 4x 1Gb network adapters. Virtual Switch ‘vSwitch0’ is part of Management Trunk and will use vmnic 2-5. Virtual Switch ‘vSwitch1’ is part of Cloud Data Trunk and will use vmnic0-1.

2. Add vmnic2-5 to vSwitch0 if it is not already done. When ESXi is installed vSwitch0 is automatically created as part of the installation.
   - **A.** From the **Hardware → Networking** view click on the **Properties** link for vSwitch0. An example of this is shown in Figure 8.

   **Figure 8.** Networking in ESXi Host

   ![Networking in ESXi Host](image)
B. From the Properties display of vSwitch0 select the Network Adapters tab. From that display, click the Add button to add the adapters to the vSwitch. Select only vmnic2, vmnic3, vmnic4 and vmnic5 network adapters. An example of this is shown in Figure 9.

![Figure 9. Adding unclaimed adapters in ESXi Host](image)

C. Press Next to continue. On the next display the Add Adapter Wizard allows the categorization of whether the new vmnics that are being added are Active or Standby. Ensure that all of the vmnics are marked as Active. An example of this is shown in Figure 10.

![Figure 10. Setting network failover order in ESXi Host](image)

D. Press Next and Finish to complete the network adapter addition to vSwitch0.
E. Return back to the Ports tab of vSwitch0 properties. Select ‘vSwitch0’ and click on Edit to get the vSwitch0 properties window. From that display, select the NIC Teaming tab. In the NIC Teaming tab, use the following values for the Policy Exceptions. An example of this is shown in Figure 11.

- Load Balancing is set to “Route based on IP hash”
- Network Failover Detection is set to “Link status only”
- Notify Switches is “Yes”
- Fallback is “Yes”

**Figure 11. Configure network teaming policy of vSwitch0**

F. Press OK to apply the changes

3. The next step is to create the port groups in vSwitch0 for the Management Trunk. Refer to Table 4 for the list of port groups which need to be created in vSwitch0 for the Management Trunk. The following steps are used to create each port group:

A. From the Ports tab of vSwitch0 properties, click on the Add to create a new port group in vSwitch0. On the next display, the Add Network Wizard allows categorization of whether the new port groups that are being added are Virtual Machine or VMkernel Connection Type. An example of this is shown in Figure 12.

**Figure 12. Creating network port group in vSwitch0**

B. Press Next to continue. On the next display, Connection Settings allows entering the Port Group name and its VLAN ID for Virtual Machine connection type. An example of this is shown in Figure 13.

**Figure 13. Virtual Machine type Network port group properties**
Additional options are chosen for the VMkernel connection type. An example of this is shown in Figure 14.

**Figure 14.** VMkernel type Network port group properties

![VMkernel type Network port group properties](image)

**Note**
For ‘vmkcompHA’ port group, select the *Use this port group for Fault Tolerance logging* option. For ‘vmkcompMigration’ port group, select the *Use this port group for vMotion* option. If the Management servers are already added to the cluster, port groups ‘vmkcompHA’ and ‘vmkcompMigration’ would already be created, there is no need to create these port groups again.

C. Click Finish to create the port group.

D. Repeat steps A-C above for creating all the port groups in vSwitch0 of Management Trunk.

4. From the *Ports* tab of vSwitch0 properties, select the port group and click on *Edit* to get the port group properties window. On the port group properties window, switch to the *NIC Teaming* tab and validate that all four 1Gb vmnics are located under the *Active Adapters* section. The active NIC team behavior for each port group should be inherited from the vSwitch configuration and set to:
   - *Load Balancing* is set to “Route based on IP hash”
   - *Network Failover Detection* is set to “Link status only”
   - *Notify Switches* is “Yes”
   - *Fallback* is “Yes”

5. Click OK to update the policy and repeat step 4 above for all the port groups on vSwitch0. Once verification of all the port groups is done close the vSwitch0 properties window.

**Cloud Data Network Trunk configuration**
For each of the DL360p Gen8 servers that make up the Helion CloudSystem management cluster, perform the following steps to configure vSwitch1 (Cloud Data Trunk):

1. Create vSwitch1 with vmnic0 and vmnic1. This vSwitch will have a single port group, ‘CS8CloudDataMgmt’. vSwitch1 will be used for the Cloud Data Trunk.
   
   A. Return back to the *Hardware ➔ Networking* view, Click on *Add Networking*. An example of this is shown in Figure 15.

   **Figure 15.** Add Networking

   ![Add Networking](image)

   B. On the next display the *Add Network Wizard* allows the categorization of whether the new port groups that are being added are *Virtual Machine or VMkernel Connection Type*. Select the *Virtual Machine* type and click Next.
C. On the next display Virtual Machines – Network Access allows the categorization of whether to create new vSwitch or use the existing vSwitch. Choose Create a vSphere standard switch option and select both vmnic0 and vmnic1. An example of this is shown in Figure 16.

Figure 16. Creating a vSwitch

![Add Network Wizard](image)

D. Press Next to continue. In the Connection Settings wizard, enter the Port Group Network Label, and its VLAN ID for Virtual Machine connection type. Enter the port group Network Label as ’CS8CloudDataMgmt’ and select VLAN ID as ‘All (4095)’ from the drop down menu. An example of this is shown in Figure 17.

Figure 17. Port group properties

E. Press Finish to complete the vSwitch1 and CS8CloudDataMgmt port group creation.

F. From the Hardware Network view click on the Properties link for vSwitch. From the Ports tab of vSwitch1 properties, click on Edit to get the vSwitch1 properties window. From that display, select the NIC Teaming tab. In the NIC Teaming tab, use the following values for the Policy Exceptions.

- Load Balancing is set to “Route based on IP hash”
- Network Failover Detection is set to “Link status only”
- Notify Switches is “Yes”
- Fallback is “Yes”

2. For HP Helion CloudSystem, the security settings of the port group for the Cloud Data Trunk and External Network need to be updated to allow for promiscuous mode traffic, MAC Address changes, and Forged Transmits.

A. In the vSwitch1 properties window, select the CS8CloudDataMgmt port group entry and press the Edit button.

B. On the properties edit window, select the Security tab (see Figure 18) and in this window:

- Click on the checkbox next to Promiscuous Mode and set the value to ACCEPT.
- Click on the checkbox next to MAC Address Changes mode and set the value to ACCEPT.
- Click on the checkbox next to Forged Transmits and set the value to ACCEPT.
- Click on OK to Accept the Changes.

C. On the same port group properties window, switch to the NIC Teaming tab and validate that both 10Gb vmnics are located under the Active Adapters section. The active NIC team behavior for the CS8CloudDataMgmt port group should be inherited from the vSwitch configuration and set to:

- Load Balancing is set to “Route based on IP hash”
- Network Failover Detection is set to “Link status only”
D. Click OK to update the policy. Close the vSwitch1 Properties dialog.

E. In the vSwitch0 properties window, select the **CS8-External** port group entry and press the Edit button.

F. On the properties edit window, select the “Security” tab (see Figure 18) and select the following options:
   - Click on the checkbox next to **Promiscuous Mode** and set the value to **ACCEPT**.
   - Click on the checkbox next to **MAC Address Changes** mode and set the value to **ACCEPT**.
   - Click on the checkbox next to **Forged Transmits** and set the value to **ACCEPT**.
   - Click on OK to Accept the Changes.

   **Figure 18. vSwitch network security properties**

G. Click OK to update the policy. Close the vSwitch0 Properties dialog.

**Important**
Ensure that steps described in Management Network Trunk configuration and Cloud Data Network Trunk configuration are also performed on the second ESXi Management cluster node.

**OneView configuration**
Use OneView to configure the networks and server profiles for your compute nodes.

**Creating Ethernet networks**
To support multiple Active/Active network paths from the enclosure to the network switches, **two** definitions for each network are made with one path being the “A” path and the other the “B” path. These “A” and “B” paths are then bound to their corresponding “A” and “B” interconnects and interconnect uplinks.

To easily identify the networks and how they are mapped back to their intended use, a convention of **CS8Provider<VLAN#>_<A|B>** for Provider Networks and **CS8Tenant<VLAN#>_<A|B>** for Private Networks is used in OneView. In this convention VLAN# represents the VLAN ID for the network that represents the provider or Private Network and <A> or <B> indicates the interconnect path.

In this environment a total of 11 VLANs (from 300 to 310) were created for both Provider and Private Networks. Out of which, VLANs 300-301 are used for Provider Networks and VLANs 302-310 are used for Private Networks. Note the VLANs specified in Table 5 correspond to the VLANs defined in Table 3 and are specific to your environment.

In this sample configuration, the following networks were configured as shown in Table 5.

**Table 5. OneView CS8.1 network list**

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Uplink Set</th>
<th>Ethernet VLAN ID</th>
<th>Preferred Bandwidth</th>
<th>Maximum Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCM_Mgmt_A</td>
<td>SUS_External_A</td>
<td>100</td>
<td>0.5Gb/s</td>
<td>1Gb/s</td>
</tr>
<tr>
<td>DCM_Mgmt_B</td>
<td>SUS_External_B</td>
<td>100</td>
<td>0.5Gb/s</td>
<td>1Gb/s</td>
</tr>
<tr>
<td>Migration_A</td>
<td>SUS_External_A</td>
<td>104</td>
<td>2Gb/s</td>
<td>3Gb/s</td>
</tr>
<tr>
<td>Migration_B</td>
<td>SUS_External_B</td>
<td>104</td>
<td>2Gb/s</td>
<td>3Gb/s</td>
</tr>
<tr>
<td>HA_A</td>
<td>SUS_External_A</td>
<td>105</td>
<td>2Gb/s</td>
<td>3Gb/s</td>
</tr>
<tr>
<td>HA_B</td>
<td>SUS_External_B</td>
<td>105</td>
<td>2Gb/s</td>
<td>3Gb/s</td>
</tr>
</tbody>
</table>
To create the networks required for Helion CloudSystem, refer to the information in Table 5 and complete the following steps:

1. Log in to OneView. Click on the OneView main menu and select Networks under the Networking tab. An example of this is shown in Figure 19.

   ![Figure 19. OneView Networks](image)

2. A new screen will open. Click on the +Create network button in the upper left portion of the screen, a new Create network window will open.
3. For each network create **network entries** using the information provided in Table 5. An example of creating a network is shown in Figure 20.

   A. Enter the **name** of the network – example **DCM_Mgmt_A**
   B. Click the **Ethernet** radio button
   C. Fill in the network’s **VLAN ID** in the VLAN input box – example **100**
   D. The **Purpose** of the network is **General**
   E. Set **Preferred Bandwidth** – example **0.5**
   F. Set **Maximum Bandwidth** – example **1**
   G. The **Smart link** checkbox should remain checked.
   H. The **Private Network** setting must be **unchecked**

   **Figure 20.** OneView Create Network

<table>
<thead>
<tr>
<th>Name</th>
<th>DCM_Mgmt_A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Ethernet</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>100</td>
</tr>
<tr>
<td>Purpose</td>
<td>General</td>
</tr>
<tr>
<td>Preferred bandwidth</td>
<td>0.5 Gb/s</td>
</tr>
<tr>
<td>Maximum bandwidth</td>
<td>1 Gb/s</td>
</tr>
</tbody>
</table>

4. Either press **Create** to create the network and return to the Network list screen or use the **Create +** button to create this network and return back to the Create network window ready for the next network create definition.

**Note**

Ensure all the networks as described in Table 5 have been created, including both the “A” and “B” network definitions for each network so that active/active connectivity can be maintained.
5. After creating all the networks, review the network configuration and verify that all the networks have been created as per the information provided in Table 5. An example of the Networks screen after all the networks are created is shown in Figure 21.

**Figure 21. OneView Network Overview**

---

**Creating Ethernet Network sets**

To support multiple Active/Active network paths from the enclosure to the network switches, two definitions for each network set are made with one path being the “A” path and the other the “B” path. These “A” and “B” paths are then bound to their corresponding “A” and “B” interconnects and interconnect uplinks. Networks belonging to the “A” path would be added to the “A” path network set and Networks belonging to the “B” path would be added to the “B” path network set.

In this sample configuration, the following network sets would be configured as shown in Table 6.

**Table 6. OneView CS8.1 network set list**

<table>
<thead>
<tr>
<th>Network Set Name</th>
<th>Network Set Members (Networks)</th>
<th>Uplink Set</th>
<th>Ethernet VLAN ID</th>
<th>Preferred Bandwidth</th>
<th>Maximum Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt_Set_A</td>
<td>DCM_Mgmt_A</td>
<td>SUS_External_A</td>
<td>100</td>
<td>0.5Gb/s</td>
<td>1Gb/s</td>
</tr>
<tr>
<td>Mgmt_Set_B</td>
<td>DCM_Mgmt_B</td>
<td>SUS_External_B</td>
<td>100</td>
<td>0.5Gb/s</td>
<td>1Gb/s</td>
</tr>
<tr>
<td>Migration_HA_A</td>
<td>Migration_A HA_A</td>
<td>SUS_External_A</td>
<td>104 105</td>
<td>2Gb/s 3Gb/s</td>
<td></td>
</tr>
<tr>
<td>Migration_HA_B</td>
<td>Migration_B HA_B</td>
<td>SUS_External_B</td>
<td>104 105</td>
<td>2Gb/s 3Gb/s</td>
<td></td>
</tr>
<tr>
<td>Network Set Name</td>
<td>Network Set Members (Networks)</td>
<td>Uplink Set</td>
<td>Ethernet VLAN ID</td>
<td>Preferred Bandwidth</td>
<td>Maximum Bandwidth</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------</td>
<td>------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>CloudTrunk_A</td>
<td>CS8Provider300_A</td>
<td>SUS_External_A</td>
<td>305</td>
<td>3.5Gb/s</td>
<td>6Gb/s</td>
</tr>
<tr>
<td></td>
<td>CS8Provider301_A</td>
<td></td>
<td>301</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant302_A</td>
<td></td>
<td>302</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant303_A</td>
<td></td>
<td>303</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant304_A</td>
<td></td>
<td>304</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant305_A</td>
<td>SUS_External_A</td>
<td>305</td>
<td>3.5Gb/s</td>
<td>6Gb/s</td>
</tr>
<tr>
<td></td>
<td>CS8Tenant306_A</td>
<td></td>
<td>306</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant307_A</td>
<td></td>
<td>307</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant308_A</td>
<td></td>
<td>308</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant309_A</td>
<td></td>
<td>309</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant310_A</td>
<td></td>
<td>310</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CloudTrunk_B</td>
<td>CS8Provider300_B</td>
<td>SUS_External_B</td>
<td>305</td>
<td>3.5Gb/s</td>
<td>6Gb/s</td>
</tr>
<tr>
<td></td>
<td>CS8Provider301_B</td>
<td></td>
<td>301</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant302_B</td>
<td></td>
<td>302</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant303_B</td>
<td></td>
<td>303</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant304_B</td>
<td></td>
<td>304</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant305_B</td>
<td>SUS_External_B</td>
<td>305</td>
<td>3.5Gb/s</td>
<td>6Gb/s</td>
</tr>
<tr>
<td></td>
<td>CS8Tenant306_B</td>
<td></td>
<td>306</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant307_B</td>
<td></td>
<td>307</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant308_B</td>
<td></td>
<td>308</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant309_B</td>
<td></td>
<td>309</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS8Tenant310_B</td>
<td></td>
<td>310</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Creation of the Network Sets is a **three-step** process. In the first step, **General** information about the network set needs to be provided (for example Name, Bandwidth details). In the second step, add the networks as members to the network set. In the third step, review the network configuration and create the network set.

To create the network sets based on information in Table 6, complete the following steps:

1. Click on the OneView main menu and select *Network Sets* under the *Networking* tab. An example of this is shown in Figure 22.

**Figure 22.** OneView Network Sets

![OneView Network Sets](image)

2. A new screen will open. Click on the +Create network set button in the upper left portion of the screen. The Create network set window will open.
3. For each network set, provide the **General** and **Network** information to create the network set using the information provided in Table 6.

   **A.** Enter the **General** Information of a network set as shown in in Figure 23.
   - Enter the **Name** of the network set – example **Mgmt_Set_A**
   - Set **Preferred Bandwidth** – example **0.5**
   - Set **Maximum Bandwidth** – example **1**

   **Figure 23.** OneView Create Network Set – General Information

<table>
<thead>
<tr>
<th>Create network set</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Mgmt_Set_A</td>
</tr>
<tr>
<td>Type</td>
<td>Ethernet</td>
</tr>
<tr>
<td>Preferred bandwidth</td>
<td>0.5 Gbps</td>
</tr>
<tr>
<td>Maximum bandwidth</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

   **B.** Click the **Add networks** button under the **Networks** section to add the networks as members to the network set. This opens a new window with a list of available networks as shown in Figure 24. From this window add all the networks that belong to this network set using the information from Table 6.

   **TIP:** Use Ctrl+click to add multiple networks with the mouse cursor (the background turns to light blue) or add multiple networks using the **Add +** button on the same screen.

   **Figure 24.** OneView Create Network Set – Add Networks

<table>
<thead>
<tr>
<th>Add Networks to Mgmt_Set_A</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Add +</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td></td>
</tr>
</tbody>
</table>
C. After adding all the networks to the network set, review the networks selected for this network set as shown in Figure 25.

![Figure 25. OneView Create Network Set – Review Networks](image)

D. After reviewing that the networks in the network set have been added correctly, click on Create to create the single network set or click on the Create + button to create the network set and open a new window for creating another network set.

**Note**

Ensure all the network sets as described in Table 6 have been created including both the “A” and “B” network sets for each network trunk so that active/active connectivity can be maintained.

4. After creating all the networks sets, review the network set configuration to verify all network sets are configured with their respective networks as per Table 6. An example of this is shown in Figure 26.

![Figure 26. OneView Network Sets Review](image)
Logical interconnect groups configuration
Once the networks and network sets are configured, the next step is to create the logical interconnect group (LIG) configuration. When a c7000 enclosure is added to the Enclosure Group, the LIG configuration of that Enclosure Group is applied to the c7000 enclosure.

The information shown in Table 7 was used to create the Logical Interconnect Group for this sample configuration.

Table 7. OneView CS8.1 LIG configuration

<table>
<thead>
<tr>
<th>Uplink Set Name</th>
<th>Uplink Set Type</th>
<th>Uplink Set Connection Mode</th>
<th>Uplink Set LACP Timer</th>
<th>Uplink Set Network Members (Networks)</th>
<th>Uplink Set Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUS_External_A</td>
<td>Ethernet</td>
<td>Automatic</td>
<td>Short</td>
<td>DCM_Mgmt_A, Migration_A, HA_A, CSBProvider300_A, CSBProvider301_A, CSBTenant302_A, CSBTenant303_A, CSBTenant304_A, CSBTenant305_A, CSBTenant306_A, CSBTenant307_A, CSBTenant308_A, CSBTenant309_A, CSBTenant310_A</td>
<td>Interconnect Bay 1 – X5, X6</td>
</tr>
<tr>
<td>SUS_External_B</td>
<td>Ethernet</td>
<td>Automatic</td>
<td>Short</td>
<td>DCM_Mgmt_B, Migration_B, HA_B, CSBProvider300_B, CSBProvider301_B, CSBTenant302_B, CSBTenant303_B, CSBTenant304_B, CSBTenant305_B, CSBTenant306_B, CSBTenant307_B, CSBTenant308_B, CSBTenant309_B, CSBTenant310_B</td>
<td>Interconnect Bay 2 – X5, X6</td>
</tr>
</tbody>
</table>

Creating the Logical Interconnect Group configuration is a multi-step process.

- In the first step General information about Logical interconnect group is provided (for example, Name).
- In the second step, Interconnects are added.
- In the third step uplink set are created.
- In the fourth step, networks are added to the uplink set.
- In the fifth step uplink ports of interconnect are added to the uplink set.
- The Final step is to review the configuration and create the logical interconnect group.

To create the Logical Interconnect Group based on information from Table 7, complete the following steps:

1. From the OneView main menu select Logical Interconnect Groups under the Networking tab as shown in Figure 27.
2. A new screen will open. Click on the + Create logical interconnect group button in the upper left portion of the screen to present the Create logical interconnect group window as shown in Figure 28.

3. Enter the logical interconnect group name **CS8_LIG_FF_A-A**

4. Scroll down and notice that eight interconnect boxes are available to be added, corresponding to eight interconnect bays in a c7000 enclosure. In this sample configuration we will use the first two bays populated with HP Virtual Connect FlexFabric modules
   
   A. Click Add Interconnect in Bay 1, and in the dropdown list select **HP VC FlexFabric 10Gb/24-Port Module**.
   
   B. Repeat the same process with interconnect in Bay 2. Notice the box is pre-populated with HP VC FlexFabric 10Gb/24-Port Module matching Bay 1.

   **Figure 28. OneView Create logical interconnect group**

   ![Create logical interconnect group](image-url)
5. After adding interconnects, we need to define **uplinks**. An uplink is an outward bound connection of interconnect to a network. Click the **Add uplink set** button. The **Create uplink set** window opens. An example of this is shown in Figure 29.

A. In the **Create uplink set** window, create the uplink sets (SUS_External_A and SUS_External_B) using the information from Table 7.
   - Enter the **Name** of the uplink set – example **SUS_External_A**.
   - Select **Type** as **Ethernet** from the dropdown list.
   - Select **Connection Mode** as **Automatic**.
   - Select **LACP timer** as **Short**.

   ![Figure 29. OneView LIG Create Uplink Set](image)

B. Click on **Add Networks** under the **Networks** tab. This will open a new window **Add Networks to Uplink Set**. Add the networks belonging to this uplink set here. For SUS_External_A uplink set, add all the networks ending with _A and for SUS_External_B uplink set add all the networks ending with _B. For details refer to Table 7. An example of this is shown in Figure 30.

   ![Figure 30. OneView LIG Add Networks to Uplink Set](image)
**TIP:** Use Ctrl+click to add multiple networks with the mouse cursor (the background turns to light blue) or add multiple networks using Add + button on the same screen. Use the filter option to reduce the number of networks displayed.

C. Once the Add Networks form is completed, the screen will return back to the **Create uplink set window** again. Click on **Add uplink ports** under the **Uplink ports** tab. This will open a new window **Add uplink ports to <uplink set name>**. Add the uplink ports that belong to this uplink set. For SUS_External_A uplink set add Interconnect Bay 1, ports X5 and X6; and for SUS_External_B uplink set add Interconnect Bay 2, ports X5 and X6. For details refer to Table 7. An example of this is shown in Figure 31.

**Figure 31.** OneView LIG Add Uplink Ports to Uplink Set

<table>
<thead>
<tr>
<th>Interconnect Module</th>
<th>Bay</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X1</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X2</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X3</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X4</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X5</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X6</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X7</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>1</td>
<td>X8</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>2</td>
<td>X1</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>2</td>
<td>X2</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>2</td>
<td>X3</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>2</td>
<td>X4</td>
</tr>
<tr>
<td>HP VC FlexFabric 10Gb/24-Port Module</td>
<td>2</td>
<td>X5</td>
</tr>
</tbody>
</table>

2 selected

Add    Add +    Cancel
D. After the uplink ports are added, the screen will return back to the Create uplink screen. Review the configuration of the uplink set to ensure all the networks and correct uplink ports have been added. An example of this is shown in Figure 32.

**Figure 32.** OneView LIG Create uplink set review

![Create uplink set screen](image)

E. After reviewing the configuration of the uplink set, click on Create to create this uplink set or click on the Create+ button to create this uplink set and open a new window for creating another uplink set.

**Note**
Ensure both SUS_External_A and SUS_External_B uplink sets are configured correctly with the respective networks and uplink ports as per the information provided in Table 7.
6. After the uplink sets are added, the screen will return back to the *Create logical interconnect group* screen. Review the configuration of the logical interconnect group. An example of this is shown in Figure 33.

**Figure 33.** OneView LIG Create logical interconnect group review

![Create LIG Screen]

**Note**
In this sample configuration, SAN traffic will use the same HP VC FlexFabric adapters in Bay 1 and Bay 2 using ports X1, X2, X3, and X4. Thus the networks for the SAN traffic need to be created and added to the CSB_LIG_FF_A-A interconnect group. Detailed steps to add SAN networks is beyond the scope of this document.

7. After reviewing and verifying the configuration of the logical interconnect group, click on *Create* to complete the creation of logical interconnect group CSB_LIG_FF_A-A.

**Creating Enclosure Group**
Enclosure Groups in OneView allow the grouping of multiple c7000 enclosures using the same configuration for network connectivity. A Logical Interconnect Group is required when creating the enclosure group.

In this sample configuration, the CSB_LIG_FF_A-A logical interconnect group which was added in earlier steps will now be added to the Enclosure Group.

Create the Enclosure Group **CSB-Compute** using the **CSB_LIG_FF_A-A** logical interconnect group using the following steps:

1. Click on the OneView main menu and select *Enclosure Groups* under the *Servers* tab. An example of this is shown in Figure 34.

**Figure 34.** OneView Enclosure Groups
2. A new screen will open. Click on *Create enclosure group* in the upper left portion of the screen. This will open a *Create Enclosure Group* window. An example of this is shown in Figure 35.

Fill in the following details

- **Name** CS8-Compute
- **Select the Logical interconnect group** CS8_LIG_FF_A-A

**Figure 35.** OneView Create Enclosure Groups

![Create Enclosure Group](image)

Modified Name to "CS8-Compute"

3. Click on the *Create* button to create the enclosure group.

**Note**

When enclosures are added to this CS8-Compute Enclosure group, the **CS8_LIG_FF_A-A** logical interconnect group configuration is applied to the enclosures.
Adding enclosure

To add a c7000 enclosure to the **CS8-Compute** Enclosure Group, complete the following steps:

1. Click on the OneView main menu and select *Enclosures* under the *Servers* tab. An example of this is shown in Figure 36.

   **Figure 36.** OneView Enclosures

   ![OneView Enclosures](image)

2. A new screen will open, click on *+ Add Enclosure* in the upper left portion of the screen. This will open the *Add Enclosure* window. An example of this is shown in Figure 37.

   Fill in the following details
   
   - Enter the OA IP address or host name.
   - Enter the OA User name and Password under the *Credentials* section.
   - Select the *Enclosure group* as **CS8-Compute**.
   - Select the appropriate OneView licensing.

   **Figure 37.** OneView Add Enclosure

   ![OneView Add Enclosure](image)

3. Click on *Add* to add the enclosure to the **CS8-Compute** enclosure group.
Note
When a c7000 enclosure is added to the enclosure group in OneView, the logical interconnect group configuration of that enclosure group is applied to the enclosure.

4. After the enclosure is added to the **CS8-Compute** enclosure group the logical interconnect configuration of that enclosure will resemble the configuration shown in Figure 38.

**Figure 38.** OneView Logical Interconnect configuration

Create Server Profiles
In this sample configuration, there are 16 BL460c Gen8 blades which are used as compute nodes. First create a server profile template using the network information from Table 8. After the template is created, use this template to apply the configuration to all 16 blades in the c7000 enclosure using the copy option.

When creating the Server Profile template use the network connection information from Table 8.

Note
While adding the network connections to the Server Profile, select a **Network Set** instead of specifying a single network.

**Table 8.** OneView Server Profile Network Connections

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Network (Network set)</th>
<th>Requested Bandwidth(Gb/s)</th>
<th>Port</th>
<th>Boot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet</td>
<td>Mgmt_Set_A</td>
<td>0.5</td>
<td>FlexibleLOM 1:1-a</td>
<td>Primary</td>
</tr>
<tr>
<td>2</td>
<td>Ethernet</td>
<td>Mgmt_Set_B</td>
<td>0.5</td>
<td>FlexibleLOM 1:2-a</td>
<td>Secondary</td>
</tr>
<tr>
<td>3</td>
<td>Ethernet</td>
<td>Migration_HA_A</td>
<td>2</td>
<td>FlexibleLOM 1:1-c</td>
<td>Not Bootable</td>
</tr>
<tr>
<td>4</td>
<td>Ethernet</td>
<td>Migration_HA_B</td>
<td>2</td>
<td>FlexibleLOM 1:2-c</td>
<td>Not Bootable</td>
</tr>
<tr>
<td>5</td>
<td>Ethernet</td>
<td>CloudTrunk_A</td>
<td>3.5</td>
<td>FlexibleLOM 1:1-d</td>
<td>Not Bootable</td>
</tr>
<tr>
<td>6</td>
<td>Ethernet</td>
<td>CloudTrunk_B</td>
<td>3.5</td>
<td>FlexibleLOM 1:2-d</td>
<td>Not Bootable</td>
</tr>
</tbody>
</table>
Complete the following steps to create the Server Profile template and apply that server profile to all the blades using the information from Table 8:

1. Click on the OneView main menu and select Server Profiles under the Servers tab. An example of this is shown in Figure 39.

   **Figure 39. OneView Server Profiles**

   ![OneView Server Profiles](image)

2. A new screen will open. Click on + Create profile in the upper left portion of the screen. This will open a Create Server profile window. From this page, we will create an unassigned server profile which we will use as a template for all of our compute nodes. An example of this is shown in Figure 40.

   A. Enter the following in the General section
      - Enter the Name of the server profile – example CS8Compute-Template
      - Enter the Description of the server profile – CS8.1 Compute Nodes Server Profile Template
      - Select Server hardware as unassigned
      - Select Server hardware type as BL460c Gen8 1
      - Select Enclosure group as CS8-Compute
      - Select Affinity as Device bay

   **Figure 40. OneView Create server profile**
B. Using the network connections information from Table 8 add the network connections to the server profile template. Click on Add Connections to add the network connection to the server profile. This will open a new window Add Connection. An example of this is shown in Figure 41.

Enter the following in the Add Connection Window
- Select the Device type – example Ethernet
- Select the Network from the available network sets – Example Mgmt_Set_A
- Enter the Requested bandwidth (Gb/s) – Example 0.5
- Select the Port – Example FlexibleLOM 1:1-a
- Select Boot – Example Primary

![Figure 41. OneView Create server profile Add Connection](image)

C. Repeat the above steps until all six network connections and two SAN network connections are added. After all the network connections have been added, the Create server profile screen should look like as shown in Figure 42.

![Figure 42. OneView Create server profile review](image)
D. After verifying all the network connections were added correctly as per the information in Table 8 click on Create to create the CS8Compute-Template Server profile.

3. Follow the steps below to create the server profile for all 16 blades using the CS8Compute-Template server profile which was created earlier.

E. From the OneView main menu select Server Profiles under the Servers tab. Click on the CS8Compute-Template server profile to view the server profile information. An example of this is shown in Figure 43.

**Figure 43.** OneView server profile overview

A. From the Actions menu in the upper right portion of the screen, select Copy which opens a new window Copy CS8Compute-Template. Enter the following details. An example of this is shown in Figure 44.

- Enter the Name of the server profile – CS8compute-vmware<Bay Number>
- Enter the Description of the server profile – CS8.1 Compute Nodes Server Profile <Bay No>
- Select Server hardware – Select the Bay Number from the dropdown list

**Figure 44.** OneView copy Server Profile

B. Click on Create + to create the server profile and apply the profile to the selected blade. Create and apply a profile for each compute node.
C. Once the server profile is applied to the blade, it will have the following networking configuration as shown in Figure 45.

**Figure 45. OneView blade overview after server profile**

This section describes the network configuration for blade servers that will be used as compute nodes. Table 9 describes the network configuration required on the blades which will be used as compute nodes.

**Table 9. Network configuration of ESXi compute nodes**

<table>
<thead>
<tr>
<th>vSwitch Type</th>
<th>vSwitch Name</th>
<th>Physical NIC of vSwitch</th>
<th>vSwitch Port Group</th>
<th>Network Type</th>
<th>VLAN ID</th>
<th>Network Trunk</th>
<th>vSwitch connection Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>vSwitch0</td>
<td>vmnic0</td>
<td>CS8-dc-mgmt</td>
<td>Data Center Management Network</td>
<td>100</td>
<td>Management</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>Standard</td>
<td>vSwitch1</td>
<td>vmnic2</td>
<td>vmkcompMigration</td>
<td>VMware Migration Network</td>
<td>104</td>
<td>VMware ClusterMgmt</td>
<td>VM Kernel</td>
</tr>
<tr>
<td>Standard</td>
<td>vSwitch1</td>
<td>vmnic2</td>
<td>vmkcompHA</td>
<td>VMware HA Network</td>
<td>105</td>
<td>VMware ClusterMgmt</td>
<td>VM Kernel</td>
</tr>
<tr>
<td>Distributed</td>
<td>CS8Cloud Data</td>
<td>vmnic4</td>
<td>NA</td>
<td>Provider and Private Networks</td>
<td>300-310</td>
<td>Cloud Data Trunk</td>
<td>NA</td>
</tr>
</tbody>
</table>

**Note**
Ensure the name of vSwitches and Port Groups are the same across all the compute nodes.
Management Network Trunk configuration

For each of the BL460c Gen8 blades that will be a compute node, perform the following steps to configure vSwitch0 (Management Trunk) and vSwitch1 (VMware Cluster Mgmt):

1. Find the network adapters on the compute node. These steps assume that the ESXi Management network is configured and the host is added to the vCenter server which is managing the ESXi Compute cluster nodes.
   A. Log in to the vCenter server that is managing the ESXi Compute cluster. Select ‘Hosts and Clusters’ under Inventory and select the compute node. Select the Configuration tab and then Hardware ➔ Network Adapters view to get the list of network adapters in the system. An example of this is shown in Figure 46.

   **Figure 46. Network Adapters in ESXi compute node**
   ![Network Adapters in ESXi compute node](image)

   B. Figure 46 shows that this compute node has six network adapters. Virtual Switch ‘vSwitch0’ which is part of the Management Trunk will use vmnic 0-1 and Virtual Switch ‘vSwitch1’ which is part of the VMware Cluster Mgmt will use vmnic 2-3. Distributed Virtual Switch CS8CloudData which is part of Cloud Data Trunk will use vmnic 4-5.

2. Add vmnic0-1 to vSwitch0 if it is not already done. When ESXi is installed vSwitch0 would have been created.
   A. From the Hardware ➔ Networking view, click on the Properties link for vSwitch0. An example of this is shown in Figure 47.

   **Figure 47. Networking in ESXi compute node**
   ![Networking in ESXi compute node](image)

   B. From the Properties display of vSwitch0 select the Network Adapters tab. From that display, click the Add button to add the adapters to the vSwitch. Select only vmnic0 and vmnic1 network adapters. An example of this is shown in Figure 48.

   **Figure 48. Adding unclaimed adapters in ESXi compute node**
   ![Adding unclaimed adapters in ESXi compute node](image)
C. Press Next to continue. The Add Adapter Wizard specifies whether the new vmnics that are being added are Active or Standby. Ensure that all of the vmnics are marked as Active. An example of this is shown in Figure 49.

Figure 49. Setting network failover order in ESXi compute node

D. Press Next and Finish to complete the network adapter addition to vSwitch0.

3. The next step is to create the port groups in vSwitch0 for the Management Trunk. There is only a single port group CS8-dc-mgmt which is required to be created in vSwitch0. Follow the steps below to create the CS8-dc-mgmt port group:

A. From the Ports tab of vSwitch0 properties, Click on Add to create a new port group in vSwitch0. Select Connection Type Virtual Machine as shown in Figure 50.

Figure 50. Creating network port group in ESXi compute node

B. Press Next to continue. Enter the port group Network Label as ‘CS8-dc-mgmt’ and select the VLAN ID as ‘100’. An example of this is shown in Figure 51.

Figure 51. Virtual Machine type Network port group properties in ESXi compute node

C. Click Finish to create the port group.
4. The next step is to create vSwitch1 and to create the port groups in vSwitch1 for the VMware Cluster Management Trunk.

**Note**
If the compute nodes are already added to the cluster, port groups 'vmkcompHA' and 'vmkcompMigration' are already created and then there is no need to create these port groups again and this step can be skipped.

A. From the Hardware → Networking view, click on Add Networking. An example of this is shown in Figure 52.

**Figure 52.** Add Networking in ESXi compute node

B. From the Add Network Wizard select the VMkernel type and click Next.

C. From the VMkernel – Network Access window choose the Create a vSphere standard switch option and select both vmnic2 and vmnic3. An example of this is shown in Figure 53.

**Figure 53.** Creating vSwitch in ESXi compute node

D. Press Next to continue. From the Connection Settings window specify port group network label as vmkcompMigration, enter the VLAN ID as **104** and select the Use this port group for vMotion option. An example of this is shown in Figure 54.

**Figure 54.** Port group properties in ESXi compute node

E. Press Next to continue. From the VMkernel IP Settings window, enter the details of the IP Address, Subnet mask and Gateway Address. Once the details are entered press Finish to complete the vSwitch1 and vmkcompMigration port group creation.

F. From the Ports tab of vSwitch1 properties, click on Add to create a new port group vmkcompHA in vSwitch1. From the Add Network Wizard select the VMkernel type.
G. Press Next to continue. From the Connection Settings window enter Network Label (port group name) as vmkcompHA, enter the VLAN ID as 105 and select the Use this port group for Fault Tolerance logging option. An example of this is shown in Figure 55.

**Figure 55.** VMkernel type Network port group properties in ESXi compute node

H. Press Next to continue. From the VMkernel IP Settings window, enter the details of the IP Address and Subnet mask. Once details are entered press Finish to complete the vmkcompHA port group creation.

**Important**

Ensure that the steps described in Management Network Trunk configuration are performed on all blades which will be used as compute nodes.
Cloud Data Network Trunk configuration
The Cloud Data Trunk for compute nodes is created as a Distributed Virtual Switch using vmnic4 and vmnic5 network adapters.

To create a Distributed Virtual Switch and add uplink ports complete the following steps:

1. Change to the networking view in the vSphere client by selecting View → Inventory → Networking from the vCenter client menu bar. Select and then right-click the compute cluster data center name data center entry and choose New vSphere Distributed Switch from the pop-up menu presented.

2. The Create vSphere Distributed Switch window appears presenting a list of available vSphere Distributed Switch versions that can be created. Select vSphere Distributed Switch Version: 5.5.0 from the list and press Next.

3. Enter a name of CS8CloudData for the new Distributed vSwitch and an uplink port count of 2 as shown in Figure 56. Press Next to continue.

Figure 56. Specifying the Name and number of port groups for Cloud Data Trunk
4. The *Add Hosts and Physical Adapters* window allows the specification of which Virtual Machine Hosts the Distributed Switch should be associated with and which vmnics on those hosts will be used for the two uplinks. From the list presented, select all of the compute nodes. Click the [+] symbol to expand the list of network adapters on those hosts and select vmnic4 and vmnic5 as the two NICs to associate with the uplinks for each compute node. An example of this is shown in Figure 57. Press Next to progress to the *Ready to Complete* summary display.

**Figure 57.** Adding vmnic4 and vmnic5 to Distributed vSwitch

5. On the summary display, uncheck the *Automatically create a default port group* checkbox (see Figure 58) and click on the *Finish* button to create the Cloud Data Trunk Distributed Switch.

**Figure 58.** Distributed Switch summary display

6. Verify that the definition of the Distributed Switch is correctly associated with each of the servers by selecting each server in turn in the vCenter client, choosing the *Hardware → Networking* panel under the *Configuration* tab.
and then pressing the vSphere Distributed Switch button. Each server should have CS8CloudData listed with the appropriate vmnics (vmnic4 and vmnic5) attached.

**Important steps during Helion CloudSystem 8.1 installation**

1. While installing Helion CloudSystem 8.1, ensure network configuration is supplied properly. The details for the Data Center Management (DCM) and Consumer Access Network (CAN) network configurations in the deployer.conf file are shown below:

   [Data Center Management Network]
   foundation_hostname = <FQDN host name of Foundation VM on DCM Network>
   type = static
   foundation_ip = <IP Address of the Foundation VM on DCM network>
   gateway = <Gateway of DCM Network>
   dns = <DNS Server of DCM Network>
   bridge = CS8-dc-mgmt

   [Access Network]
   foundation_hostname = <FQDN host name of Foundation VM on CAN Network>
   type = static
   foundation_ip = <IP Address of the Foundation VM on CAN network>
   gateway = <Gateway of CAN Network>
   bridge = CS8-can-mgmt

**Important Points to note**

- Ensure there is a DNS Server configured on the DCM network. Add Foundation and Enterprise VM names in the DNS server and ensure the hostnames are resolvable. Both DCM and CAN hostnames should be resolvable via this DNS Server for both Foundation and Enterprise VMs.
- Set the Gateway Address on only ONE network, either on the DCM or the CAN network. It is recommend to set the default Gateway on the CAN network, instead of on the DCM network.

**Note**

In Helion CloudSystem 8.1 and 8.1 Update 1 versions there is a known limitation, where a login to the CSA Marketplace portal fails with “Service Unavailable” if the gateway is configured on the CAN network. Manual changes are required to correct the issue. This issue has been resolved in the Helion CloudSystem 8.1 Update 2 release. For more information on the manual steps refer the *HP CloudSystem 8.1 Update 2 Release Notes* from the *Enterprise Information Library*.

For more information on the gateway and how to set the static routes, refer the *HP CloudSystem 8.1 Installation and Configuration guide* from the *Enterprise Information Library*.

**Sample network configuration of KVM based environments using HP Virtual Connect Manager**

The KVM based environment is configured with a single DL360p Gen8 server for management and a c7000 with BL460c Gen8 servers for computer nodes.

**Environment details**

- **Management Server Configuration**
  One DL360p Gen8 configured as Helion CloudSystem Management server. This server has a dual port 10Gb NIC and a four port 1Gb NIC. Out of the four port 1Gb NIC, only a single port is used in this configuration. These network ports are used as shown below:

  - 1x 10Gb NIC used for the Management Trunk
  - 1x 10Gb NIC used for Cloud Data Trunk
  - 1x 1Gb NIC used for External Network Trunk
• Compute nodes configuration
  16x BL460c Gen8 blades as compute nodes hosted in a single c7000 Enclosure. The c7000 Enclosure has (4) I/O Interconnect Bays installed in Bays 1, 2, 5, and 6 of type HP FlexFabric 10Gb/24-Port Module.
  Bays 1 and 2 are used for Network traffic. Bays 5 and 6 are used for SAN traffic.
  In Bays 1 and 2, Uplink Ports X5 and X6 are connected to an HP 5900 series Top of Rack Switch and Uplink Ports X7 and X8 are used as Stacking Links.
  In Bays 5 and 6, Uplink ports X1, X2, X3, and X4 are connected to the SAN Director Switch and Uplink ports X7 and X8 are used as Stacking Links.
  Each compute node is presented with 2x 10Gb ports. These network ports are used as shown below:
  – 1x 10Gb NIC used for the Management Trunk
  – 1x 10Gb NIC used for Cloud Data Trunk

**Important**
In this sample configuration, a single network adapter was used in the network trunks which means there is no Active/Active network configuration. For Active/Active networking configurations the following changes are required.
  • Create the network trunks in the ToR Switches
  • Configure the HP Virtual Connect Manager (VCM) in Active-Active Network configuration
  • Instead of using the physical interfaces in the Management Server and compute nodes, create the network bonding interfaces and create the bridge interface on the bonded interfaces

Detailed step by step instructions are beyond the scope of this document.

**Important**
The VLAN IDs and network device names which were used in this sample configuration are specific to this environment.

Figure 59 and Figure 60 describe the physical and logical networking configuration used in this sample configuration.
Figure 59. Physical Network configuration – KVM Environment
Figure 60. Sample network configuration – KVM Management server and KVM compute nodes

HP 5900 Series Network Switch configuration

Table 10 provides details about the physical network connections to the HP 5900 network switch from Management Server and the c7000 enclosure. It also provides details about the VLANs which need to be configured on the network switch.

Table 10. Physical Network configuration details – KVM environment

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Physical NIC</th>
<th>Connected Network Switch Port</th>
<th>Bridge Aggregate</th>
<th>Uplink Set Name</th>
<th>Network Trunk</th>
<th>VLAN IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Server</td>
<td>10Gb Port1 (eth0)</td>
<td>Port 11</td>
<td>NA</td>
<td>NA</td>
<td>Management</td>
<td>437, 637, 737</td>
</tr>
<tr>
<td></td>
<td>10Gb Port2 (eth1)</td>
<td>Port 12</td>
<td>NA</td>
<td>NA</td>
<td>Cloud Data Trunk</td>
<td>2901-2906</td>
</tr>
<tr>
<td></td>
<td>1Gb Port 4 (eth5)</td>
<td>Port 13</td>
<td>NA</td>
<td>NA</td>
<td>External Network</td>
<td>537</td>
</tr>
<tr>
<td>Compute nodes (VC Modules)</td>
<td>Interconnect Bay 1 Port X5</td>
<td>Port 1</td>
<td>4</td>
<td>SUS_External_A</td>
<td>Management</td>
<td>437, 737, 2901-2906</td>
</tr>
<tr>
<td></td>
<td>Interconnect Bay 1 Port X6</td>
<td>Port 2</td>
<td></td>
<td></td>
<td>Cloud Data Trunk</td>
<td>2901-2906</td>
</tr>
<tr>
<td></td>
<td>Interconnect Bay 2 Port X5</td>
<td>Port 4</td>
<td>5</td>
<td>SUS_External_B</td>
<td>Cloud Data Trunk</td>
<td>437, 737, 2901-2906</td>
</tr>
<tr>
<td></td>
<td>Interconnect Bay 2 Port X6</td>
<td>Port 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Complete the Network switch side configuration using the information from Table 10 following these steps:

1. **Management Server Configuration**
   
   A. Use SSH to log into the switch and supply the appropriate username and password.

   B. Enter the following commands to set up eth0 with VLANs 437, 637, and 737 as tagged networks. The commands needed are in **bold**.

   ```
   <snetsw>system-view
   System View: return to User View with Ctrl+Z.
   [snetsw]interface Ten-GigabitEthernet 1/0/11
   [snetsw-Ten-GigabitEthernet1/0/11]port link-type trunk
   [snetsw-Ten-GigabitEthernet1/0/11]port trunk permit vlan 437 637 737
   [snetsw-Ten-GigabitEthernet1/0/11]quit
   
   C. Enter the following commands to set up eth1 with VLANs 2901-2906 as tagged networks. The commands needed are in **bold**. You should already be in `system-view`.

   ```
   [snetsw]interface Ten-GigabitEthernet 1/0/12
   [snetsw-Ten-GigabitEthernet1/0/12]port link-type trunk
   [snetsw-Ten-GigabitEthernet1/0/12]port trunk permit vlan 2901 to 2906
   [snetsw-Ten-GigabitEthernet1/0/12]quit
   
   D. Enter the following commands to set up eth5 with VLAN 537 as an untagged network. The commands needed are in **bold**. You should already be in `system-view`.

   ```
   [snetsw]interface Ten-GigabitEthernet 1/0/13
   [snetsw-Ten-GigabitEthernet1/0/13]port access vlan 537
   [snetsw-Ten-GigabitEthernet1/0/13]quit
   
   E. Save the configuration.

   [snetsw]save
   ```

2. **Compute nodes configuration (Virtual Connect Modules of c7000 Enclosure)**

   A. Use SSH to log into the switch and supply the appropriate username and password.

   B. Configure Bridge-Aggregation 4 as a static LACP Link-Aggregation as required for Virtual Connect. The commands needed are in **bold**.

   ```
   <snetsw>system-view
   System View: return to User View with Ctrl+Z.
   [snetsw]interface Bridge-Aggregation 4
   [snetsw-Bridge-Aggregation4]description Interconnect 1 ports X5 and X6
   [snetsw-Bridge-Aggregation4]link-aggregation mode dynamic
   [snetsw-Bridge-Aggregation4]quit
   
   C. Insert the Interconnect 1 X5 and X6 into Bridge-Aggregation 4.

   ```

   ```
   [snetsw]interface range Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/2
   [snetsw-if-range]port link-aggregation group 4
   [snetsw-if-range]quit
   ```
D. Configure Bridge-Aggregation 4 to pass VLANs 437, 737 and 2901-2906 as tagged networks.

```
[snetsw] interface Bridge-Aggregation 4
[snetsw-Bridge-Aggregation4] port link-type trunk
[snetsw-Bridge-Aggregation4] port trunk permit vlan 437 737 2901 to 2906
[snetsw-Bridge-Aggregation4] quit
```

E. Configure Bridge-Aggregation 5 as a static LACP Link-Aggregation as required for Virtual Connect.

```
[snetsw] interface Bridge-Aggregation 5
[snetsw-Bridge-Aggregation5] description Interconnect 2 ports X5 and X6
[snetsw-Bridge-Aggregation5] link-aggregation mode dynamic
[snetsw-Bridge-Aggregation5] quit
```

F. Insert the Interconnect 2 X5 and X6 into Bridge-Aggregation 5.

```
[snetsw] interface range Ten-GigabitEthernet 1/0/3 to Ten-GigabitEthernet 1/0/4
[snetsw-if-range] port link-aggregation group 5
[snetsw-if-range] quit
```

G. Configure Bridge-Aggregation 5 to pass VLANs 437, 737 and 2901-2906 as tagged networks.

```
[snetsw] interface Bridge-Aggregation 5
[snetsw-Bridge-Aggregation5] port link-type trunk
[snetsw-Bridge-Aggregation5] port trunk permit vlan 437 737 2901 to 2906
[snetsw-Bridge-Aggregation5] quit
```

H. Save the configuration.

```
[snetsw] save
```

**KVM Management Server configuration**

To configure the DL360p Gen8 server as a Helion CloudSystem management server, complete the following steps:

1. Download and install the Red Hat Enterprise Linux (RHEL) OS on the Management Cluster node.

---

**Note**

For software requirements refer the *HP CloudSystem 8.1 Installation and Configuration Guide* from the Enterprise Information Library.

---

2. Ensure VLAN software is installed and configured on the system:
    - Ensure that the module is loaded by entering the following command:
      ```
      #lsmod | grep 8021q
      ```
    - If the module is not loaded, load it with the following command:
      ```
      #modprobe 8021q
      ```
3. Table 11 describes the network configuration required on the Management server. Using this information configure the VLAN interfaces and Bridges accordingly.

**Table 11.** Network configuration on the Management Server

<table>
<thead>
<tr>
<th>Physical NIC</th>
<th>VLAN Interface</th>
<th>Bridge Interface</th>
<th>Network Type</th>
<th>Boot Proto</th>
<th>IP Address</th>
<th>Network Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>eth0.437</td>
<td>br-dc-mgmt</td>
<td>Data Center Management Network</td>
<td>Static</td>
<td>X.X.X.X</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth0</td>
<td>eth0.737</td>
<td>br-cmn-mgmt</td>
<td>Cloud Management Network</td>
<td>none</td>
<td>None</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth0</td>
<td>eth0.637</td>
<td>br-can-mgmt</td>
<td>Consumer Access Network</td>
<td>none</td>
<td>None</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth1</td>
<td>none</td>
<td>br-cloud-trunk</td>
<td>Provider and Private Networks</td>
<td>none</td>
<td>None</td>
<td>Cloud Data Trunk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth5</td>
<td>none</td>
<td>br-external</td>
<td>External Network</td>
<td>none</td>
<td>None</td>
<td>External Network</td>
</tr>
</tbody>
</table>

**Note**

In Figure 4 the External Network is shown as it is part of the Management Trunk. The External Network can be configured in the Management trunk as shown in Figure 4 or the External Network can be configured using a dedicated network trunk if hardware resources are available. In this sample configuration the External Network is configured using a dedicated network trunk. The External Network is ONLY required in the Management Server.

4. Configure the Management Trunk Network:
   - Configure the physical interface in `/etc/sysconfig/network-scripts/ifcfg-eth0`, as follows:
     ```
     #vi ifcfg-eth0
     DEVICE=eth0
     HWADDR=6C:3B:E5:BA:D5:80
     TYPE=Ethernet
     UUID=d406960a-3af3-4711-be96-9afa8154ef7
     ONBOOT=yes
     NM_CONTROLLED=no
     BOOTPROTO=none
     ```

**Important**

Don’t copy and paste the HWADDR or UUID from the above configuration. HWADDR and UUID are unique for each system and interface.
- Configure the VLAN interface in `/etc/sysconfig/network-scripts`. The configuration filename should be the physical interface plus a `.` character plus the VLAN ID number. For example, if the VLAN ID is 437, and the physical interface is eth0, then the configuration filename should be `ifcfg-eth0.437`:

  ```
  #vi ifcfg-eth0.437
  DEVICE=eth0.437
  BOOTPROTO=None
  ONBOOT=yes
  USERCTL=no
  VLAN=yes
  BRIDGE=br-dc-mgmt
  ```

  ```
  #vi ifcfg-eth0.737
  DEVICE=eth0.737
  BOOTPROTO=None
  ONBOOT=yes
  USERCTL=no
  VLAN=yes
  BRIDGE=br-cmn-mgmt
  ```

  ```
  #vi ifcfg-eth0.637
  DEVICE=eth0.637
  BOOTPROTO=None
  ONBOOT=yes
  USERCTL=no
  VLAN=yes
  BRIDGE=br-can-mgmt
  ```

- Create the bridge devices and configure the IP accordingly

  ```
  #vi ifcfg-br-dc-mgmt
  DEVICE=br-dc-mgmt
  TYPE="Bridge"
  IPADDR=X.X.X.X
  NETMASK=X.X.X.X
  BOOTPROTO=static
  ONBOOT=yes
  NM_CONTROLLED=no
  DELAY=0
  DNS1=<IP of the DNS Server>
  # Data Center Mgmt Network (DCM), vlan 437
  ```

  ```
  #vi ifcfg-br-cmn-mgmt
  DEVICE=br-cmn-mgmt
  TYPE="Bridge"
  BOOTPROTO=None
  ONBOOT=yes
  NM_CONTROLLED=no
  DELAY=0
  # Cloud Management Network (CMN), vlan 737
  ```

**Note**
In the Management server only, configure the IP Address and DNS server details in the DCM Network interface, i.e., `br-dc-mgmt`. 
#vi ifcfg-br-can-mgmt
DEVICE=br-can-mgmt
TYPE="Bridge"
BOOTPROTO=none
ONBOOT=yes
NM_CONTROLLED=no
DELAY=0
# Consumer Access Network (CAN), vlan 637

5. Configure the Cloud Trunk Network:
   - Configure your physical interface in /etc/sysconfig/network-scripts/ifcfg-ethX,
     where X is a unique number corresponding to a specific interface, as follows:

```
#vi ifcfg-eth1
DEVICE=eth1
HWADDR=6C:3B:E5:BA:D5:84
TYPE=Ethernet
UUID=94e4454e-8a74-4277-bbd8-71e530148682
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BRIDGE=br-cloud-trunk
```

**Important**
Don’t copy and paste the HWADDR or UUID from the above configuration. HWADDR and UUID are unique for each system and interface.

   - Create the br-cloud-trunk bridge device

```
#vi ifcfg-br-cloud-trunk
DEVICE=br-cloud-trunk
TYPE="Bridge"
BOOTPROTO=none
ONBOOT=yes
NM_CONTROLLED=no
DELAY=0
# VLAN All - <Provider/Private Network VLAN Ranges>
```

**Note**
In a Helion CloudSystem configuration, Provider and Private Networks data passes through the Cloud Trunk Network and it may contain multiple VLANs. There is no IP Assignment required for this br-cloud-trunk bridge.

6. Configure the External Network:
   - Configure your physical interface in /etc/sysconfig/network-scripts/ifcfg-ethX,
     where X is a unique number corresponding to a specific interface, as follows:

```
#vi ifcfg-eth5
DEVICE=eth5
HWADDR=AC:16:2D:86:8E:33
TYPE=Ethernet
UUID=c0779951-432f-4ee6-9d50-79ac684742c6
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BRIDGE=br-external
```
Important
Don’t copy and paste the HWADDR or UUID from the above configuration. HWADDR and UUID are unique for each system and interface.

- Create the br-external bridge device:

```bash
#vi ifcfg-br-external
DEVICE=br-external
TYPE="Bridge"
BOOTPROTO=None
ONBOOT=yes
NM_CONTROLLED=no
DELAY=0
# ext net VLAN 537
```

7. After configuring the network, restart the networking service to put these changes into effect:

```
#service network restart
```

VCM configuration
When using server blades as compute nodes, use the VCM to configure the networks and server profiles.

In the compute nodes, the following network trunks need to be configured:

1. Management Trunk – In this trunk, Data Center Management Network (DCM) and Cloud Management Trunk (CMN) must be configured. There is no need to configure the External Network and Consumer Access Network (CAN) since those networks are only needed on the Helion CloudSystem Management server.

2. Cloud Data Trunk – In this trunk, networks for both Provider and Private Networks must be configured.

Create Shared Uplink Sets
In this sample configuration, Shared Uplink Set ‘SUS_External_A’ is created using Interconnect Bay 1, Ports X5 and X6. Shared Uplink Set ‘SUS_External_B’ is created using Interconnect Bay 2, Ports X5 and X6.

To create the two Shared Uplink sets, complete the following steps:

1. Log in to the VCM. Click on Shared Uplink Sets under the Connections section and then click on ‘+ Add’. An example of this is shown in Figure 59.
2. Create the Uplink Set by defining the name and add the Ports using the information contained in Table 12. An example of this is shown in Figure 62.

**Table 12. VCM Uplink Set configuration**

<table>
<thead>
<tr>
<th>Uplink Set Name</th>
<th>Interconnect</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUS_External_A</td>
<td>Bay 1</td>
<td>X5, X6</td>
</tr>
<tr>
<td>SUS_External_B</td>
<td>Bay 2</td>
<td>X5, X6</td>
</tr>
</tbody>
</table>

A. Define the Uplink Set Name, example ‘SUS_External_A’.
B. Click on Add Port to add the uplink ports.
C. Select the interconnect bay and add the ports, example Bay 1, ports X5, X6.
D. Click on Apply once the ports are added to the respective Uplink Set Name to apply the configuration.
E. Repeat steps A-D for creating the 2nd Uplink set.

**Figure 62. VCM Define Shared Uplink Set**

3. After creating both uplink sets, the Shared Uplink Sets should resemble the configuration shown in Figure 63.

**Figure 63. VCM Shared Uplink Sets final configuration**
Create networks
Create all the networks required in both the Management Trunk and the Cloud Data Trunk using the following steps:

1. Log in to the VCM and click on Ethernet Networks under the Connections section and click on ‘+ Add’. An example of this is shown in Figure 64.

   Figure 64. VCM Create Networks

2. Create the Networks by defining the Name and adding External Ports using the information from Table 13. An example of this is shown in Figure 65.

   Table 13. VCM Networks details in Management and Cloud Data Trunks

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Shared Uplink Set</th>
<th>Ethernet VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCM_Network_A</td>
<td>SUSExternal_A</td>
<td>437</td>
</tr>
<tr>
<td>CMN_Network_A</td>
<td>SUSExternal_A</td>
<td>737</td>
</tr>
<tr>
<td>CloudTrunk_B2901</td>
<td>SUSExternal_B</td>
<td>2901</td>
</tr>
<tr>
<td>CloudTrunk_B2902</td>
<td>SUSExternal_B</td>
<td>2902</td>
</tr>
<tr>
<td>CloudTrunk_B2903</td>
<td>SUSExternal_B</td>
<td>2903</td>
</tr>
<tr>
<td>CloudTrunk_B2904</td>
<td>SUSExternal_B</td>
<td>2904</td>
</tr>
<tr>
<td>CloudTrunk_B2905</td>
<td>SUSExternal_B</td>
<td>2905</td>
</tr>
<tr>
<td>CloudTrunk_B2906</td>
<td>SUSExternal_B</td>
<td>2906</td>
</tr>
</tbody>
</table>
A. Define the Network name, example 'DCM_Network_A'.
B. Select the tick mark ‘Use Shared Uplink Set’ under the External Ports tab.
C. Select the desired ‘Shared Uplink Set’, example ‘SUS_External_A’.
D. Enter the desired ‘Ethernet VLAN ID’, example 437.
E. Click on ‘Apply’ to create the network.

**Figure 65.** VCM Define the Ethernet Network

F. Repeat steps A-E to create all the additional networks.

3. After creating all the networks as described in Table 13, the network screen should resemble the configuration shown in Figure 66.

**Figure 66.** Ethernet Network overview
Note
For this environment 6 networks were created using ‘CloudTrunk_B2901’ to ‘CloudTrunk_B2906’ with VLAN IDs from 2901 to 2906 using SUS_External_B Uplink Set.

Create Server Profiles for compute nodes
The following network configuration will be used when creating the server profiles:

Port 1 (LOM1:1-a) of the Server has multiple networks that belong to the Management Trunk which are connected to Shared Uplink Set ‘SUS_External_A’. These are DCM_Network_A and CMN_Network_A.

Port 2 (LOM1:2-a) of the Server has multiple networks that belong to the Cloud Data Trunk which are connected to Shared Uplink Set ‘SUS_External_B’. These are all the networks which are created for both Provider and Private Networks, i.e., CloudTrunk_B2901 to CloudTrunk_B2906.

Using this configuration, Management Network traffic passes through a single Uplink Set, i.e., SUS_External_A; and Cloud Data Trunk Network traffic passes through SUS_External_B.

Note
In a Helion CloudSystem Environment, compute nodes do not require access to the Consumer Access Network (CAN) or the External Network. Instances running on the compute nodes will access the External Network via Floating IPs using the Virtual Routers residing on the network nodes.

Complete the following steps to create the Server Profiles and assign those server profiles to all the Blades which will be used as compute nodes:

1. To create the server profile, log in to the VCM and click on Server Profiles under the Connections section, then click on ‘+ Add’. An example of this is shown in Figure 67.

![Figure 67. VCM Create Server Profiles](image)

2. Create and apply the server profile:
   A. Define the Profile name under Profile Name, example – novacompute_08.
   B. Under Ethernet Adapter Connections, for Port 1 select ‘Multiple Networks’ under Network Name using the dropdown menu. An example of this is shown in Figure 68.

![Figure 68. VCM Defining Ethernet Adapter Connections to first port](image)
C. Selecting Multiple Networks will display a new screen. Drag and drop DCM_Network_A and CMN_Network_A to the Networks in mapping section, then click OK to add the networks. An example of this is shown in Figure 69.

**Figure 69. VCM Adding Ethernet Adapter Connections**

![VCM Adding Ethernet Adapter Connections](image)

D. Under Ethernet Adapter Connections, for Port 2 select ‘Multiple Networks’ under Network Name using the dropdown menu.

E. Selecting Multiple Networks will display a new screen. Drag and drop CloudTrunk_B2901 to CloudTrunk_B2906 to the Network in mapping section, then click OK to add the networks. An example of this is shown in Figure 70.

**Figure 70. VCM Adding Ethernet Connections to second port**

![VCM Adding Ethernet Connections to second port](image)

F. Under the ‘Assign Profile to Server Bay’ section, select the server to which this profile will be assigned, then click on ‘Apply & Close’ to apply the server profile to the blade that will be used as a compute node. An example of this is shown in Figure 71.

**Figure 71. VCM Assign Server Profiles to Server Bay**

![VCM Assign Server Profiles to Server Bay](image)
G. Repeat steps A thru F to create and apply the server profiles to the remaining blade servers that will be used as compute nodes.

**KVM compute nodes configuration**

Complete the following steps to configure blade servers as compute nodes:

1. Download and Install the RHEL OS on the compute nodes.

Note
For software requirements refer the *HP CloudSystem 8.1 Installation and Configuration Guide* from the Enterprise Information Library.

2. Ensure VLAN software is installed and configured on the system:
   - Ensure that the module is loaded by entering the following command:
     ```
     #lsmod | grep 8021q
     ```
   - If the module is not loaded, load it with the following command:
     ```
     #modprobe 8021q
     ```

3. Table 14 describes the network configuration required on the compute nodes. Use the information in this table to configure VLAN interfaces and Bridges.

   **Table 14. Network configuration on the KVM compute nodes**

<table>
<thead>
<tr>
<th>Physical NIC</th>
<th>VLAN Interface</th>
<th>Bridge Interface</th>
<th>Network Type</th>
<th>Boot Proto</th>
<th>IP Address</th>
<th>Network Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>eth0.437</td>
<td>br-dc-mgmt</td>
<td>Data Center Management Network</td>
<td>Static</td>
<td>X.X.X.X</td>
<td>Management</td>
</tr>
<tr>
<td>eth0</td>
<td>eth0.737</td>
<td>br-cmn-mgmt</td>
<td>Cloud Management Network</td>
<td>DHCP</td>
<td>None</td>
<td>Management</td>
</tr>
<tr>
<td>eth1</td>
<td>None</td>
<td>None</td>
<td>Provider and Private Networks</td>
<td>None</td>
<td>None</td>
<td>Cloud Data Trunk</td>
</tr>
</tbody>
</table>

Note
'Consumer Access Network' and 'External Network' are not configured on compute nodes.

4. Configure the Management Trunk Network:
   - Configure the physical interface in `/etc/sysconfig/network-scripts/ifcfg-eth0`, as follows:
     ```
     #vi ifcfg-eth0
     DEVICE=eth0
     HWADDR=6C:3B:E5:BA:D5:80
     TYPE=Ethernet
     UUID=d406560a-3afc-471f-be96-9afa81549ef7
     ONBOOT=yes
     NM_CONTROLLED=no
     BOOTPROTO=None
     ```
**Important**

Don't copy and paste the HWADDR or UUID from the above configuration. HWADDR and UUID are unique for each system and interface.

- Configure the VLAN interface in `/etc/sysconfig/network-scripts`. The configuration filename should be the physical interface plus a "." character plus the VLAN ID number. For example, if the VLAN ID is 437, and the physical interface is eth0, then the configuration filename should be `ifcfg-eth0.437`:

  ```
  #vi ifcfg-eth0.437
  DEVICE=eth0.437
  BOOTPROTO=none
  ONBOOT=yes
  NM_CONTROLLED=no
  USERCTL=no
  VLAN=yes
  BRIDGE=br-dc-mgmt
  
  #vi ifcfg-eth0.737
  DEVICE=eth0.737
  BOOTPROTO=none
  ONBOOT=yes
  NM_CONTROLLED=no
  USERCTL=no
  VLAN=yes
  BRIDGE=br-cmn-mgmt
  ```

- Create the bridge devices and configure the IP accordingly.

**Note**

In Helion CloudSystem, a static IP address is configured for both the br-dc-mgmt and br-cmn-mgmt bridges. The IP address for br-cmn-mgmt is allocated by DHCP from the DHCP server running on the Foundation VM on the CMN network.

```
#vi ifcfg-br-dc-mgmt
DEVICE=br-dc-mgmt
TYPE="Bridge"
IPADDR=X.X.X.X
NETMASK=X.X.X.X
BOOTPROTO=static
ONBOOT=yes
NM_CONTROLLED=no
DELAY=0
DNS1=<IP of the DNS Server>
# dc-mgmt, vlan 437

#vi ifcfg-br-cmn-mgmt
DEVICE=br-cmn-mgmt
TYPE="Bridge"
BOOTPROTO=dhcp
ONBOOT=yes
NM_CONTROLLED=no
DELAY=0
# cmn-mgmt, vlan 737
```
5. Configure the Cloud Trunk Network
   o Configure your physical interface in /etc/sysconfig/network-scripts/ifcfg-ethX, where X is a unique number corresponding to a specific interface, as follows:
     #vi ifcfg-eth1
     DEVICE=eth1
     HWADDR=6C:3B:E5:BA:D5:84
     TYPE=Ethernet
     UUID=94e4454e-8a74-4277-bbd8-71e530148682
     ONBOOT=yes
     NM_CONTROLLED=no
     BOOTPROTO=none

Important
Don’t copy and paste the HWADDR or UUID from the above configuration. HWADDR and UUID are unique for each system and interface.

Note
In Helion CloudSystem Provider and Private Networks, data passes through the Cloud Trunk Network which may contain multiple VLANs. There is no IP Assignment required for the eth1 interface.

6. Modify the /etc/sysconfig/network file:
   o Modify the /etc/sysconfig/network file and add the compute node's hostname as shown below. Replace 'compute01' with the actual host name of the compute node:
     #vi /etc/sysconfig/network
     NETWORKING=yes
     HOSTNAME=compute01.domainame
     DHCP_HOSTNAME=compute01

Note
HOSTNAME should contain the FQDN name, whereas DHCP_HOSTNAME should contain only NON-FQDN name.

7. After configuring the network, restart the networking service to put these changes into effect.
   #service network restart
Repeat the steps in this section for each of your compute nodes.

Important steps during the Helion CloudSystem 8.1 installation
1. While installing Helion CloudSystem 8.1, ensure the network configuration is properly defined. Below are the details for the DCM and CAN network configuration in the deployer.conf file:
   [Data Center Management Network]
   foundation_hostname = <FQDN host name of Foundation VM on DCM Network>
   type = static
   foundation_ip = <IP Address of the Foundation VM on DCM network>
   gateway = <Gateway of DCM Network>
   dns = <DNS Server of DCM Network>
   bridge = br-dc-mgmt
[Access Network]
foundation_hostname = <FQDN host name of Foundation VM on CAN Network>
type = static
foundation_ip = <IP Address of the Foundation VM on CAN network>
gateway = <Gateway of CAN Network>
bridge = br-can-mgmt

### Important Points to note
- Ensure there is a DNS Server configured on the DCM network. Add the Foundation and Enterprise VM names in the DNS server and ensure the host names are resolvable. Both DCM and CAN hostnames should be resolvable via this DNS Server for both Foundation and Enterprise VMs.
- Set the Gateway Address on only ONE network, either on the DCM or the CAN network. It is recommend to set the default Gateway on the CAN network, instead of on the DCM network.

### Note
In Helion CloudSystem 8.1 and 8.1 Update 1 versions there is a known limitation, where a login to the CSA Marketplace portal fails with “Service Unavailable” if the gateway is configured on the CAN network. Manual changes are required to correct the issue. This issue has been resolved in the Helion CloudSystem 8.1 Update 2 release. For more information on the manual steps refer the HP CloudSystem 8.1 Update 2 Release Notes from the Enterprise Information Library.

For more information on the gateway and how to set the static routes, refer the HP CloudSystem 8.1 Installation and Configuration Guide from the Enterprise Information Library.

2. When activating the compute nodes, choose ‘eth1’ as the Cloud Data Trunk interface.

### Network operations in Helion CloudSystem

#### Provider Networks
A Provider Network is a data center network routed through the existing data center infrastructure. Provider Networks give admins the ability to plumb legacy networks into their cloud and choose whether or not to let OpenStack Networking manage the network. Adding a Provider Network allows you to add an existing data center network to any number of virtual machine instances in the cloud. A Provider Network is typically shared by multiple tenants at the discretion of the administrator.

Provider Networks are configured from the CloudSystem Console.

A Provider Network is part of the Cloud Data Trunk, which is the physical network hosting the VLANs that OpenStack Networking makes available to users. The Cloud Data Trunk connects compute nodes and allows virtual machine instances to communicate with each other.

Example use cases of Provider Networks:
- A shared database server which currently resides in the legacy data center infrastructure network and cloud instances across multiple tenants would like to access the database.
- A shared software hosting server which currently resides in the legacy data center infrastructure network and cloud instances across multiple tenants would like to access the server.

#### Private Networks
Private Networks are part of the Cloud Data Trunk. Private Networks are created from a pool of VLANs. The cloud administrator configures this pool in the CloudSystem Console. Then, when the cloud administrator switches to the CloudSystem Portal and creates a Private Network, the OpenStack Neutron Networking service assigns a VLAN from the pool. End users create individual Private Networks using the pool of VLANs which are configured by the Cloud Administrator. Therefore, each Private Network is shared exclusively among members of a given project.

OpenStack Neutron Networking manages all aspects of this network, including external routing.

Private Networks are created within the cloud and they are private in nature. This means these networks can’t be accessed outside the cloud environment. Only instances within that Private Network can talk to each other by default. If instances need to talk to another Private Network, a virtual router must be created. Connect both Private Networks to the router so the instances can communicate across the tenants.
The following steps must be completed if the instances need to communicate outside the cloud environment:

- A virtual router needs to be created if none exists.
- Add the Private Network to the router.
- Ensure the External Network subnet is already configured (this will be done by the Cloud Administrator) and configure the External Network as a gateway to the router.
- Allocate a floating IP Address from the pool.
- Associate a floating IP Address to the instance (which would create a NAT entry between the private and floating IP).

Once the above steps are completed, the instance can communicate outside the private cloud via floating IP Address.

**External Network**

The External Network allows users to route Private Networks on virtual machine instances out from the CloudSystem private cloud to the data center, the corporate intranet, and the Internet via a floating IP. One External Network is automatically created during CloudSystem Foundation installation. Virtual machines are not directly attached to the External Network. Internal Provider and Private Networks connect directly to virtual machine instances. The External Network connects to network nodes.

After installation, one can use the features in the CloudSystem Portal to enable use of the External Network for accessing VM instances on cloud networks. The Cloud Administrator creates a subnet for the External Network. Cloud users can then create routers to connect the External Network to the Private Networks for their projects. Traffic from the External Network is routed to selected virtual machines inside the cloud using floating IP addresses.

Only a single subnet is allowed for the External Network. Be sure to configure the External Network subnet with an address range that is large enough to accommodate future expansion.

**Routers**

Cloud users can create routers to connect Private Networks for their projects to the External Network or to another Private Network within the same project. These virtual routers are created in network nodes and provide the routing functionality within the cloud.

**Security Groups**

Access to the instances is controlled by security groups which are a collection of inbound (ingress) and outbound (egress) rules about which sources, protocols and ports a server can send/receive traffic from. No traffic can be received by a server unless a security group rule explicitly allows it.

Whenever a new project (or tenant) is created, a default security group is created for that project. In Helion CloudSystem default security groups have the following rules:

- Allow all the outbound (egress) traffic by default from the instance. There are two rules for this egress traffic, one for IPv4 and the other for IPv6.
- Allow inbound (ingress) traffic only between the instances belonging to the same security group, i.e., default security group in this case. Inbound (ingress) traffic outside the default security group is dropped. There are two rules for this ingress traffic, one for IPv4 and the other for IPv6.

If the default security group is assigned to an instance (if we don't assign any security group to the instance during the instance creation, default security group is assigned to the instance), then PING and SSH requests sent to the instance are blocked by the firewall. Instances within the same project can connect only via the Private IP.

Create new security groups or modify the default security group and define additional ingress rules to allow access to virtual machines in the private cloud. Additional security groups can be applied to an instance after it is deployed. These new security groups can be defined to allow SSH, ICMP, HTTP or any other source or protocol required for your environment.

When ESXi clusters are used as compute nodes, security group functionality is provided by VMware vCNS, and not exclusively by the security group rules configurable from the CloudSystem Portal. To use the security group functionality with ESXi clusters as compute nodes the following must be true:

- Cloud Data Trunk Network should be configured as ‘Distributed Virtual Switch (DVS)’. All the ESXi hosts in that compute cluster should have uplink ports to this Distributed Virtual Switch.
- VMware vShield Manager virtual appliance must be installed and configured for each managed vCenter Server, as a single vShield Manager can serve only a single vCenter Server environment.
• vShield App virtual appliance must be installed from vShield Manager on each ESXi host in the cluster that is managed from the management vCenter Server.

• CloudSystem Foundation requires that all vShield Manager certificate names match compute host names.

• vShield Manager is registered in the CloudSystem Console as part of the vCenter Server registration.

**Important**
Security group rules in default security groups were configured differently between different releases of Helion CloudSystem versions, for more details refer HP CloudSystem 8.1 and 8.1 Update 1 Release Notes from the Enterprise Information Library.

**Role of network nodes**
The network nodes play a very important role in Helion CloudSystem environments.

Neutron DHCP agents run on the network nodes and provide the IP address to the instances if the neutron networks are configured with DHCP enabled.

Virtual Routers are created in the network nodes to allow:

• Network traffic across different Private Networks (intra network communication) within the cloud travels through the network nodes (East-West Routing)

• Network traffic between VMs Private Network and External Network (using Floating IPs) travels through the network nodes (North-South Routing)

**Note**
Network traffic across VMs that belong to the same Private Network will not pass through the network node even if the VMs are running on different compute nodes.

**Important**
When using the Provider Networks, network traffic does not travel through the network nodes.

Network throughput of the instances (intra network and External Network communication) is dependent on the performance of the network nodes and the physical link capacity of the External Network trunk on the Management server.

In Helion CloudSystem environments network nodes are virtual machines, so there will be additional overhead when converting the virtual network packets to physical network packets and vice versa.

Helion CloudSystem has three network nodes which run in high availability mode. If any one of the network nodes is down, agents running on that network node will be migrated to the surviving network nodes. If all the network nodes are down, the DHCP agents and virtual routers running on the network nodes will not be available. When all the network nodes are down:

• Instances that are configured to get the IP address via DHCP will not be allocated an IP address if they are rebooted.

• Instances across different Private Networks cannot communicate with each other.

• Instances cannot communicate via the External Network using floating IPs.
Figure 72 describes the network packet flow between two VM instances residing on the same compute node and connected to different Private Networks.

- VM1 and VM2 belong to the same tenant and reside on the same compute node but on different Private Networks.
- When VM1 wants to communicate with VM2, packets have to traverse from VM1 to the network node and then back from the network node to VM2 because the Virtual Router is currently running on the network node.

**Figure 72.** Network flow between two VMs across different Private Networks in KVM environment (east–west routing)
Figure 73 describes the network packet flow between a VM instance and the External Network via Floating IP.

- If VM1 wants to communicate outside the cloud environment using a Floating IP Address via the External Network, network packets from VM1 have to pass-through the network node to reach the External Network and vice versa since virtual routers reside in the network nodes.

**Figure 73.** Network flow between VM and External Network in KVM environment (north-south routing)
Figure 74 describes the network packet flow between the VM instance and a system in the Provider Network.

- If VM1 wants to communicate with a system in the Provider Network, network packets from VM1 are transmitted directly to the system in the Provider Network without traveling through the network nodes.

**Figure 74.** Network flow between VM and Provider Network in KVM environment

---

**Troubleshooting Helion CloudSystem network issues**

**KVM compute node does not appear in CloudSystem Console for activation**

When the network is configured correctly, compute nodes automatically get a DHCP address from the Foundation VM on the Cloud Management Network. Check for the following:

- Check whether the compute node got the IP address on the Cloud Management Network bridge interface.
  - If the compute node is not getting the IP address on CMN Bridge interface:
    - Check whether the ‘BOOTPROTO’ setting is set to ‘dhcp’ for CMN network bridge interface. If it is not set to ‘dhcp’, change the setting to ‘dhcp’ and run ‘ifdown <CMN bridge interface>’ and ‘ifup <CMN bridge interface>’.
    - If the compute node is still not getting the IP address on CMN Bridge interface, check whether the Cloud Management Network is correctly configured on the network switch, HP OneView/VCM configuration, and VLAN/Bridge interfaces on the compute node.

- Check whether the correct host names were added in the /etc/sysconfig/network file:
  - `HOSTNAME=<FQDN of the hostname of compute node>`
  - `DHCP_HOSTNAME=<NON FQDN hostname of compute node>`

  Example
  
  `HOSTNAME=compute01.mydomain.net`
  
  `DHCP_HOSTNAME=compute01`

  If entries are not added correctly, make the configuration changes and restart the compute node.
Common networking configuration issues

Here are some of the common networking configuration issues which affect the networking functionality in Helion CloudSystem environments:

- Management Trunk and Cloud Data Trunk VLANs were not added in the ToR switches.
- Management Trunk and Cloud Data Trunk Networks are not created or created with incorrect VLANs.
- In a VCM environment, Management Trunk and Cloud Data Trunk Networks were not added to the server profiles.
- In a OneView environment, Management Trunk and Cloud Data Trunk Networks were not added to the network sets or incorrect Network sets were added to server profiles.
- In an ESXi environment on Management Servers, “Promiscuous mode”, “MAC Address Changes” and “Forged Transmits” were not set to Accept for Cloud Trunk and External Network port groups.
- In an Active/Active configuration, network teaming (ToR Switch side), active-active network configuration (VCM or OneView) or bonding (KVM or ESXi hosts) was not configured correctly, which causes intermittent network packet losses.

Check and correct the network configuration issues using the Sample network configuration of ESXi based environments using HP OneView and Sample network configuration of KVM based environments using HP VCM steps.

Common Helion CloudSystem networking issues

Instances in error state due to network port creation failure

When creating an instance, if the network port is not created then the instance fails to get created and reports a status of error. Some possible causes are:

- neutron-server process in Foundation appliance VM or SDN controller is not able to create the network port.
- L2 agents running on the compute nodes are not able to create the network port.

Follow the steps below to identify and troubleshoot the issue:

1. Check the CloudSystem Console activity log for any error messages.
2. Verify that the SDN Controller appliance VM is up and running on the Management cluster nodes.
3. Check for any network configuration mismatches on the Cloud Data Trunk configuration in compute nodes (KVM) or vCenter-proxy appliance VM (ESXi).
4. Log in to the Foundation appliance console as described in Logging in to the appliance consoles.
5. Check the neutron-server process log file “/var/log/neutron/server.log” for any errors.
6. Check the state of the L2 agents from the CloudSystem Portal. Log in to the CloudSystem Portal, click on the Admin tab, then click on System Info tab, and then click on Network Agents as shown in Figure 75 and Figure 76.

Figure 75. Network agents status in KVM environment
7. If the state of the L2 agent shows “Up” then the agent is up and running, otherwise the agent is not running and there are problems with that agent.

**Note**
For KVM compute nodes, each compute node has its own L2 agent (Open vSwitch agent). For ESXi compute nodes there is an L2 agent (HP ISC L2 Agent) per vCenter and the L2 agent runs on the vCenter-proxy vm.

8. If any of the L2 agents are down, log in to the respective compute node (KVM) or vCenter-proxy appliance VM via the console (ESXi). Check the following logs and take corrective actions to fix the issue.

   **KVM compute nodes:**
   - /var/log/sdn/hp-vcn/hp-sdn-agent.log
   - /var/log/sdn/hp-vcn/hp-ovs-agent.log
   - /var/log/nova/compute.log

   **ESXi – vCenter-proxy VM:**
   - /var/log/sdn/isc-neutron-agent.log
   - /var/log/sdn/hp-vcn/hp-sdn-agent.log
   - /var/log/nova/compute.log

**Note**
To log in to the vCenter-proxy appliance VM, console access needs to be enabled as described in Enabling appliance console access for this VM and logging in to the console of the VM is described in Logging in to the appliance consoles.

### Instance not able to get the DHCP IP address

When an instance is created successfully, its state becomes active and the IP address assigned to the instance is visible in the CloudSystem Portal. However, when booting the instance, it is not able to get the DHCP address.

When instances are booted, the IP address is assigned by the DHCP agent running on the network node appliance VM. There is a DHCP agent running on each network node. A single DHCP agent can manage multiple networks. Subnets belonging to the network should be configured with DHCP enabled in order for the instance to get a DHCP address.

Follow the steps below to identify and troubleshoot the issue

1. Check whether DHCP is enabled for the specified subnet/network. If DHCP is not enabled for the subnet, edit the subnet and enable DHCP.

   Perform the following steps to check and enable DHCP on the particular subnet.
A. From the Horizon portal, click on **Networks** under the **Manage Network** section, then click on the required network.

**Figure 77. Networks**

B. Under the Network Overview screen, click on the desired subnet.

**Figure 78. Network Overview**

C. Under the Subnet Overview screen, check whether DHCP is enabled for this subnet.

**Figure 79. Subnet Overview**

---

**Note**

If DHCP is not enabled for the subnet or the instance is not configured to get an IP address from DHCP then the instance will not get a DHCP address.
D. To enable DHCP for the subnet go back to the Network Overview screen and click on **Edit Subnet** for the desired subnet as shown in Figure 80.

**Figure 80. Network overview**

![Network overview](image)

E. Under the Update Subnet screen, click on the Subnet Detail tab and click the **Tick Mark** to enable DHCP for this subnet and click **Update** as shown in Figure 81.

**Figure 81. Update Subnet**

![Update Subnet](image)

F. Check whether the instance is able to get an IP address from DHCP. If the instance is still not getting an IP address proceed to the next step.
2. Find the DHCP agent’s interface IP address that belongs to the subnet. From the **Network Overview** screen of the CloudSystem Portal, under the **Ports** section find the IP address of the `networkdhcp` network port. In Figure 8.2, 10.0.1.2 is the IP address of the DHCP agent interface for this network.

   **Figure 8.2.** Network port details

   ![Network Overview Screen](image)

3. Log in to the instance console and assign a manual IP address.

   **Note**
   For ESXi based instances, log in to the instance console using vSphere. For KVM based instances, log in to the instance console using CloudSystem Portal.

   ```bash
   Linux based instances:
   #ifconfig eth0 <IP address of the instance> netmask <netmask of the network> up
   
   Example:
   #ifconfig eth0 192.168.146.10 netmask 255.255.255.0 up
   
   **Note**
   If the DHCP IP is not assigned to the instance we can manually assign the same IP to the instance and check any network connectivity issues or any issues with the DHCP agents on the network nodes.

4. From the instance console check the connectivity to the DHCP network port of that network:

   ```bash
   #ping <IP address of the DHCP agent interface of the network>
   ```

5. If we are able to ping the DHCP agent interface IP address then network connectivity between the compute node and Management server is working fine. There might be a problem with the `dnsmasq` process of this network running on the network node. Proceed to Step 8 for further troubleshooting on page 76.

6. If we are not able to ping the DHCP agent interface IP address, the probable causes include:
   - All three network nodes are down or DHCP agents on all three network nodes are down.
   - There might be a network configuration or communication problem between the compute node and the Management nodes where the network nodes are running.
7. Check the status of the network nodes. Log in to the CloudSystem Portal, click on the Admin tab, click on System Info tab, and then click on Network Agents.

**Figure 83.** Network agents status

![Network Agents](image)

If the state of the **DHCP agent** shows “Up” then the agent is up and running, otherwise the agent is not running. All three network nodes should report **DHCP agent State is **Up** otherwise instances cannot get a DHCP IP address.

Network node appliance VMs cannot be accessed via the console using ‘cloudadmin’ to check why DHCP agents are down on the network nodes. At this stage engage the HP Support team to troubleshoot further why the DHCP agents are down.

If all the **DHCP agents** states show ‘Up’ then there might be some network configuration or communication problem between Management servers and compute nodes, proceed to step **Check Physical network connectivity between the Management Servers and compute nodes** for further troubleshooting.

8. Find out which network node is managing the network by logging in to the Foundation appliance VM console:
   - Log in to the Foundation appliance VM Console using cloudadmin.
   - Source the environment variables.
   - Find the network ID of the instance which failed to get the DHCP IP after sourcing the environment variables:

```
$ neutron net-list
```

**Figure 84.** Example neutron net list output

```
+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| Id              | Subnet          | Name            | Network         | Devices         |dhcp enable      | ipv4 mode       |
|-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| 9d17bcf2-1eb6-4774-8565-4022d7a3ed19 | private_2001 | 172.16.255.101/24 | 172.16.255.102  | 172.16.255.103  | 172.16.255.101  | 172.16.255.100  |
| 9d17bcf2-1eb6-4774-8565-4022d7a3ed19 | private_2001 | 172.16.255.101/24 | 172.16.255.102  | 172.16.255.103  | 172.16.255.101  | 172.16.255.100  |
| 9d17bcf2-1eb6-4774-8565-4022d7a3ed19 | private_2001 | 172.16.255.101/24 | 172.16.255.102  | 172.16.255.103  | 172.16.255.101  | 172.16.255.100  |
| 9d17bcf2-1eb6-4774-8565-4022d7a3ed19 | private_2001 | 172.16.255.101/24 | 172.16.255.102  | 172.16.255.103  | 172.16.255.101  | 172.16.255.100  |
```

76
Determine which network node is managing this network:

```
# neutron dhcp-agent-list-hosting-net <network ID>
```

**Figure 85.** Example neutron net list output

<table>
<thead>
<tr>
<th>id</th>
<th>host</th>
<th>admin_state_up</th>
<th>alive</th>
</tr>
</thead>
<tbody>
<tr>
<td>a5f95eda-47e0-4409-9daa-59a9cc0ad3c</td>
<td>hp-nn1</td>
<td>True</td>
<td>:-)</td>
</tr>
</tbody>
</table>

From the example above, hp-nn1 network node is managing the network with ID 77564121-a46a-4136-8df9-79101f4e1b03.

We cannot access the network node appliance VMs via console using 'cloudadmin' to check any issues with `dnsmasq` on the network node or to try restarting the DHCP agent service. At this stage we can try restarting the network node and check whether the issue is fixed or contact HP support to further troubleshoot the issue.

**Note**

Restarting a network node might cause a slight network interruption to the active instances which belong to the networks managed by this network node. For more details refer to Role of network nodes.

9. Check Physical network connectivity between the Management Servers and compute nodes

A. Check whether the issue is only with a single instance or all the instances belonging to the same network. If the issue is with all the instances belonging to a particular network, then check whether the VLAN of the network is properly added/configured in VCM/OneView Networks and correct networks were added to the Server Profiles of the compute nodes.

B. Check whether the issue is with a single instance or all the instances that belong to the same compute node. If the issue is with all the instances running on one particular compute node, then check that the Cloud Data Trunk is correctly configured on this compute node.

C. If the Management servers and compute nodes are connected via a ToR switch, ensure the VLAN of the network is properly configured on all ToR switch interfaces of both Management servers and compute nodes.

D. If some instances are getting DHCP IP addresses and some instances are not getting DHCP IP addresses from the same network when running on the same compute node, check if teaming (ToR switches), Active/Active network configuration (VCM/OneView) and bonding (KVM/ESXi hosts) are configured correctly.

For more details on network configuration, refer to the sample network configurations Sample network configuration of KVM based environments using HP VCM, Sample network configuration of ESXi based environments using HP OneView and HP CloudSystem 8.1 Installation and Configuration Guide and HP CloudSystem 8.1 Administrator Guide from the Enterprise Information Library.

10. If the issue still persists contact HP support.

**Instances cannot be accessed from the External Network**

Instances can communicate outside the cloud via two ways:

- Legacy systems in the customer data center can connect to the instances in the cloud via a Provider Network.
- External systems can connect to the instances in the cloud via Floating IP using the External Network.
There are situations where instances can communicate with each other within the same network, but instances cannot be accessed from the External Network. To communicate with the instances from the External Network the following should be configured already:

- A virtual router needs to be created if none exists.
- Add the Private Network to the router.
- Ensure the External Network subnet is already configured (this will be done by Cloud Administrator) and configure the External Network as a gateway to the router.
- Allocate a floating IP address from the pool.
- Associate a floating IP address to the instance (which will create a NAT entry between the private and floating IP).
- Check that Security group rules are configured properly for ingress traffic.

If the above steps are done, and the instances still cannot be accessed from the External Network, follow the steps below to troubleshoot the issue further.

1. Verify that the Private Network and External Network is correctly configured:
   
   A. Check the network topology diagram. Log in to the CloudSystem Portal, click on the Network Topology under the Manage Network section. In the example shown in Figure 86, networks private_2903, private_2904 and External Network are connected to the router. Network private_2905 is not connected to the router which means that instances connected to this network cannot be accessed from the External Network.

   Figure 87. Network Topology

   B. Validate that the Private Network and External Network are configured correctly and attached to the router. From the CloudSystem Portal, click on the Routers under the Manage Network section to get the list of routers for this tenant. Then click on the router name to get the overview for that router.

   Private Networks should be added as internal interface type to the router, whereas the External Network should added as External Gateway type.
Note the IP address of the router interface for the Private Network of this router. In Figure 88 it is 10.0.1.1.

Note the IP address of the router interface for the External Network IP address for this Router. In Figure 88 it is 10.137.96.160.

**Figure 88. Router Overview**

---

**Note**

If the External Network is not added as ‘External Gateway’ type to the router, instances cannot communicate via the External Network.

---

C. Log in to the instance via the console and check whether the instance is able to ping the router interface IP address for this Private Network. In Figure 88 the router interface IP address is **10.0.1.1**. This IP address is the **gateway IP** address for the Private Network. If the instance is not able to ping the Private Network router interface IP then skip to Check whether L3 services are up and running on the network nodes.

D. If the instance is able to ping the Private Network router interface IP address (in this example it is **10.0.1.1**), then try to ping the External Network router interface IP address (in this example it is **10.137.96.160**). If we are not able to ping the External Network router interface IP then skip to Check whether L3 services are up and running on the network nodes.

E. If the instance is able to ping both the interfaces on the router, then find the Gateway IP address of the External Network. Log in to the CloudSystem Portal, click on Networks under the Manage Network section to get the list of networks for this tenant. Then click on the External Network name to get the overview for that network. Find the Gateway IP address under the subnets section. In this example, shown in Figure 89, the Gateway IP of the External Network is **10.137.96.1**.

**Figure 90. Network Overview**
F. From the instance console, ping the External Network gateway IP address (in this example it is 10.137.96.1). If we are not able to ping the external gateway then there might be a configuration or communication problem between the Management server and the External Network gateway, skip to the Check the network configuration between the Management Servers and External Network section for further troubleshooting.

G. If we are able to ping the External Network gateway IP address then outbound communication from the instance is working fine and we have an issue with the inbound connection (i.e., from the External Network to the instance). Check that proper security group rules are configured and assigned to this instance.

H. If security groups are configured properly then the issue might be related to external routing or firewall issues outside the cloud environment. Work with the network administrator to address the issue.

2. Check whether L3 services are up and running on the network nodes.

   Log in to the CloudSystem Portal, Click on the Admin tab, click on System Info tab, and then click on Network Agents. Check the State of the L3 agents on all the 3 network nodes.

   ![Network Agents Status](image)

   If the state of the L3 agent shows 'Up' then the agent is up and running, otherwise the agent is not running and there may be a problem associated with that agent. If all three network nodes L3 agent states are not 'Up' then instances cannot be accessed via the External Network.

   The network node appliance VMs are not accessible via the console using the 'cloudadmin' to check any issues with the L3 agent on the network node or to try restarting the L3 agent service. At this stage we can try restarting the network node and check whether the issue is fixed or contact HP support to further troubleshoot the issue.

   **Note**
   Restarting a network node might cause a slight network interruption to the active instances which belongs to the networks managed by this network node. For more details refer to Role of network nodes.

3. Check the network configuration between the Management Servers and External Network:

   A. Check whether the External Network is configured properly on the Management servers.
      - In the KVM environment Ethernet (when configured in separate trunk) or VLAN configuration (when combined in the management trunk)
      - In the ESXi environment vSwitch (when configured in separate trunk) or port group configuration (when combined in the management trunk)

   B. When the External Network is configured in the Management Trunk, ensure the VLAN is properly configured on the ToR switches.
C. If some instances are able to communicate and some instances are not able to communicate from the External Network within the same network, check that teaming (ToR switches), Active/Active network configuration (VCM/OneView) and bonding (KVM/ESXi hosts) are configured correctly.

D. Check any external routing or firewall configurations that may be preventing access to deployed instances from External Network.

E. If the issue still persists contact HP support.

For more details on network configuration, refer to the sample network configurations Sample network configuration of KVM based environments using HP VCM, Sample network configuration of ESXi based environments using HP OneView and HP CloudSystem 8.1 Installation and Configuration Guide and HP CloudSystem 8.1 Administrator Guide from the Enterprise Information Library.

**Appendix**

**Enabling appliance console access**

CloudSystem appliance VMs do not have SSH access enabled and console access to the appliances is disabled by default.

To enable console access on the CloudSystem appliance VMs

1. On a Windows or Linux system where csadmin is run, open a command shell.

2. Set the password for the 'cloudadmin' user for the appliance VM:
   
   ```
   csadmin console-users set-password --vm-name <name of VM> --password <Password> --os-username <CloudSystem_Console_Username> --os-password <CloudSystem_Console_Password> --os-auth-url <CloudSystem_Appliance_IP_Address>:5000/v2.0 --insecure
   ```

3. Enable the console access for the appliance VM:
   
   ```
   csadmin console-users enable --vm-name <name of VM> --os-username <CloudSystem_Console_Username> --os-password <CloudSystem_Console_Password> --os-auth-url <CloudSystem_Appliance_IP_Address>:5000/v2.0 --insecure
   ```

**Note**

We can enable the console access only for Foundation, Enterprise and vCenter-proxy appliance VMs.

For additional information on enabling console access and supported console operations for the cloudadmin user refer to the HP CloudSystem 8.1 Installation and Configuration Guide and HP CloudSystem 8.1 Administrator Guide from the Enterprise Information Library.

**Logging in to the appliance consoles**

After the console is enabled for a given appliance and you have access to the appliance console, you can log in to the appliance by specifying the cloudadmin user name and the password set in the csadmin console-users set-password command. Make sure you have set a password for the appliance you are trying to access.

**ESXi Management Cluster**

1. Log in to vCenter and select the appliance VM. Right-click on the appliance VM and select the 'open console' option.

2. Access the appliance console login screen that you enabled in Enabling appliance console access by pressing Alt-Ctl-F1.

3. Log in to the appliance console with the following credentials:
   
   - **User name:** cloudadmin
   - **Password:** <Password> that you set for the appliance in Enabling appliance console access.
**KVM Management Cluster**

From KVM Management server via CLI:

1. Log in to the KVM Management Server.
2. Run `virsh console <appliance VM name>` and connect to the console of the appliance, then press Enter and you will get the login prompt.
3. Log in to the appliance console with the following credentials:
   - User name: `cloudadmin`
   - Password: `<Password>` that you set for the appliance in Enabling appliance console access
4. To exit from the console, press Ctrl+] 

For more information on how to log in to appliance consoles refer to the *HP CloudSystem 8.1 Installation and Configuration Guide* and *HP CloudSystem 8.1 Administrator Guide* from the Enterprise Information Library.

**Sourcing environment variables**

We can source the environment variables required to work with OpenStack commands from the Foundation appliance VM console.

```bash
export OS_USERNAME=administrator
export OS_PASSWORD=<appliance password>
export OS_TENANT_NAME=administrator
export OS_AUTH_URL=http://127.0.0.1:5000/v2.0
export NOVA_ENDPOINT_TYPE=internalURL
export OS_REGION_NAME=public
export OS_ENDPOINT_TYPE=internalURL
```

**Note**

The above environment variables can only be used when logged into the Foundation appliance VM via the console.
For more information

See [hp.com/go/cloudsystem/docs](http://hp.com/go/cloudsystem/docs) for CloudSystem user documentation and technical white papers.

See [hp.com/go/oneview](http://hp.com/go/oneview) for details on HP OneView.

See [vmware.com](http://vmware.com) for more information on the VMware.

See [hp.com/go/vc/manuals](http://hp.com/go/vc/manuals) for more information on Virtual Connect.

See [redhat.com/products/enterprise-linux](http://redhat.com/products/enterprise-linux) for more information on Red Hat Enterprise Linux.

See [docs.openstack.org](http://docs.openstack.org) for more details on OpenStack.

To help us improve our documents, please provide feedback at [hp.com/solutions/feedback](http://hp.com/solutions/feedback).