SDN v praxi overlay sítí pro OpenStack

5.10.2015

Daniel Prchal
daniel.prchal@hpe.com

Agenda

- OpenStack
- OpenStack Architecture
- SDN – Software Defined Networking
- OpenStack Networking
- HP Helion OpenStack
- HP Helion CloudSystem

OpenStack – WTF ?

Open source software for creating private and public clouds.

What is OpenStack?
OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface.

Openstack distributions:
http://www.openstack.org/marketplace/distros/
Openstack drivers:
http://www.openstack.org/marketplace/drivers/
Openstack public clouds:
http://www.openstack.org/marketplace/public-clouds/

EurOpen

OpenStack – Public Clouds

openstack™
CLOUD SOFTWARE

Using a cloud

There are OpenStack powered public clouds all over the world. Explore the possibilities.

hp
rackspace
the #1 managed cloud company
ULTIMUM TECHNOLOGIES
DreamHost
Enter Cloud Suite
DataCentred
VEXXHOST
Dualtec Cloud Builders
ELASTX

EurOpen

OpenStack – Contributors

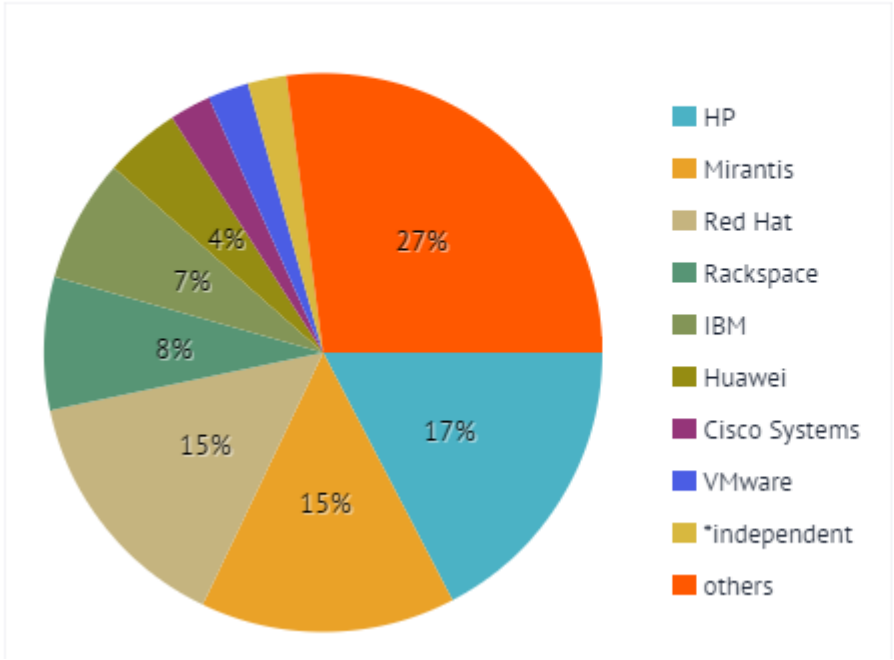
STACKALYTICS

http://stackalytics.com

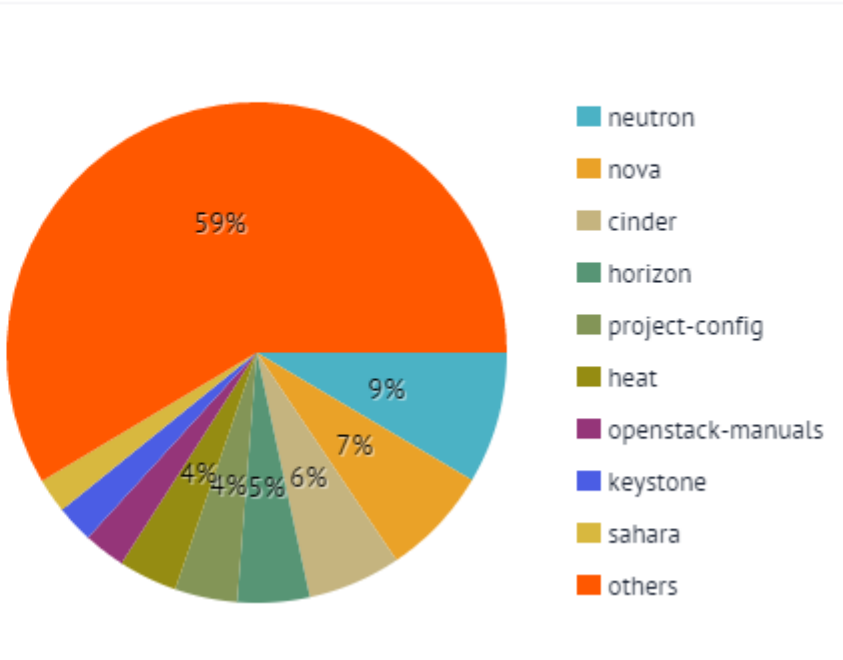
Release: Liberty | Project Type: OpenStack | Module: Any module | Company: Any company | Contributor: Any contributor | Metric: Reviews

Last updated on 01 Oct 2015 09:45:11 UTC

Contribution by companies



Contribution by modules



EurOpen

OpenStack – Contributors

STACKALYTICS

http://stackalytics.com

Last updated on 01 Oct 2015 09:45:11 UTC

Release	Project Type	Module	Company	Contributor	Metric
Liberty	OpenStack	*Any module*	*Any company*	*Any contributor*	Reviews

#	Company	Reviews
1	HP	28693
2	Mirantis	24455
3	Red Hat	24137
4	Rackspace	12736
5	IBM	11806
6	Huawei	7263
7	Cisco Systems	3952
8	VMware	3916
	*independent	3714
9	Intel	3676

Showing 1 to 10 of 158 entries

#	Module	Reviews
1	neutron	14082
2	nova	11679
3	cinder	9982
4	horizon	7710
5	project-config	6682
6	heat	6294
7	openstack-manuals	4451
8	keystone	4004
9	sahara	3691
10	kolla	3594

Showing 1 to 10 of 404 entries

EurOpen

OpenStack – WTF ?

Open Source

Cloud Operating System

Many Contributors

All major vendors are producing OpenStack drivers

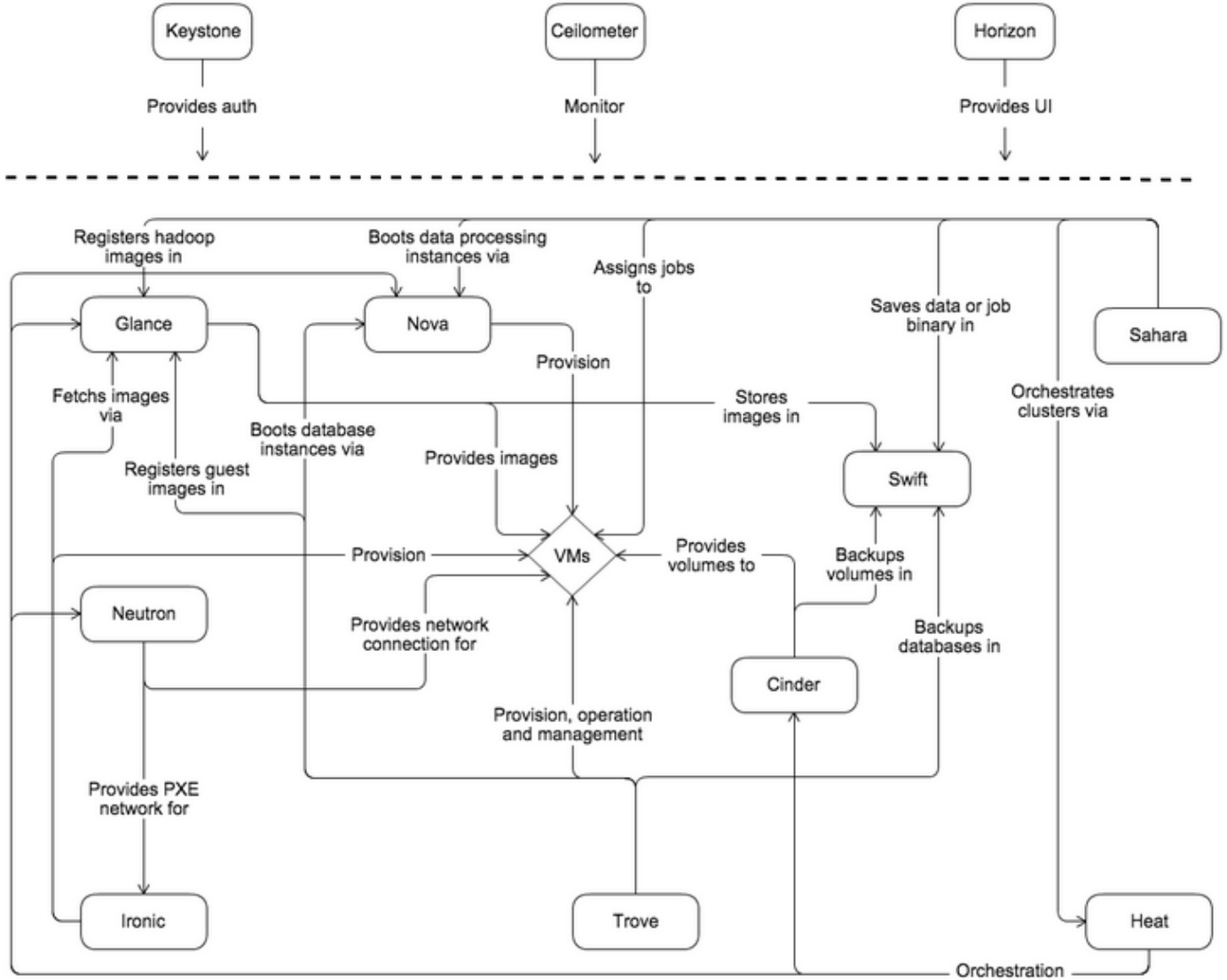
Managed through a GUI, CLI or API

Simple Integration

EurOpen

Architecture

OpenStack – Conceptual Architecture

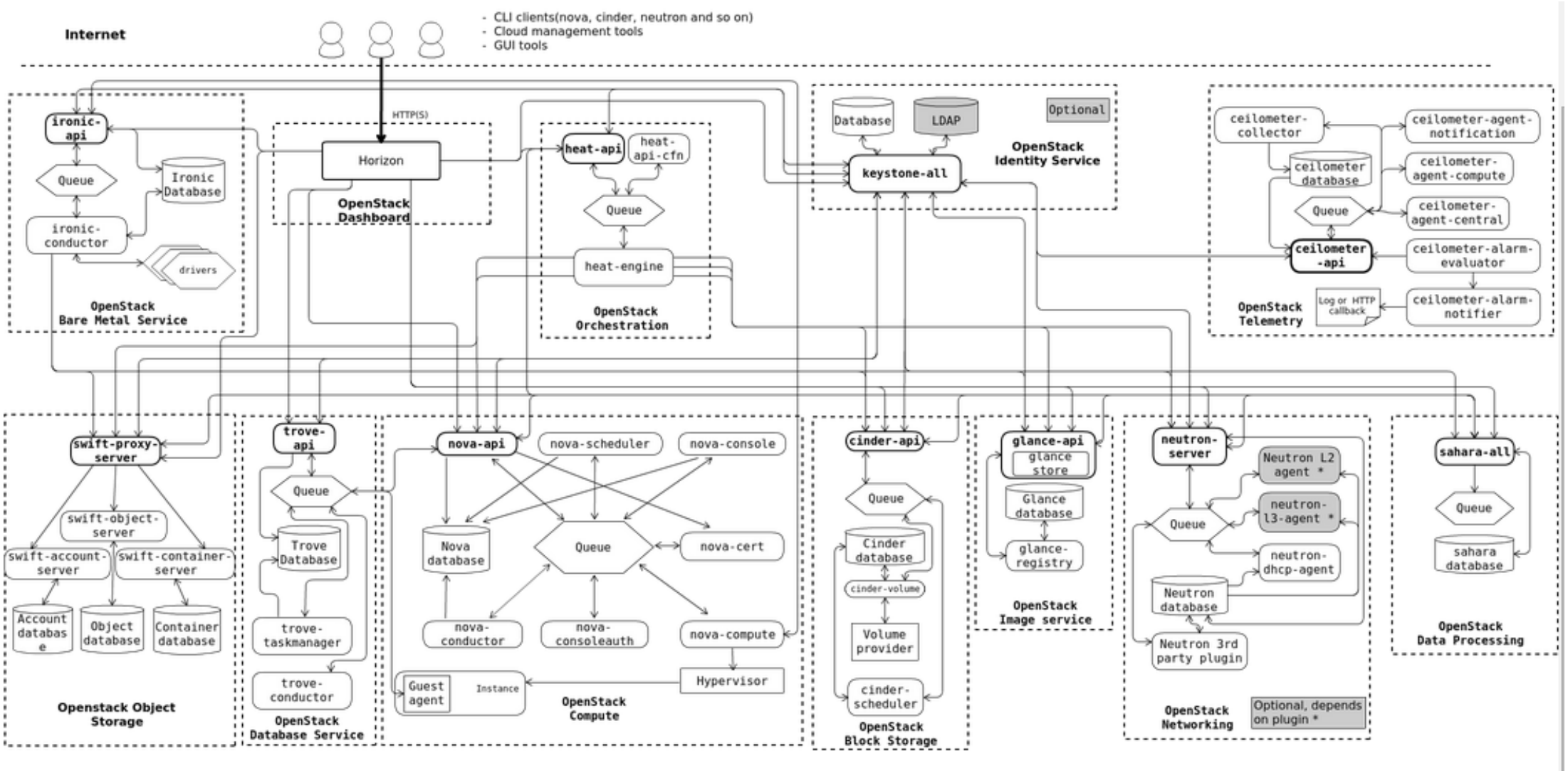


Keystone – Authorization
Horizon – User Interface
Ceilometer – Monitor

Glance – Image service
Nova – Compute
Swift – Object Storage
Cinder – Block Storage
Neutron – Networking

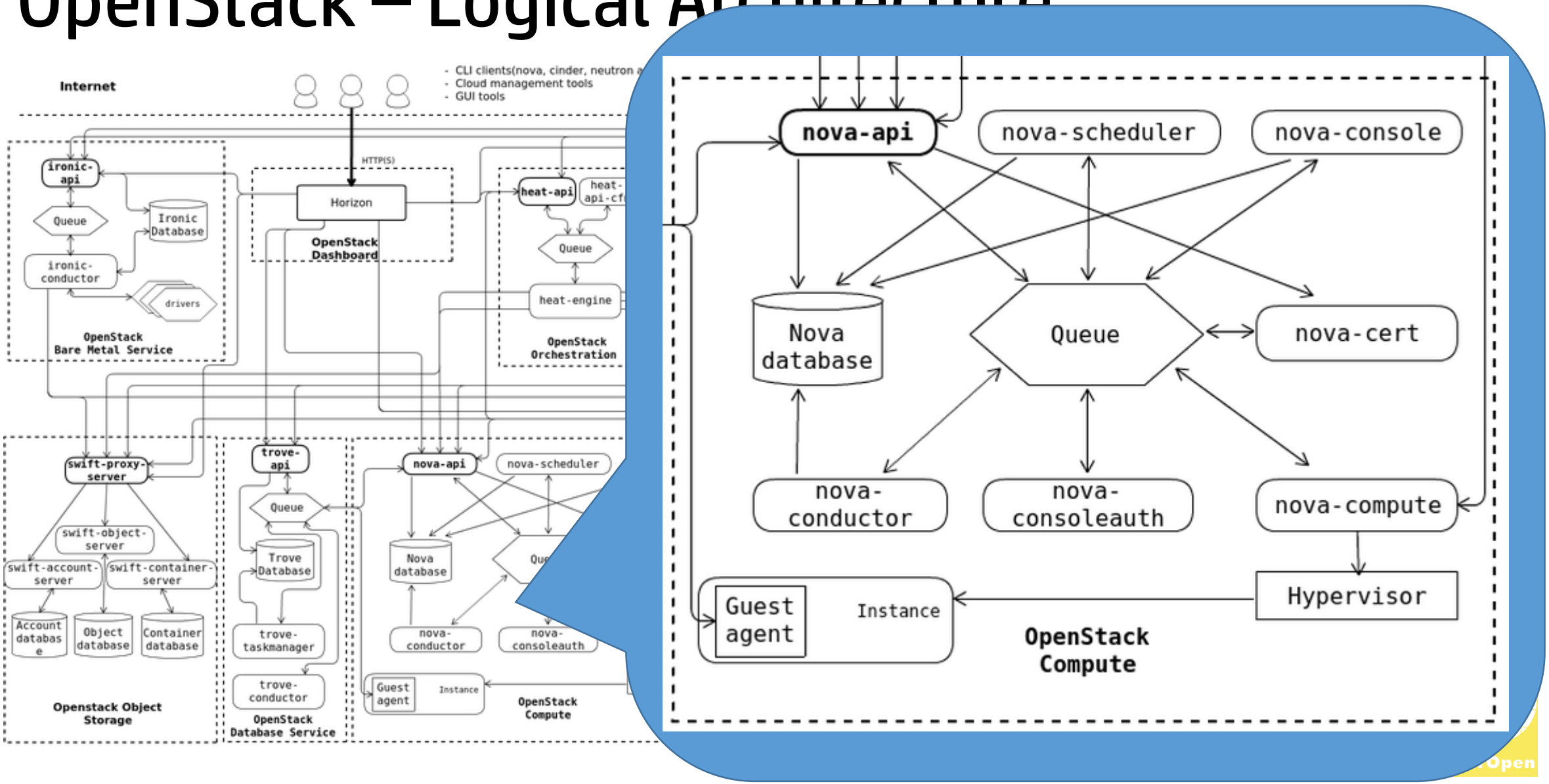
Ironic – Deployment
Trove – Database
Heat – Stack orchestration
Sahara – Data-intensive application cluster

OpenStack – Logical Architecture

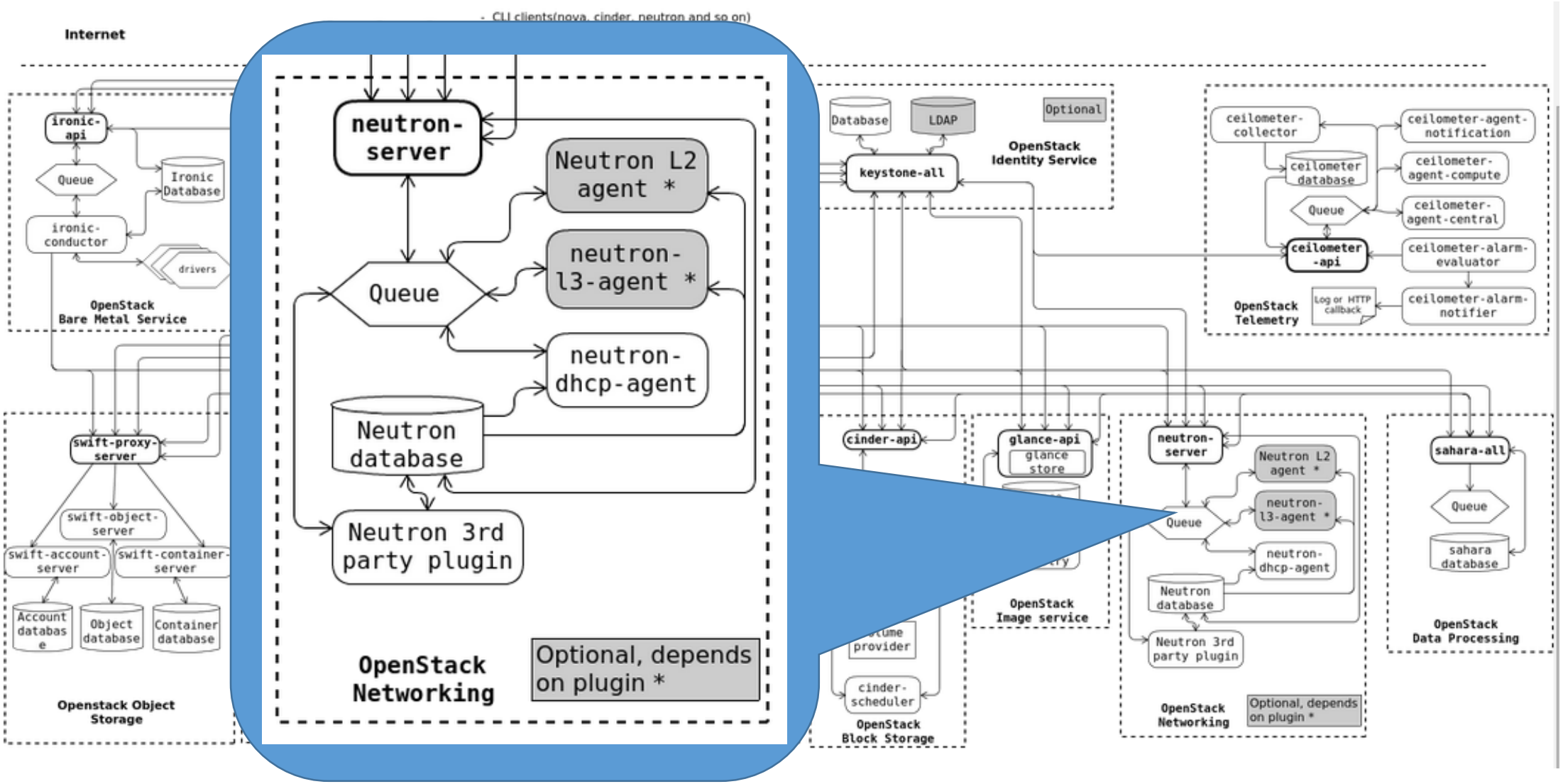


EurOpen

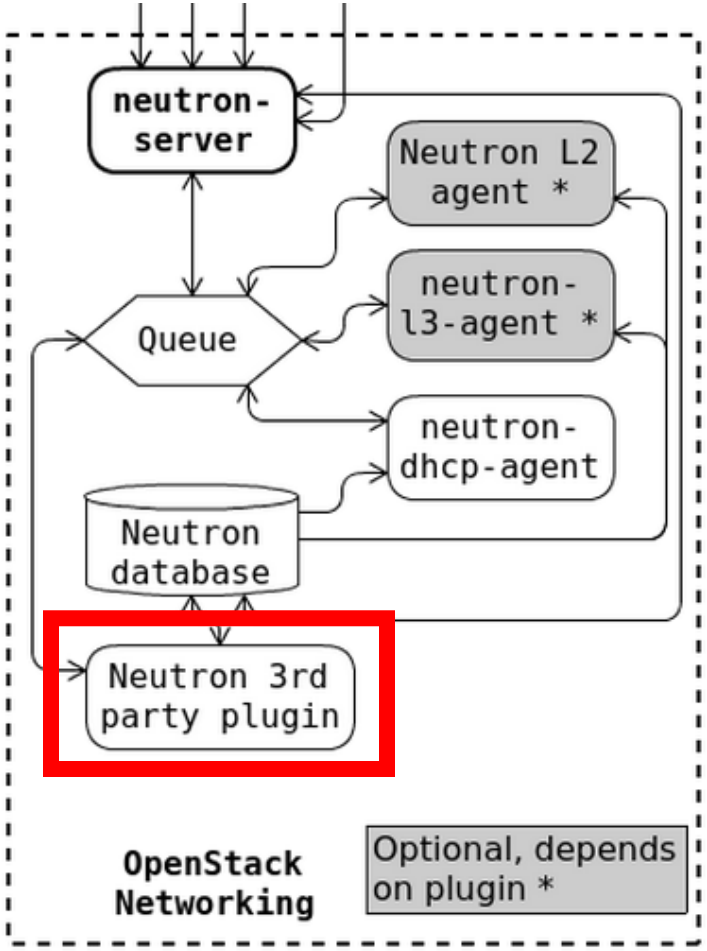
OpenStack – Logical Architecture



OpenStack – Logical Architecture



OpenStack – Neutron



The OpenStack Networking service provides an API that allows users to set up and define network connectivity and addressing in the cloud.

Plugins can extend networking functionality.

OpenStack – Neutron plugins

- LBaaS

  The Load-Balancer-as-a-Service (LBaaS) API provisions and configures load balancers. The reference implementation is based on the HAProxy software load balancer.

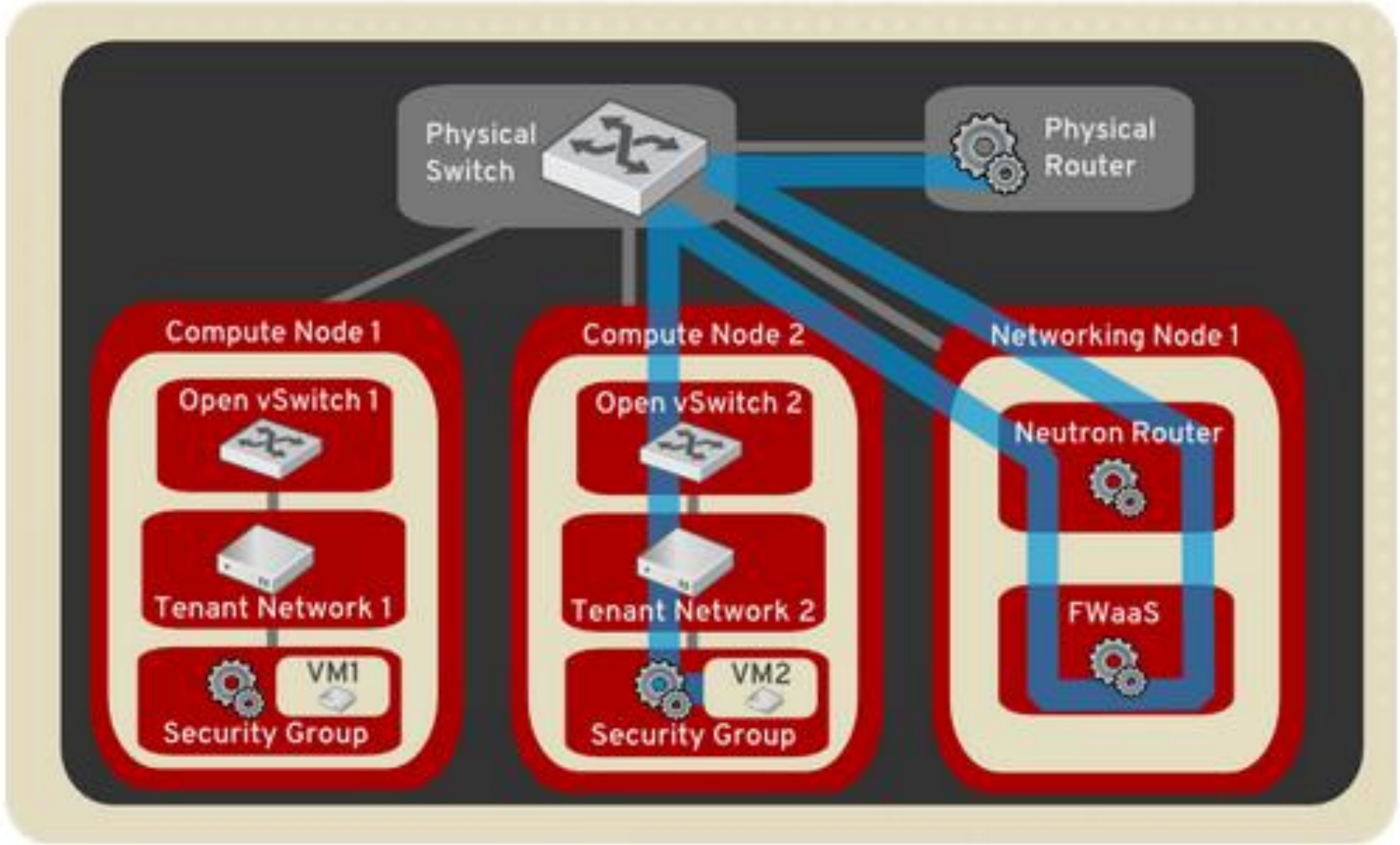
- FWaaS

  The Firewall-as-a-Service (FWaaS) API is an experimental API that enables early adopters and vendors to test their networking implementations.

- VPNaaS

  The Virtual Private Network as a Service (VPNaaS) is a neutron extension that introduces the VPN feature set.

OpenStack – Neutron plugins



SDN – Software Defined Networking

EurOpen

SDN

Definition from the Open Network Foundation:

... In the SDN architecture, the **control** and **data planes** are **decoupled**, network **intelligence** and state are logically **centralized**, and the underlying network **infrastructure is abstracted from the applications**. As a result, enterprises and carriers gain unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs. ...

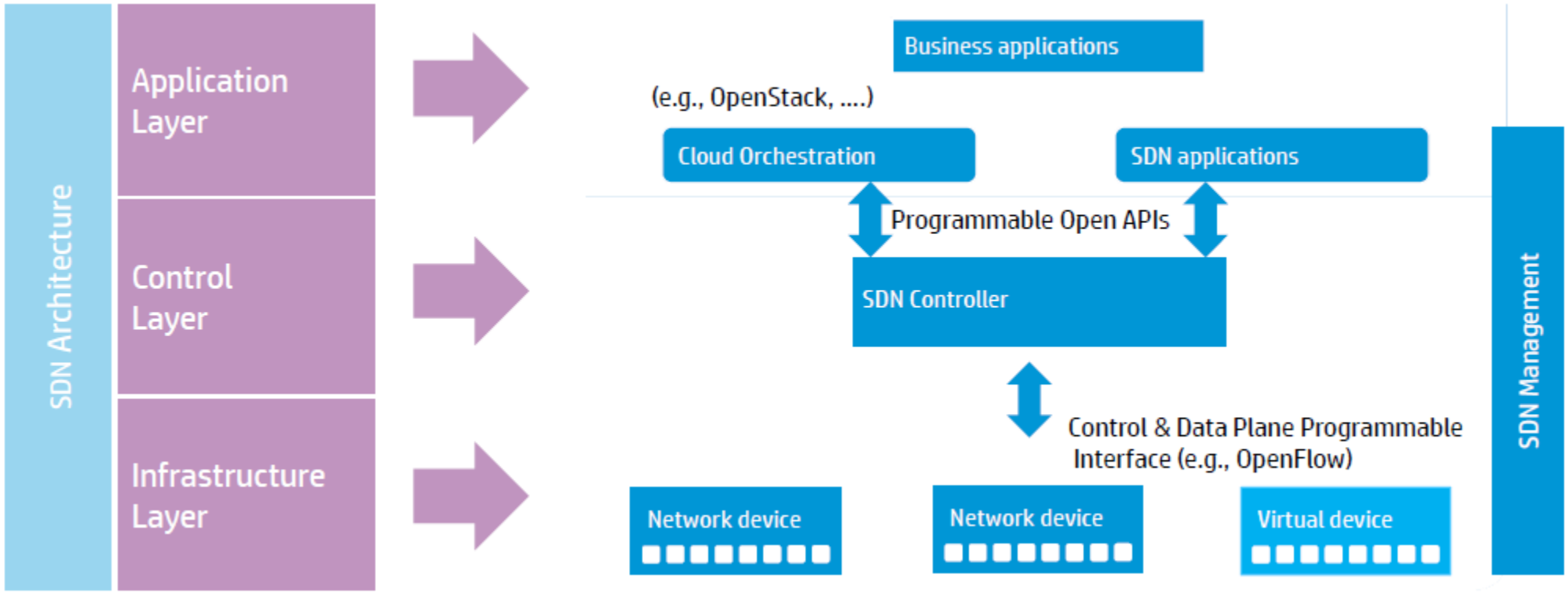
Source:

https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

EurOpen

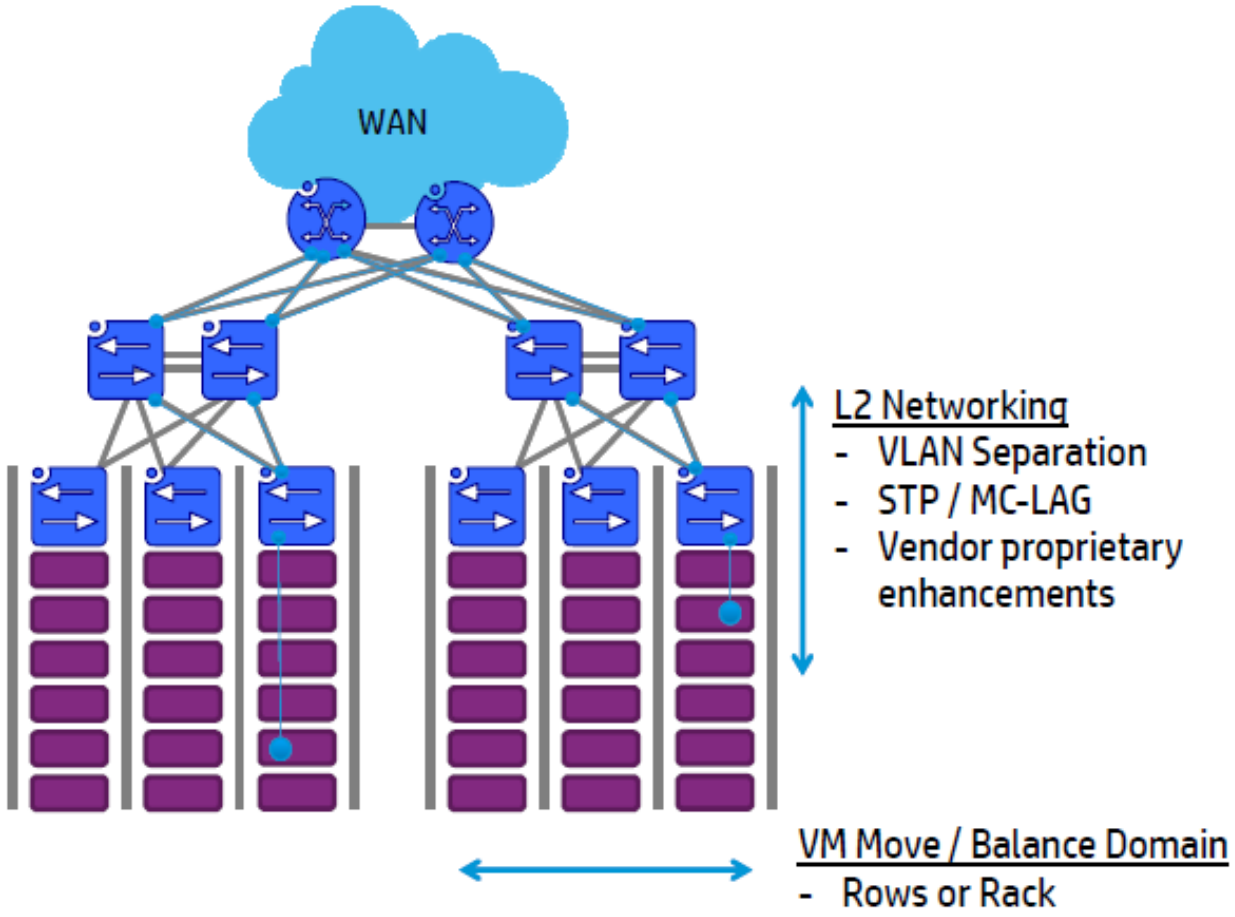
SDN - Architecture

Ability to Apply Business Logic to Network Behavior in Dynamic Fashion



SDN

Challenges with traditional 3 Tier datacenter design



Challenges:

- MAC Address Explosion
- **VLAN ID Limitations**
- Subnet alignment with L2 domains

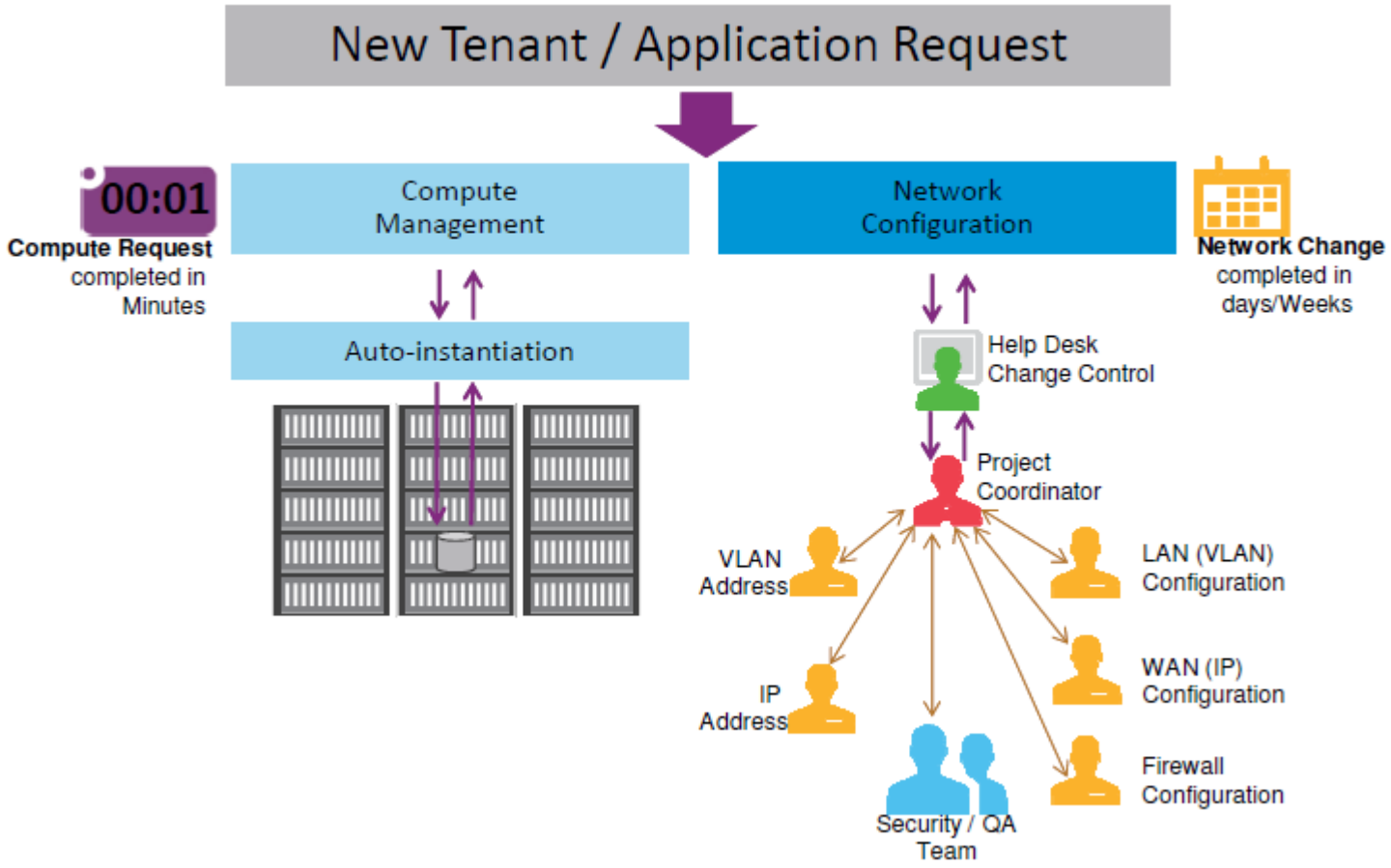
Results in:

- Asset isolation
- Scaling bounded by platform density
- Complex provisioning / mobility of endpoints
- Vendor lock-in
- Constrained growth / moves within a POD

EurOpen

SDN

Challenges with traditional 3 Tier datacenter design



Compute is Virtualized

- Available in Minutes !!!

Network is Partially Virtualized

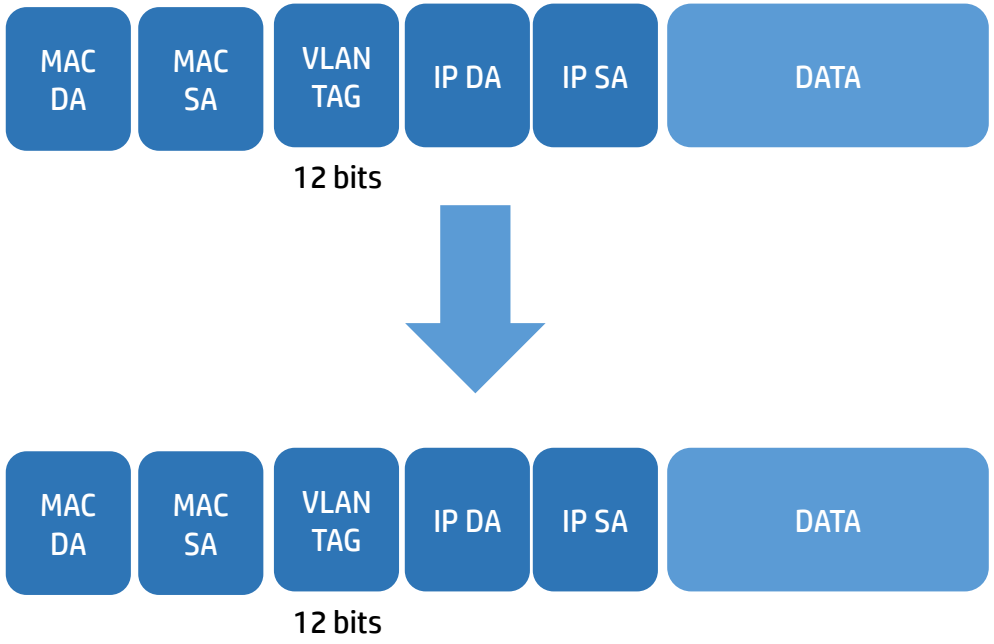
- Configuration takes Days/Weeks

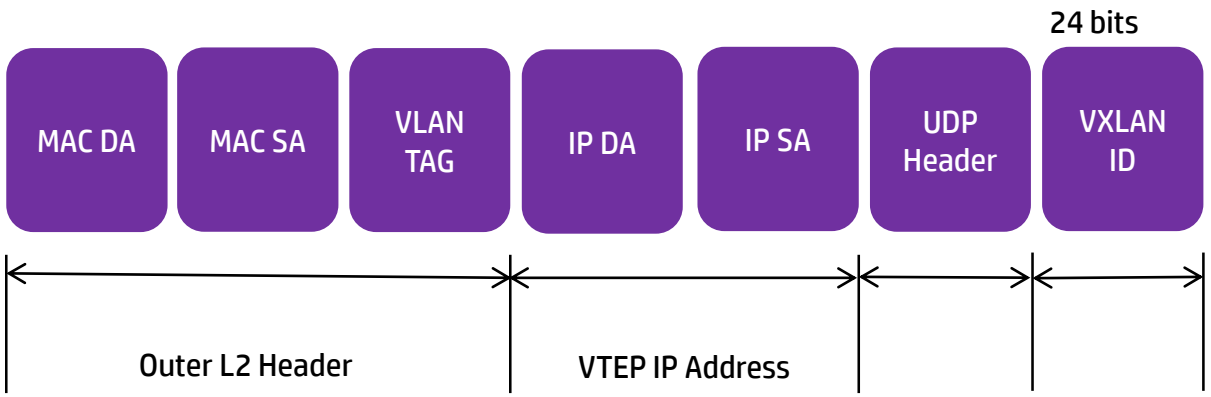
EurOpen

VXLAN - Virtual eXtensible Local Area Network

VLAN

- Ideal for private cloud scale (up to 4k subnet)
- Uses L2 fabric underlay
- Universally supported technology





VXLAN

- Ideal for public cloud scale (up to 16M subnet)
- Uses L3 fabric underlay

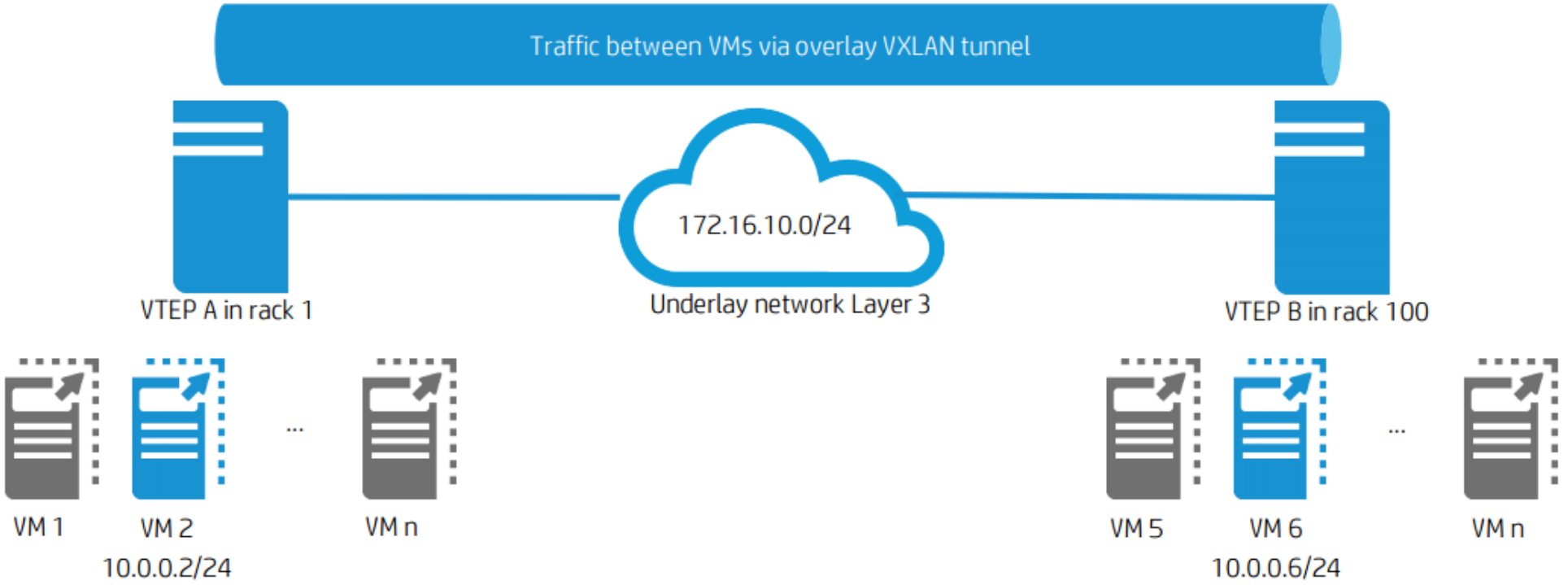
EurOpen

VXLAN - Virtual eXtensible Local Area Network

VXLAN benefits

1. Enables VMs to be deployed on any physical hypervisor within the DC

2. Provides Layer 2 connectivity between VMs even though underlay network is L3

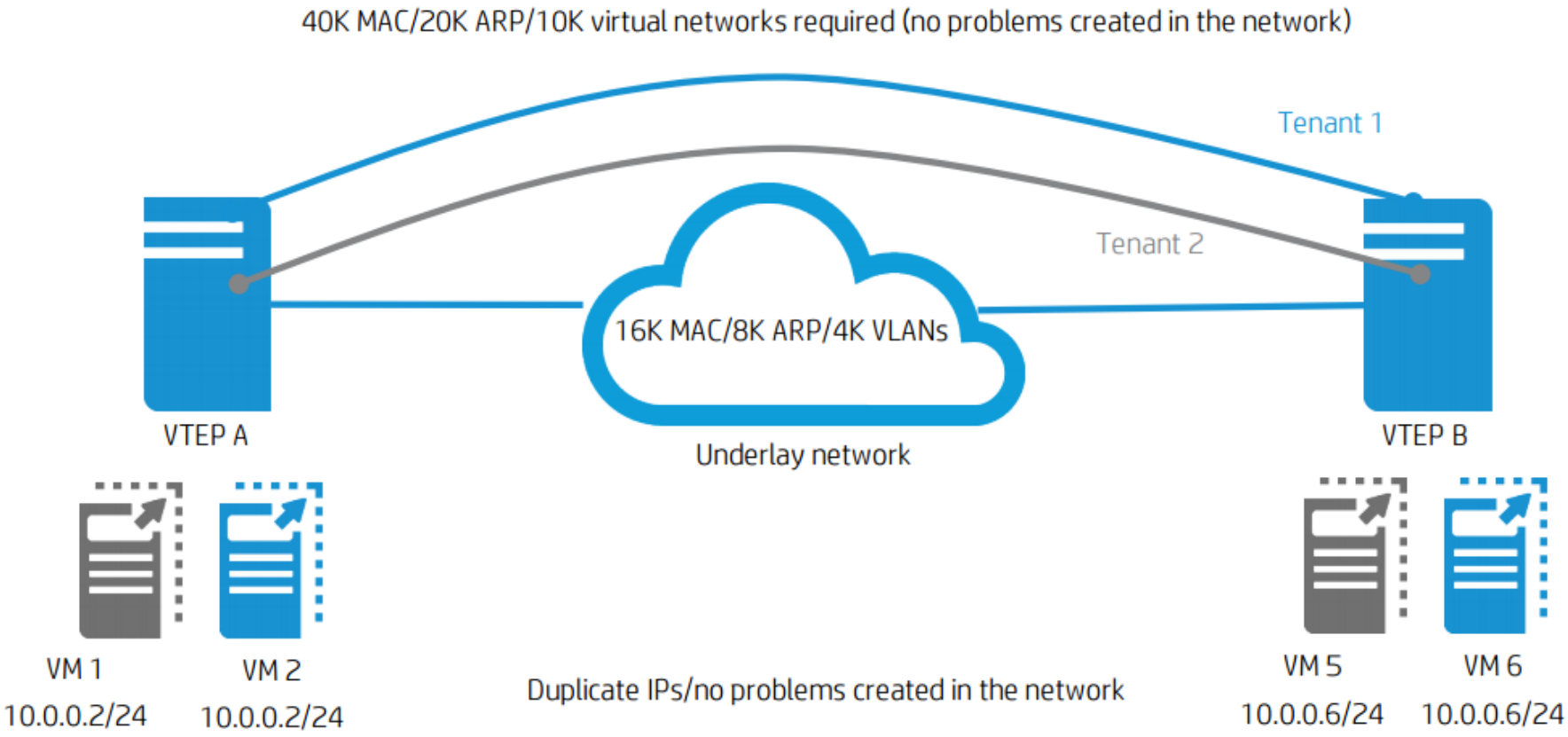


VXLAN - Virtual eXtensible Local Area Network

VXLAN benefits

3. Overcomes MAC/ARP table and VLAN scalability limitations of the physical underlay network

4. Enables multitenant networks with duplicate Ips

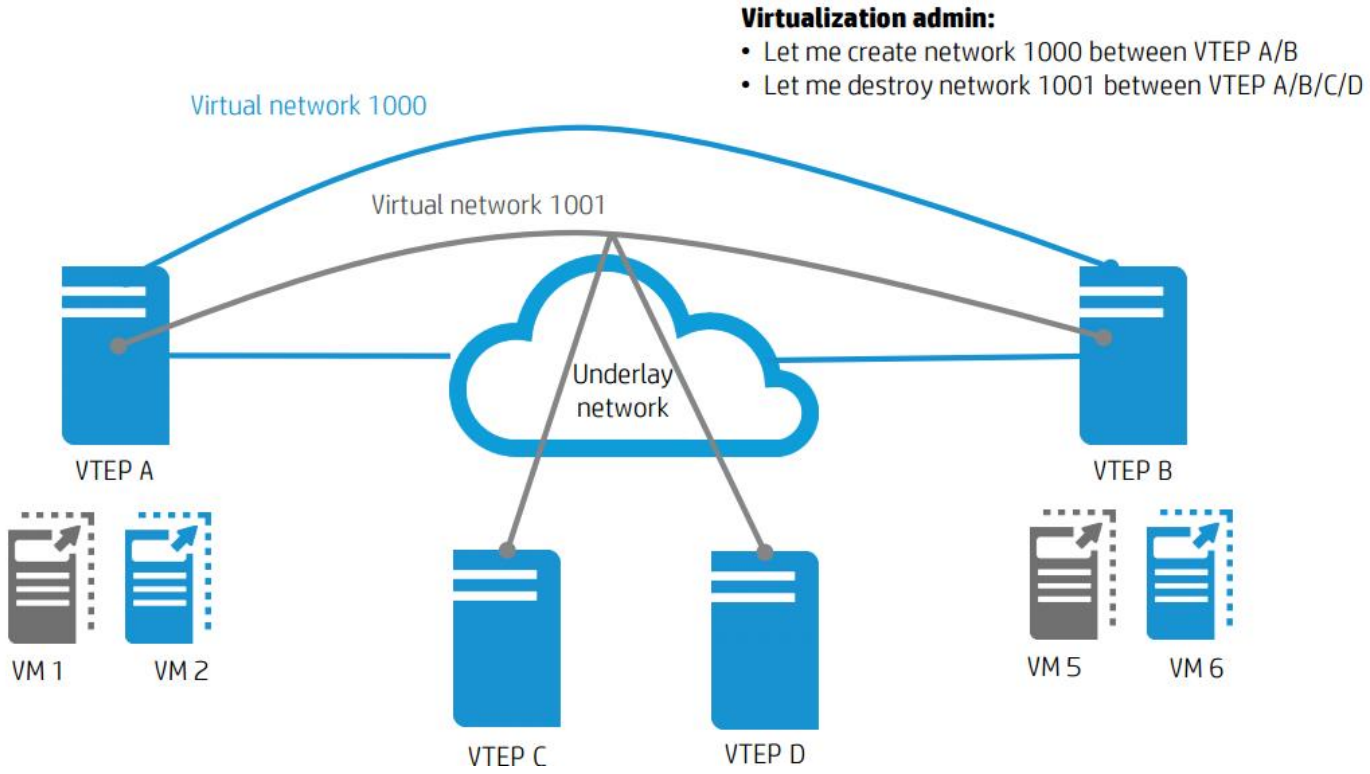


VXLAN - Virtual eXtensible Local Area Network

VXLAN benefits

5. Allows the virtualization admin to self-provision their required networks without waiting for the network admin

6. Increases the speed and agility of deploying virtual networks. Manual Command Line Interface (CLI) is not required and devices in the path do not need to be provisioned, providing for easier network automation using exposed application programming interface (APIs)

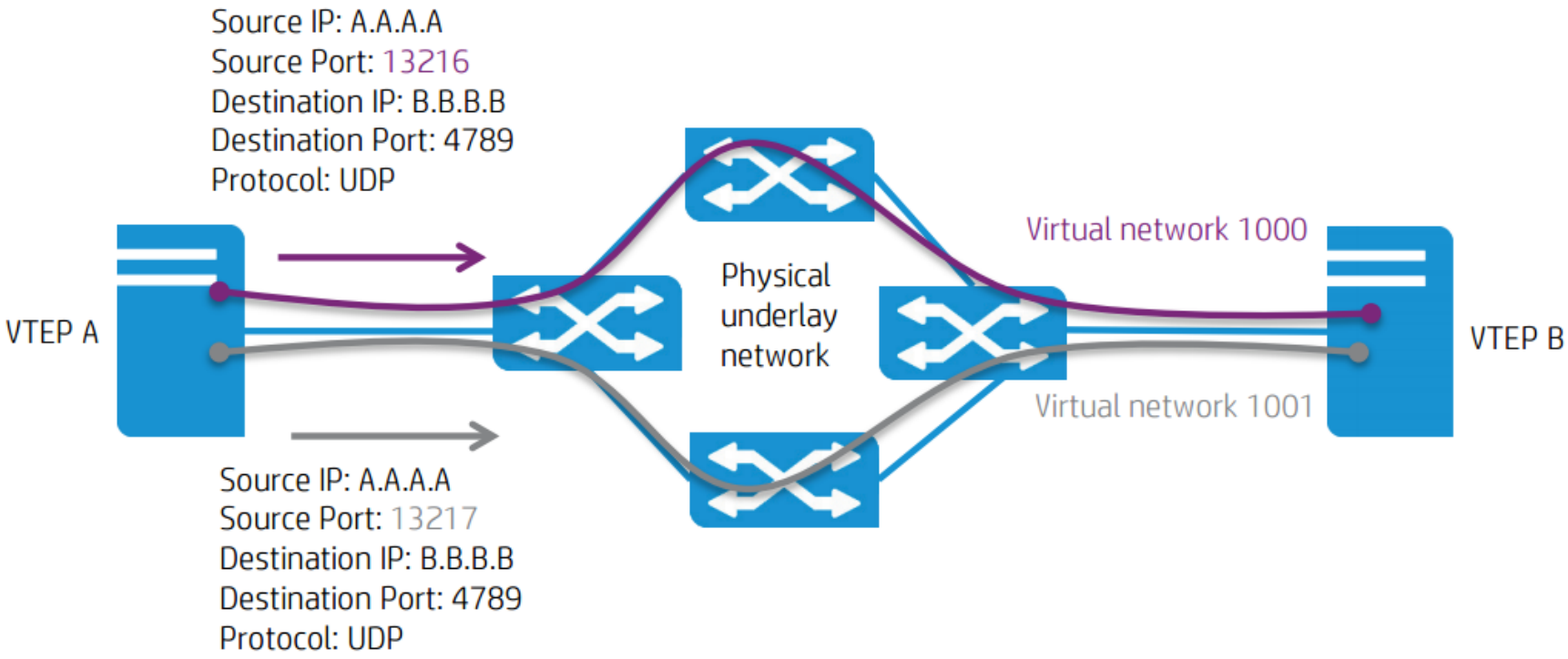


VXLAN - Virtual eXtensible Local Area Network

VXLAN benefits

7. Allows physical underlay network to load share tunneled traffic based on 5 tuple connection info

- Source IP address/port number
- Destination IP address/port number
- Protocol (UDP)



EurOpen

OpenStack - Networking

EurOpen

OpenStack - Networking

- Tenant networks
  - Created by user
  - Provide connectivity between instances in a tenant
  - A lot of different network types are used
    - Local
      - Isolated network from other instances and nodes. Instances connected to same local network can communicated with other instances on same compute node
      - Mostly only used for testing purposes
    - Flat
    - VLAN
    - VXLAN and GRE
      - Can be used with Open vSwitch to create overlay networks
      - Use peer to peer tunnels to create mesh network
- Provider networks
  - Created by OpenStack administrator
  - Mapped directly to physical network in datacenter
  - Most useful network types:
    - Flat (untagged)
    - VLAN (802.1q tagged)
    - VXLAN (vxlan support on physical switches)
- External Network
  - Created by OpenStack administrator
  - Mapped directly to physical network in datacenter
  - Used for External communication to internet
  - Floating IP can be assigned from this network

OpenStack – Networking components

- **Subnets**
  A block of IP addresses and associated configuration state. This is also known as the native IPAM (IP Address Management) provided by the networking service for both tenant and provider networks. Subnets are used to allocate IP addresses when new ports are created on a network.

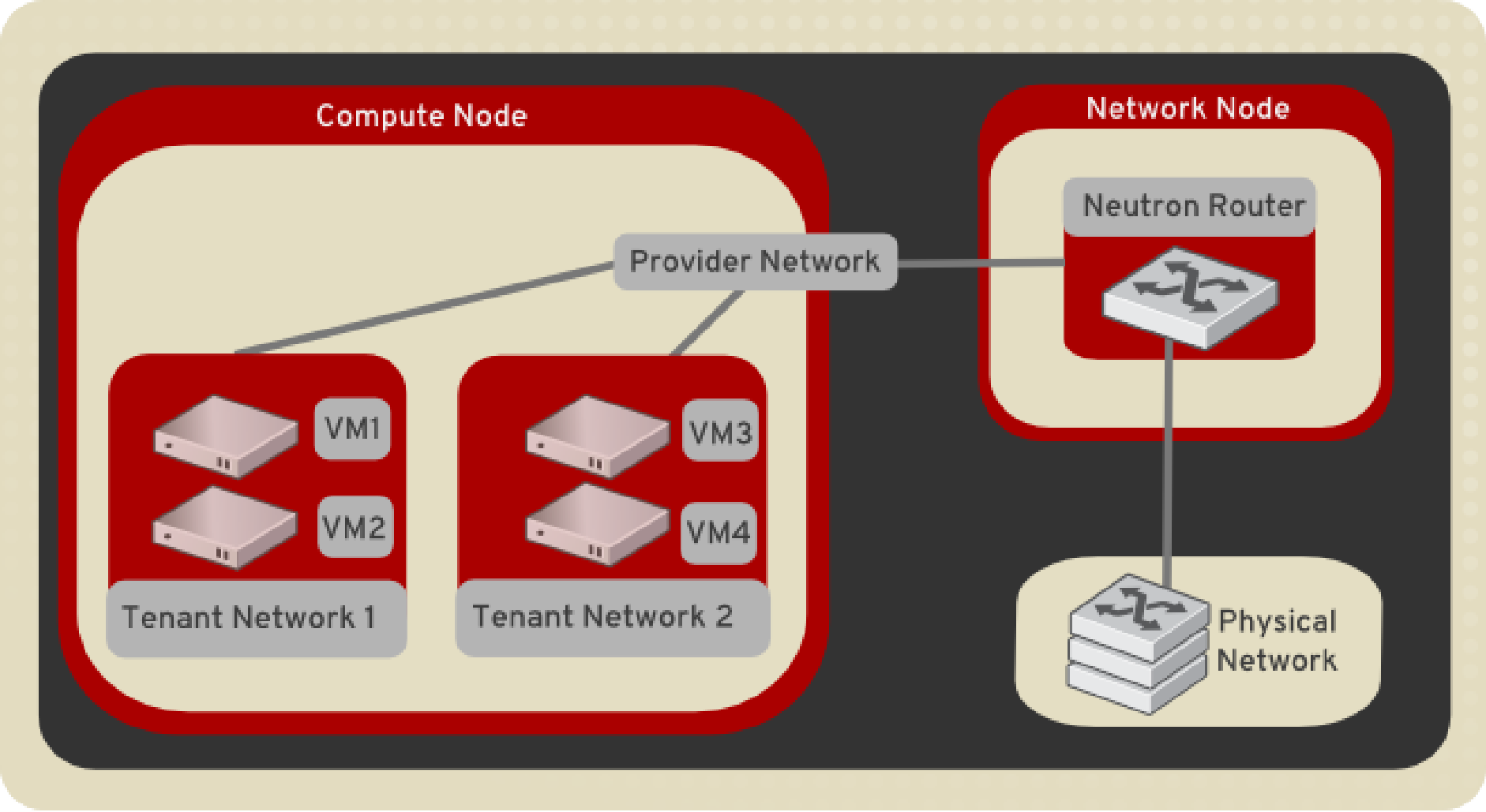
- **Ports**
  A port is a connection point for attaching a single device, such as the NIC of a virtual server, to a virtual network. Also describes the associated network configuration, such as the MAC and IP addresses to be used on that port.

- **Routers**
  This is a logical component that forwards data packets between networks. It also provides L3 and NAT forwarding to provide external network access for VMs on tenant networks. Required by certain plug-ins only.

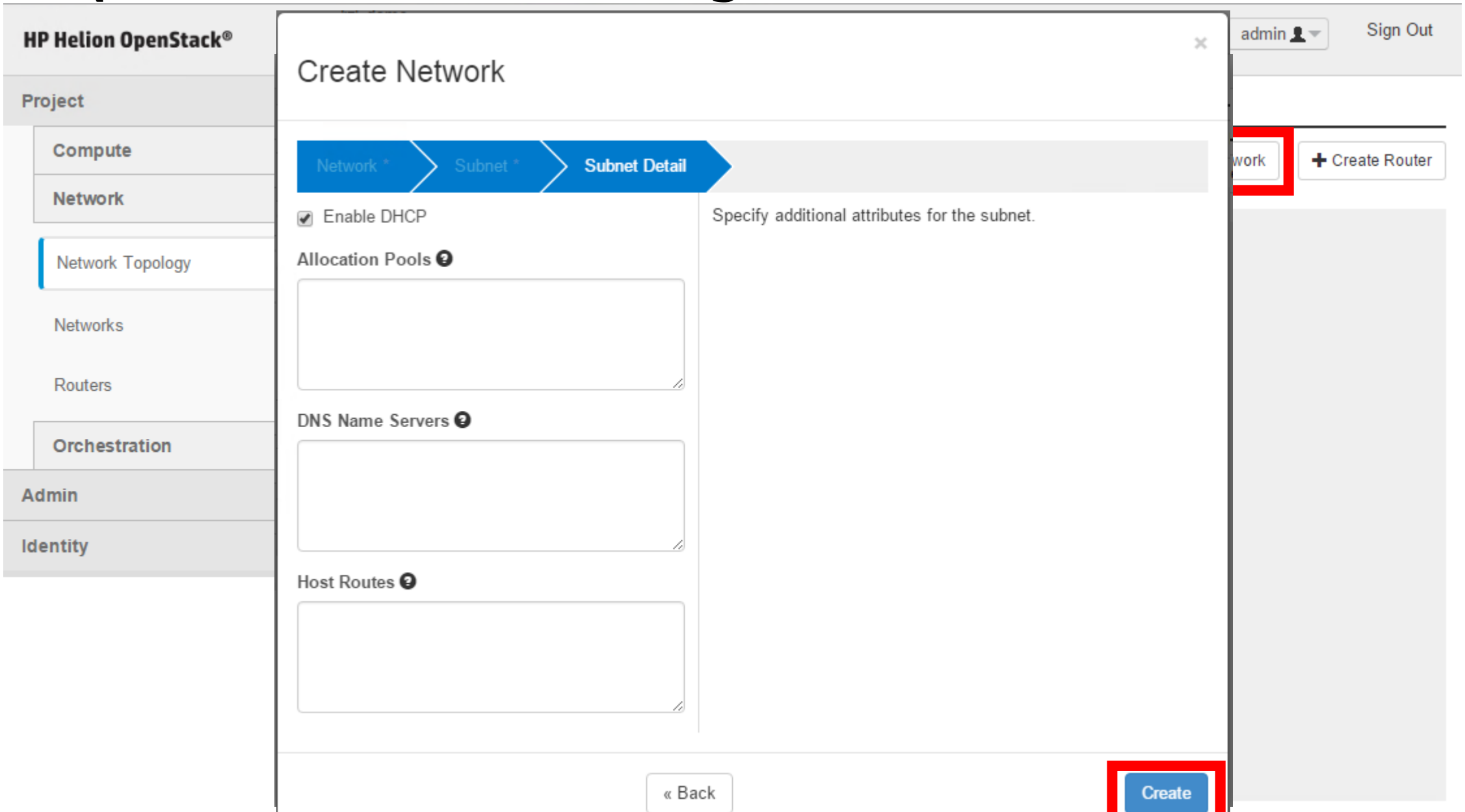
- **Security Groups**
  A security group acts as a virtual firewall for your compute instances to control inbound and outbound traffic. Security groups act at the port level, not the subnet level. Therefore, each port in a subnet could be assigned to a different set of security groups

- **Extensions**
  The OpenStack networking service is extensible. Extensions serve two purposes: they allow the introduction of new features in the API without requiring a version change and they allow the introduction of vendor specific niche functionality.

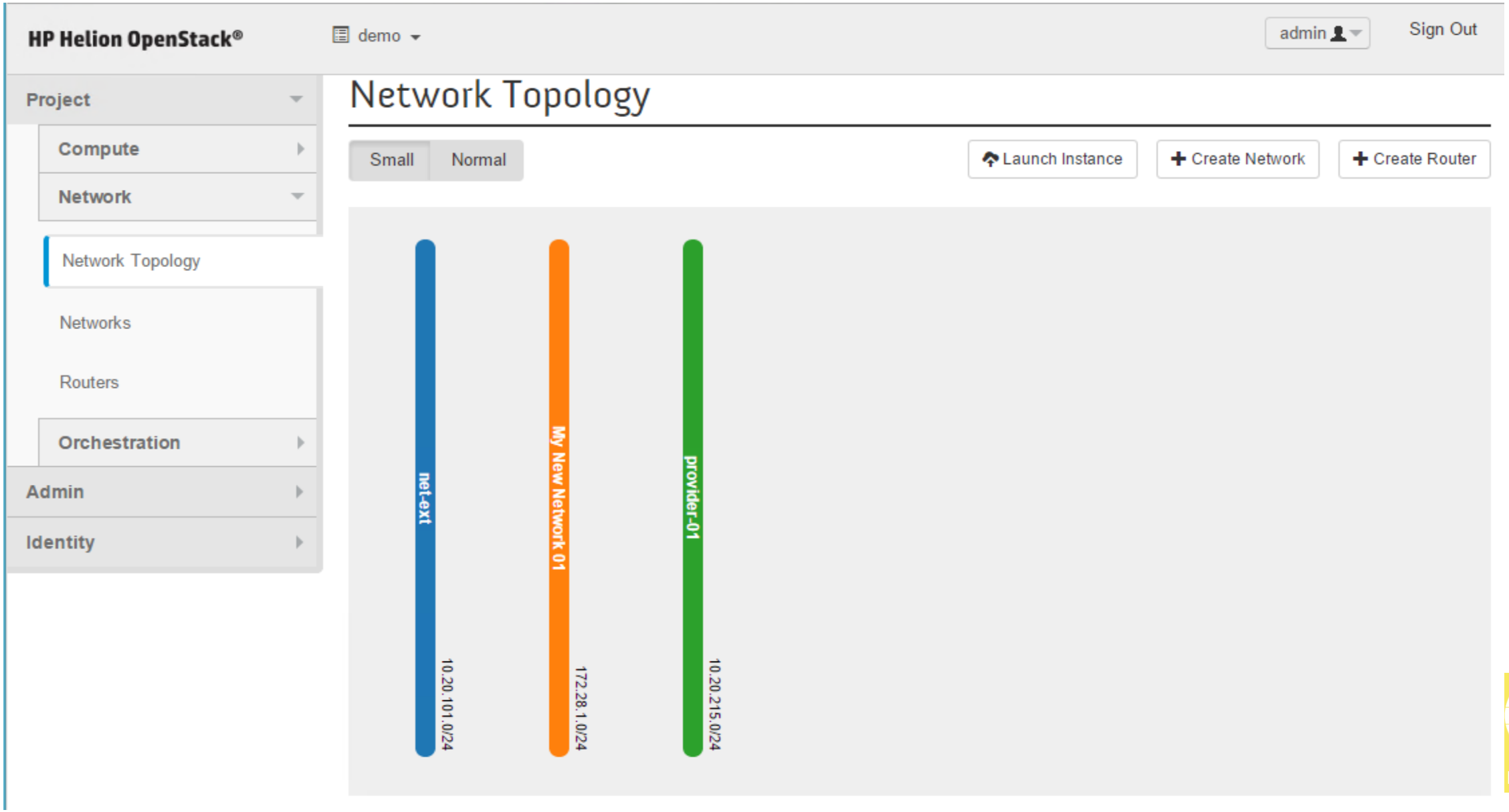
OpenStack - Networking



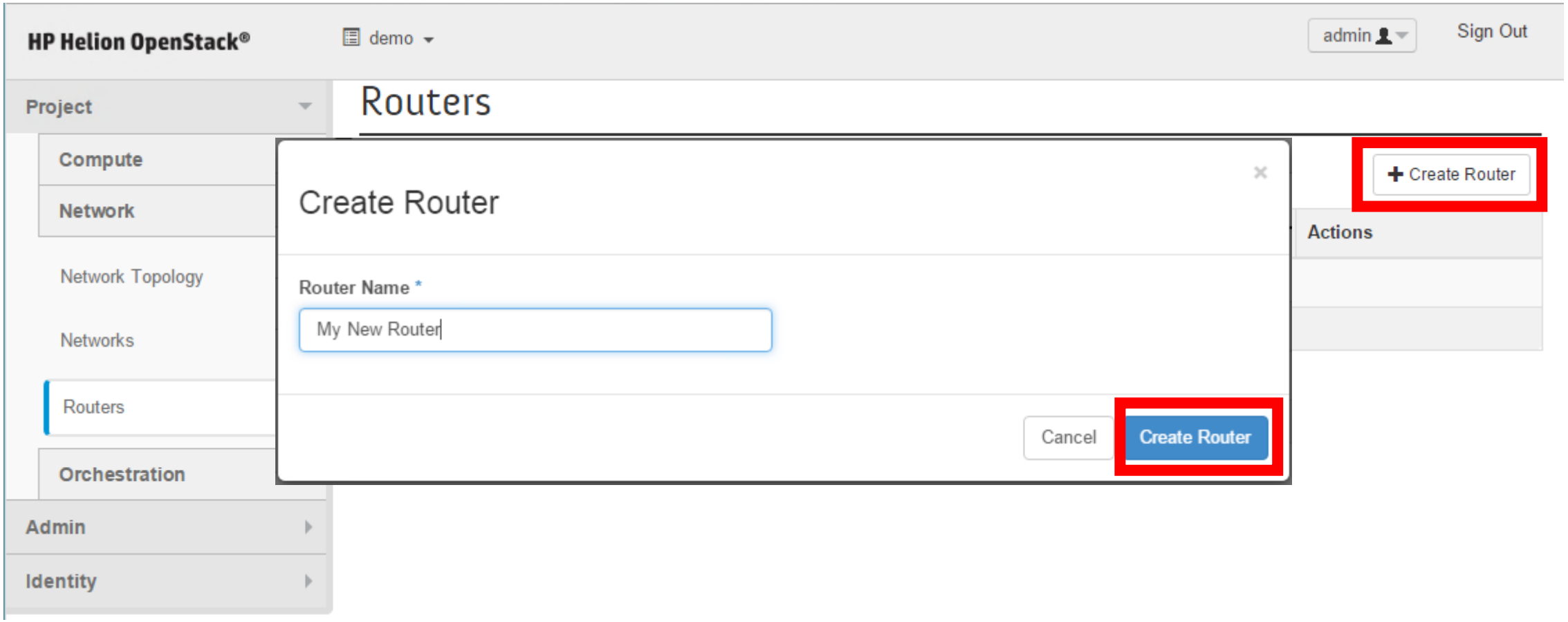
OpenStack - Networking



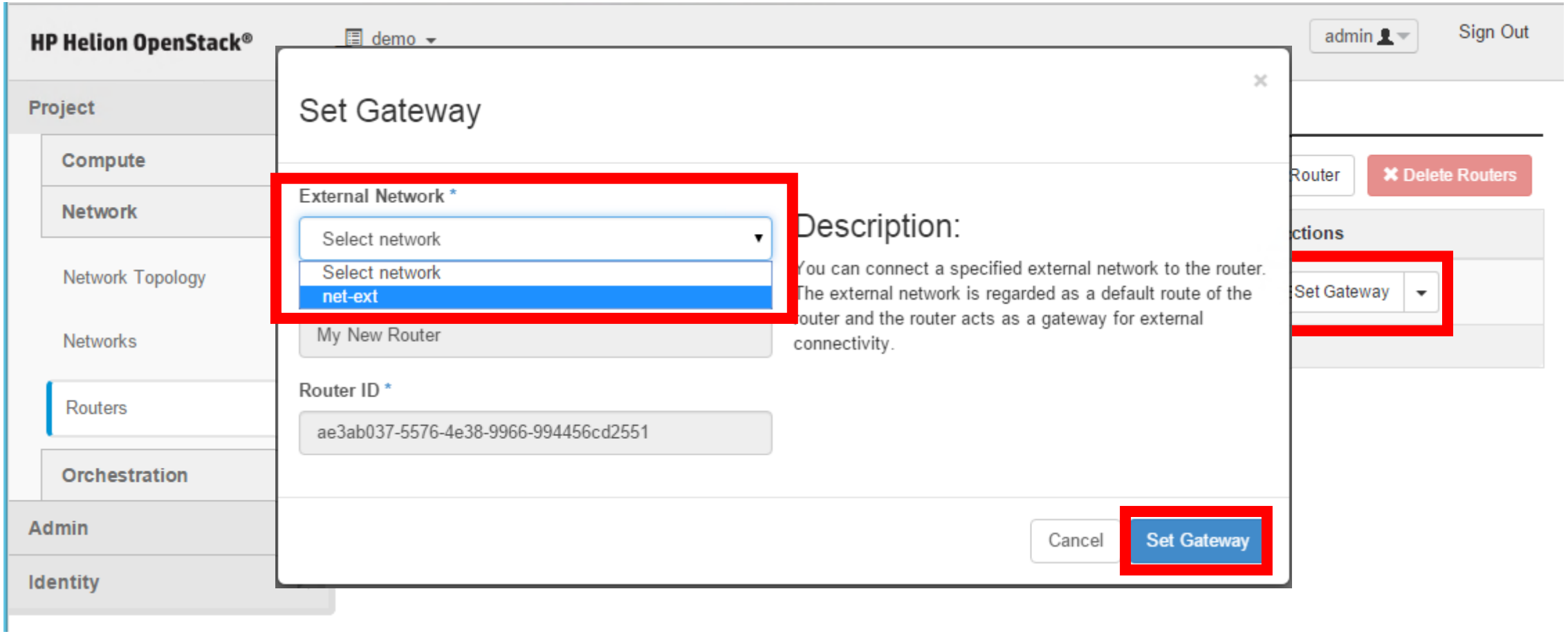
OpenStack – Networking



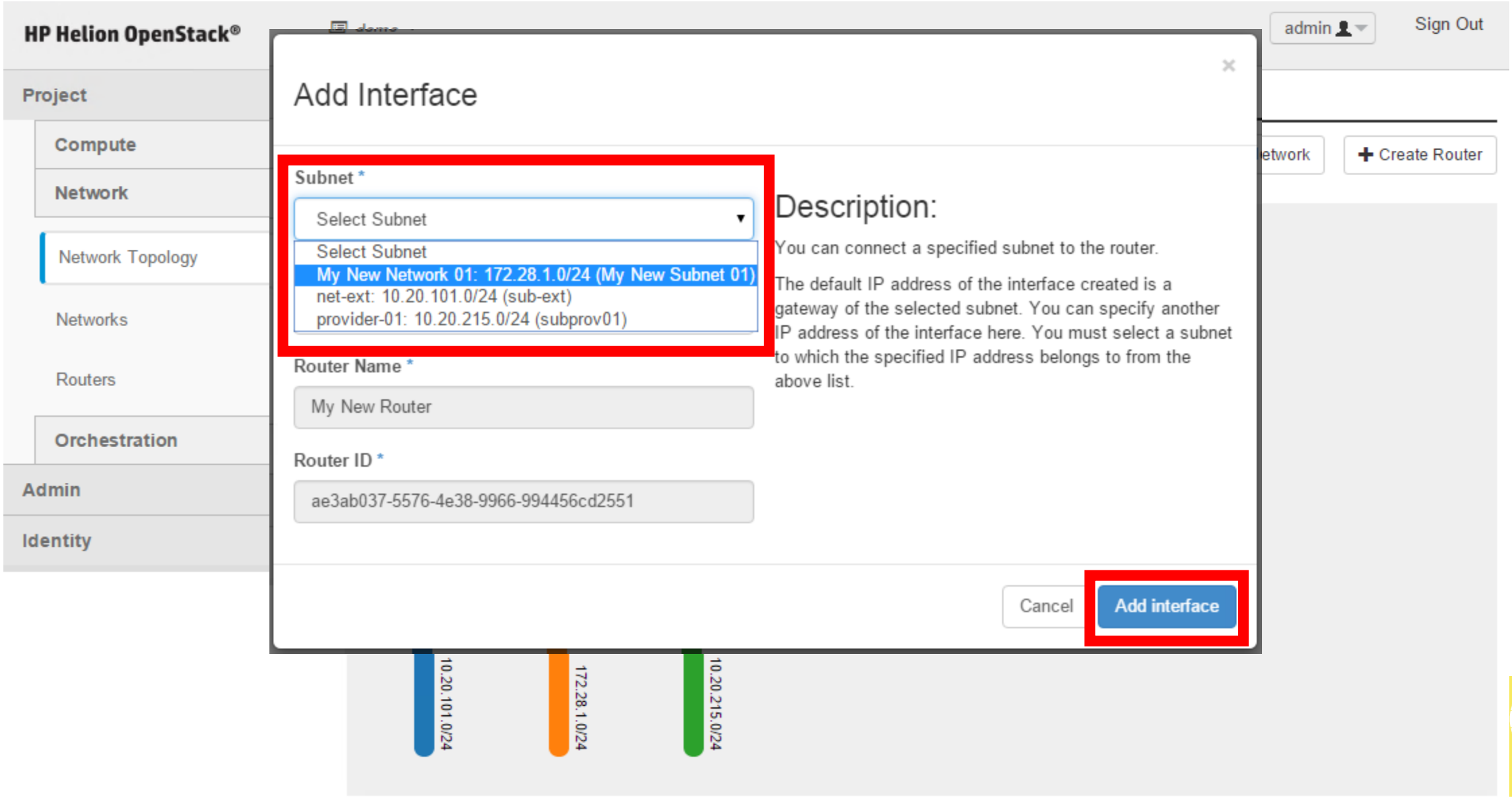
OpenStack – Networking



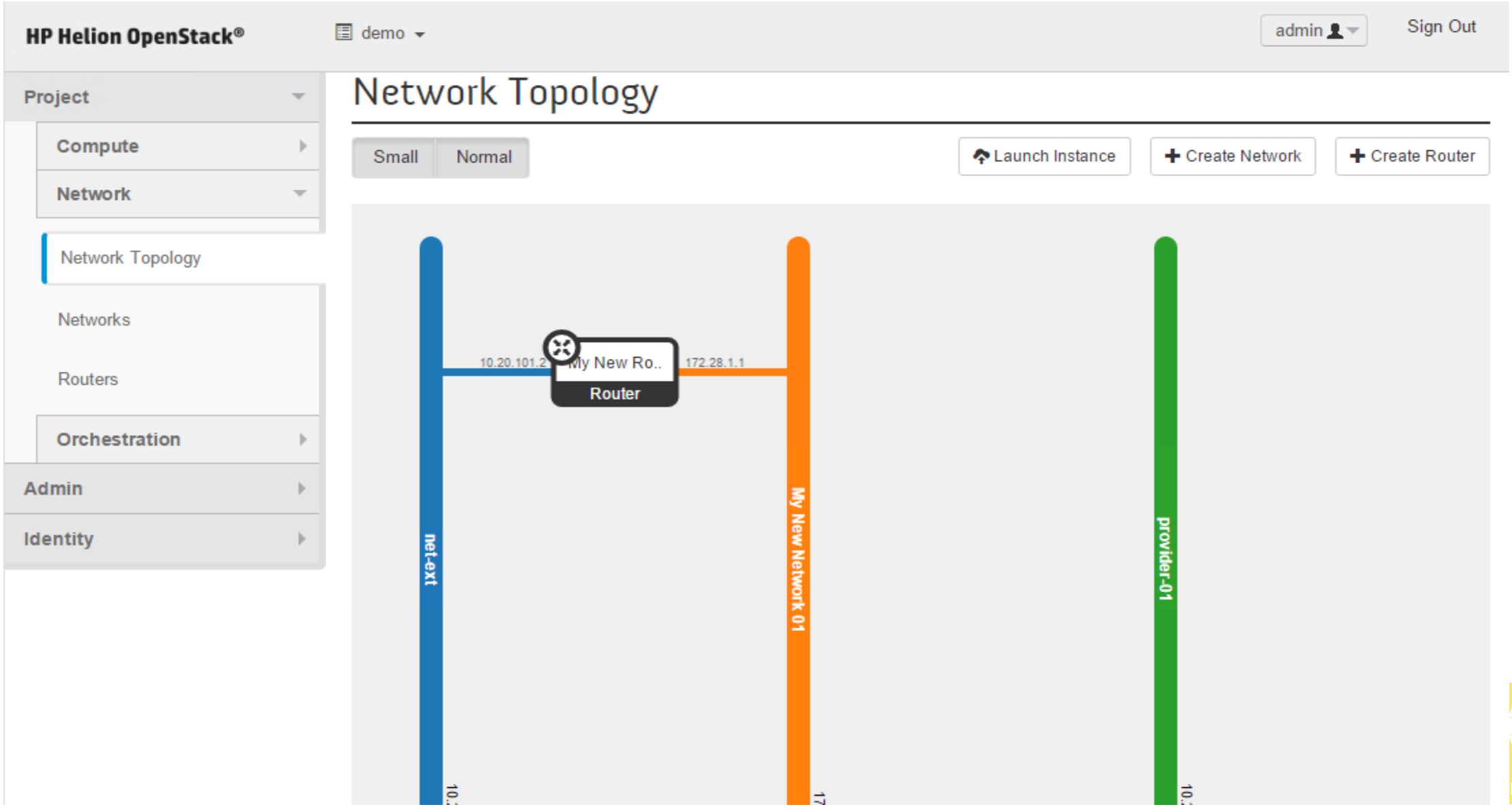
OpenStack – Networking



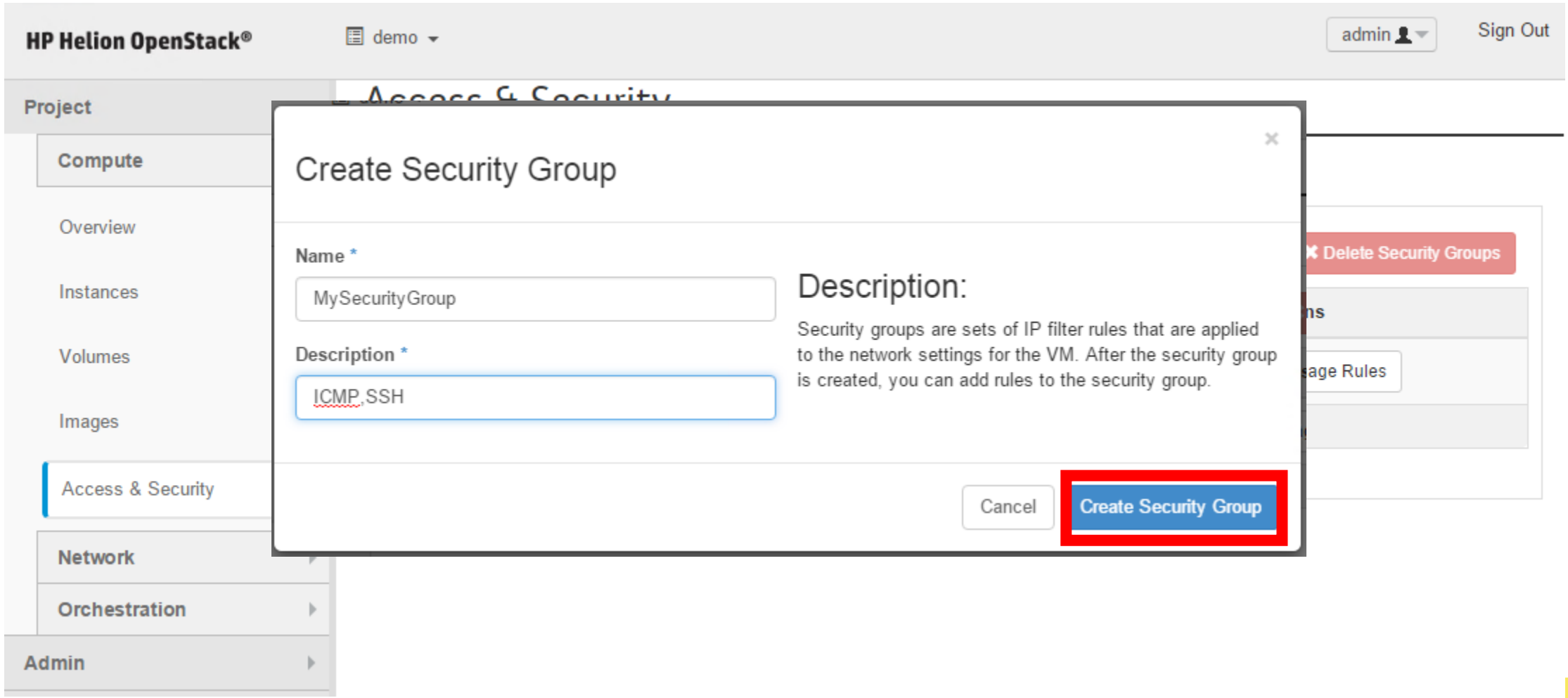
OpenStack – Networking



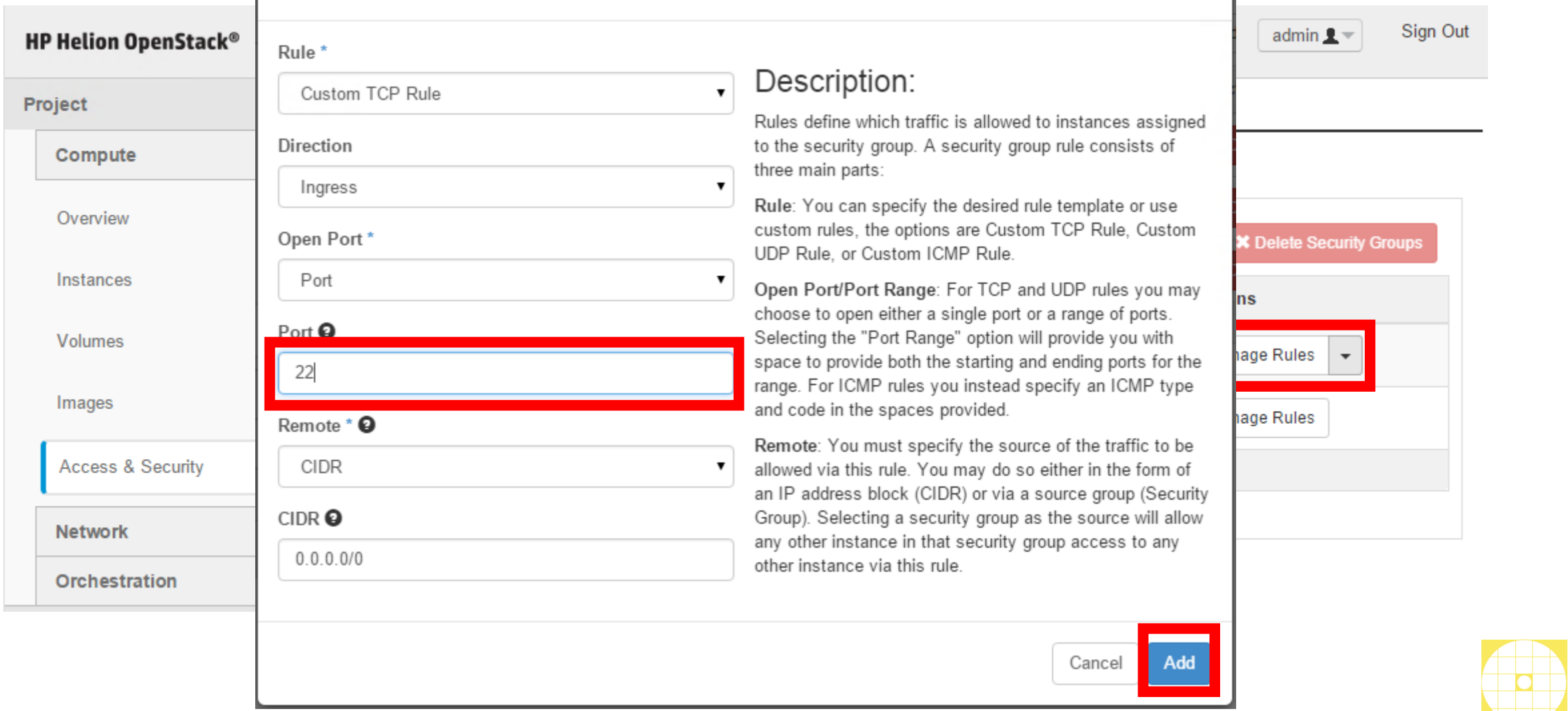
OpenStack – Networking



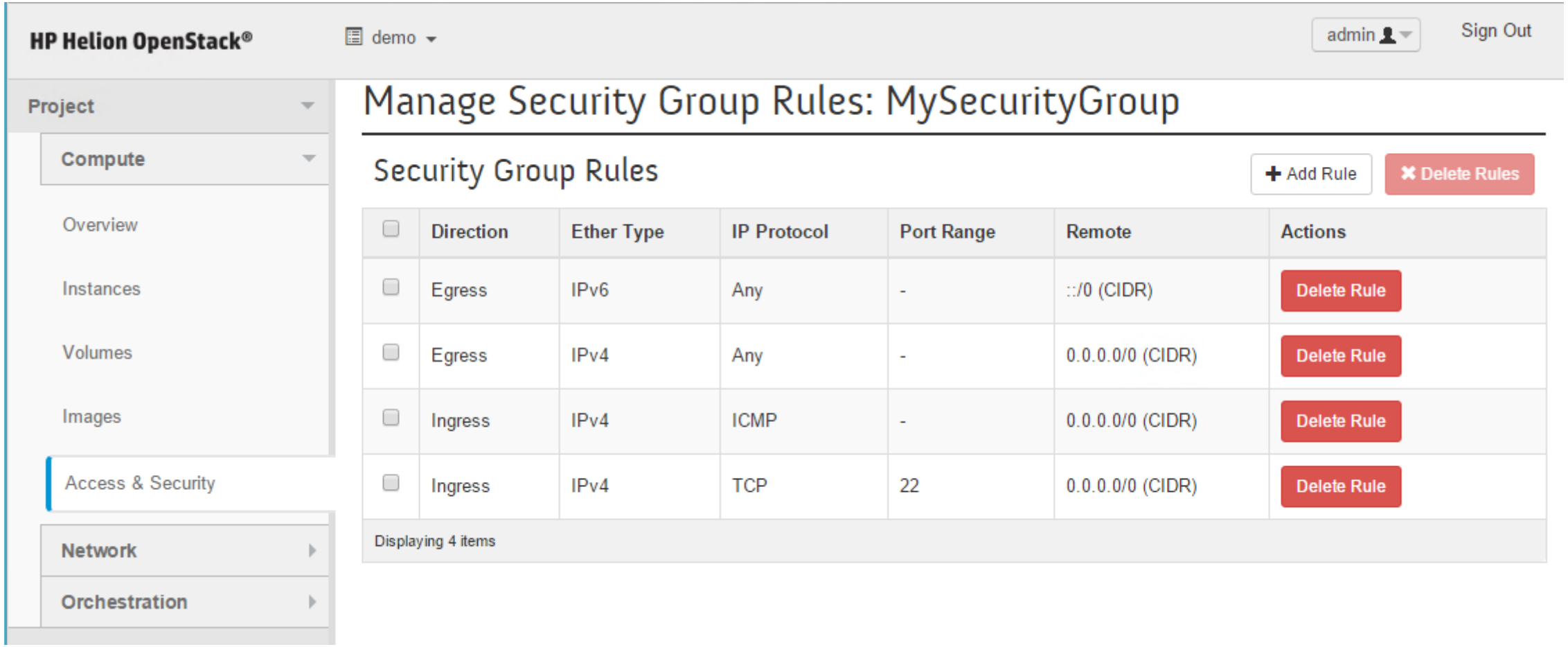
OpenStack – Networking



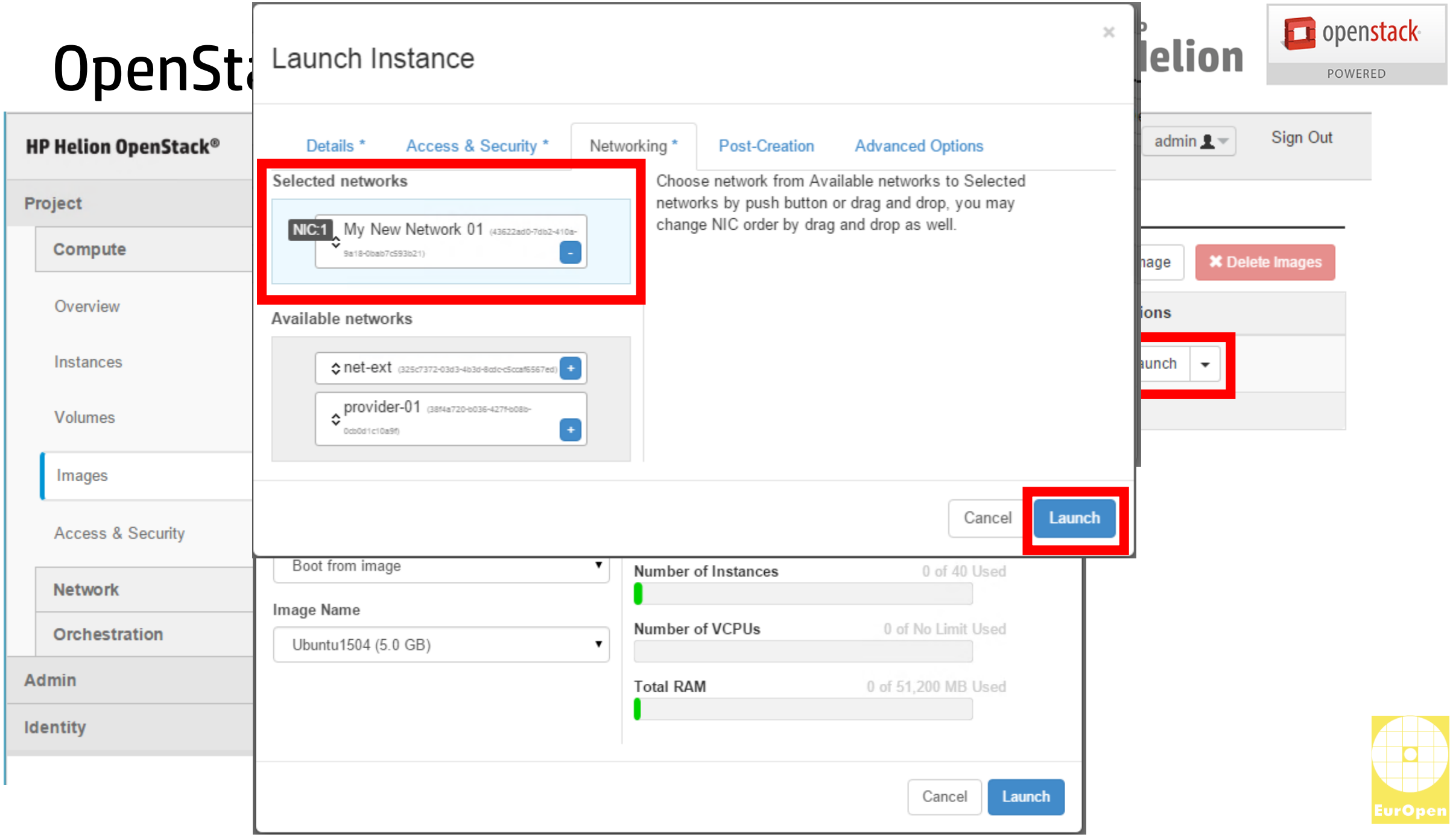
OpenSta


HP Helion OpenStack®
Project
Compute
Overview
Instances
Volumes
Images
Access & Security
Network
Orchestration
admin
Sign Out
Delete Security Groups
Add Rule
Rule *
Custom TCP Rule
Direction
Ingress
Open Port *
Port
Port
22
Remote *
CIDR
CIDR
0.0.0.0/0
Description:
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:
Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.
Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.
Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.
Cancel
Add

OpenStack – Networking



OpenSta

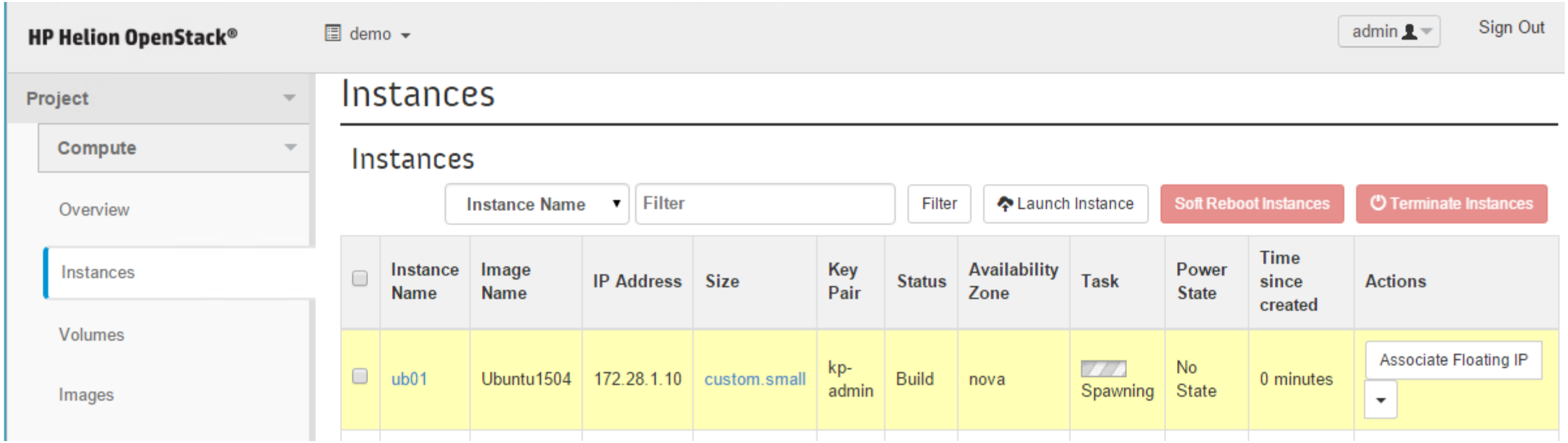


helion

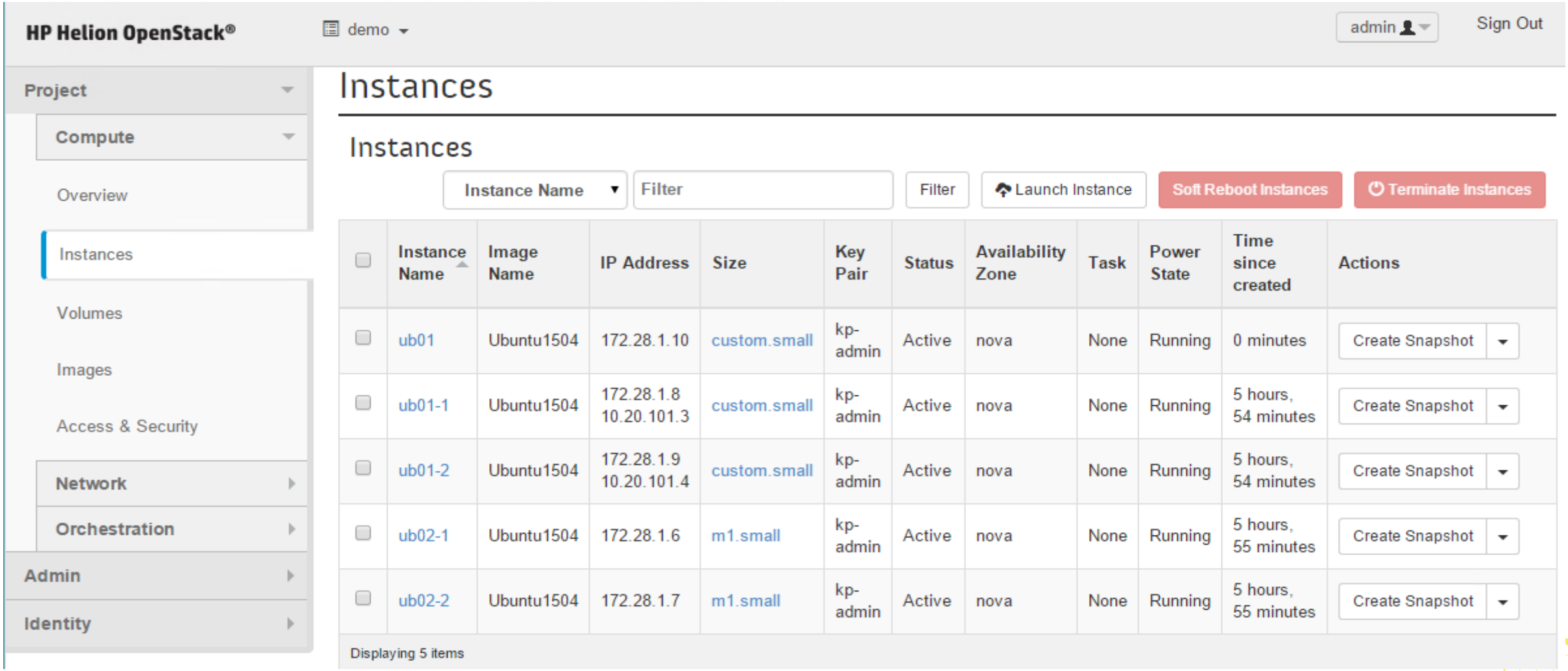
openstack
POWERED

EurOpen

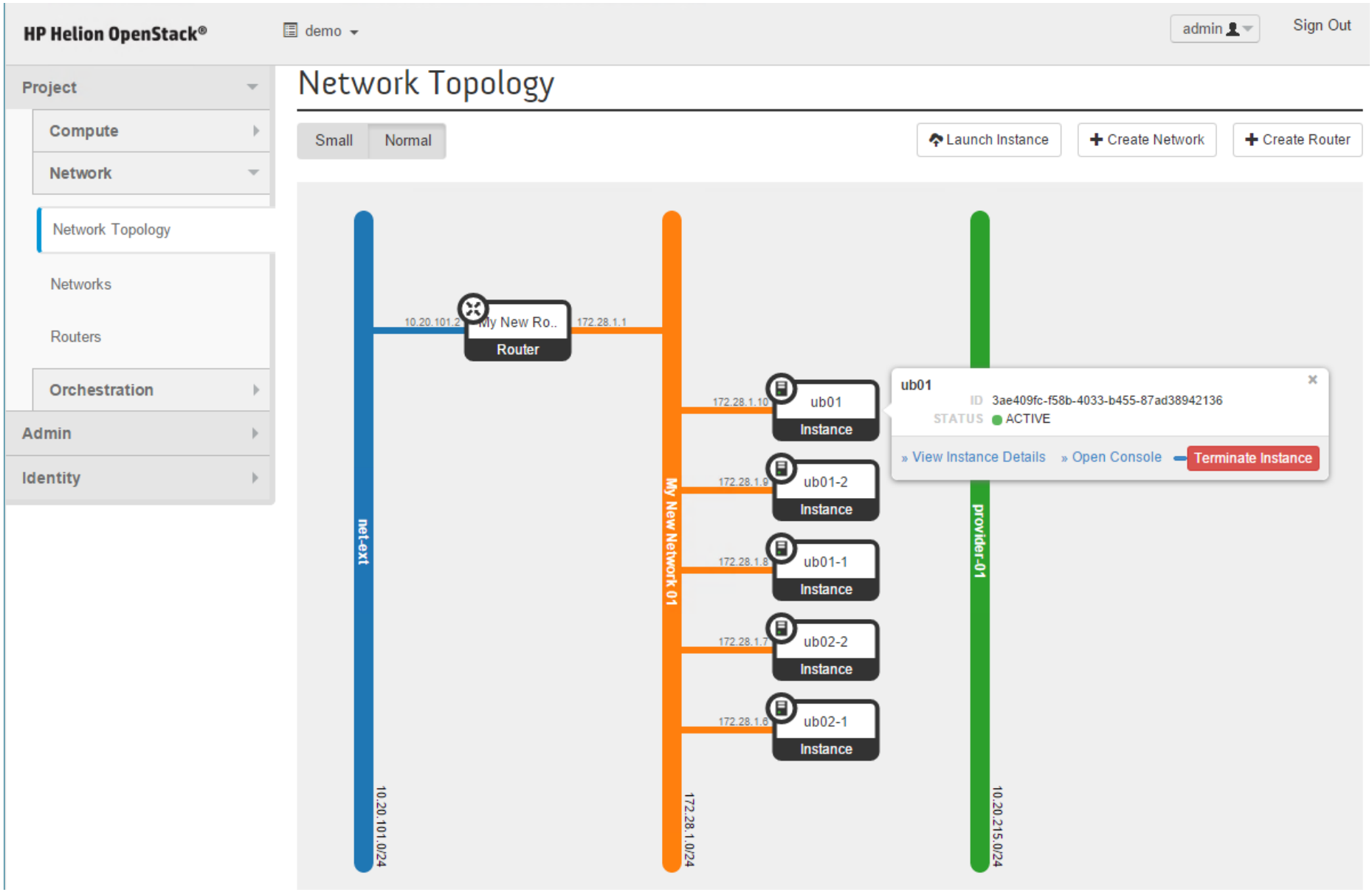
OpenStack – Networking



OpenStack – Networking



OpenStack – Networking



OpenStack – Neutron

HP Helion

openstack POWERED

Neutron CLI

```
root@ma1:~# neutron router-list
+--------------------------------------+----------------+-------------------------------------------------------------------------------------------------------------------------------------------------------------------------+-------------+--------+
| id                                   | name           | external_gateway_info                                                                                                                                                   | distributed | ha     |
+--------------------------------------+----------------+-------------------------------------------------------------------------------------------------------------------------------------------------------------------------+-------------+--------+
| ae3ab037-5576-4e38-9966-994456cd2551 | My New Router | {"network_id": "325c7372-03d3-4b3d-8cdc-c5ccaf6567ed", "enable_snat": true, "external_fixed_ips": [{"subnet_id": "e5cdd900-6467-4966-b8e7-9e0b070a996b", "ip_address": "10.20.101.2"}]} | False       | False |
+--------------------------------------+----------------+-------------------------------------------------------------------------------------------------------------------------------------------------------------------------+-------------+--------+
```

```
root@ma1:~# neutron net-list
+--------------------------------------+-------------------+-----------------------------------------------------+
| id                                   | name              | subnets                                             |
+--------------------------------------+-------------------+-----------------------------------------------------+
| 325c7372-03d3-4b3d-8cdc-c5ccaf6567ed | net-ext           | e5cdd900-6467-4966-b8e7-9e0b070a996b 10.20.101.0/24 |
| 38f4a720-b036-427f-b08b-0cb0d1c10a9f | provider-01       | 5f2a980c-9731-41bb-9019-262780d2a486 10.20.215.0/24 |
| 43622ad0-7db2-410a-9a18-0bab7c593b21 | My New Network 01 | cede6ecb-0118-4392-b73d-e2cf924fcbd5 172.28.1.0/24  |
+--------------------------------------+-------------------+-----------------------------------------------------+
```

```
root@ma1:~# neutron subnet-list
+--------------------------------------+------------------+----------------+----------------------------------------------------+
| id                                   | name             | cidr           | allocation_pools                                   |
+--------------------------------------+------------------+----------------+----------------------------------------------------+
| 5f2a980c-9731-41bb-9019-262780d2a486 | subprov01        | 10.20.215.0/24 | {"start": "10.20.215.100", "end": "10.20.215.200"} |
| cede6ecb-0118-4392-b73d-e2cf924fcbd5 | My New Subnet 01 | 172.28.1.0/24  | {"start": "172.28.1.2", "end": "172.28.1.254"}     |
| e5cdd900-6467-4966-b8e7-9e0b070a996b | sub-ext          | 10.20.101.0/24 | {"start": "10.20.101.2", "end": "10.20.101.254"}   |
+--------------------------------------+------------------+----------------+----------------------------------------------------+
```

EurOpen

OpenStack – Neutron

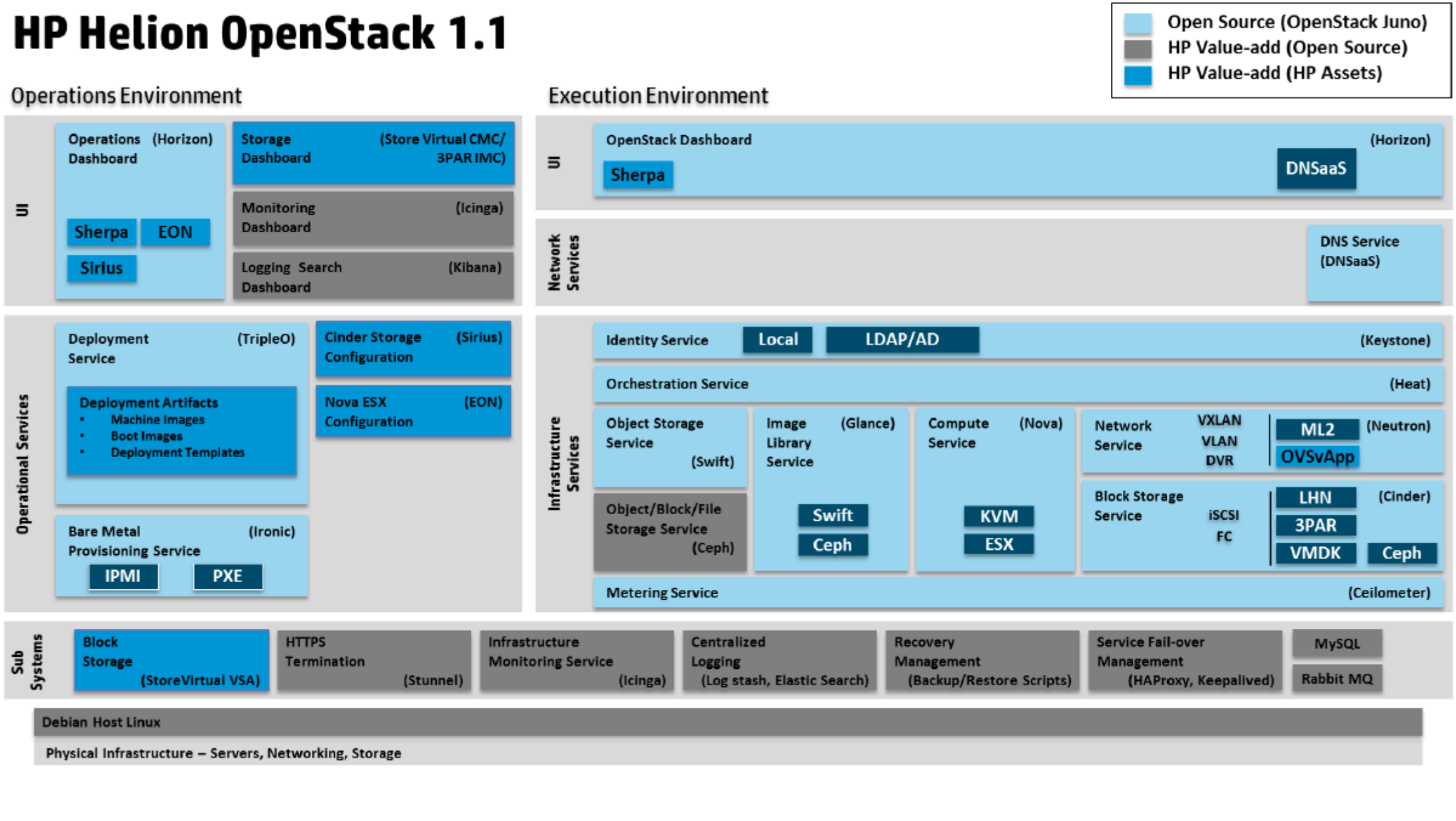
Neutron CLI

root@ma1:~# neutron agent-list

id	agent_type	host	alive	admin_state_up	binary
0b42e813-e11f-43a5-b978-e5e354f9d388	HP VCN L2 Agent	ovsvapp-esxcptnode.example.org	:-)	True	hpvcn-neutron-agent
182d27c6-1aca-4fe5-a7a7-92ac961def10	Metadata agent	cc1	:-)	True	neutron-metadata-agent
1f04c00b-c73f-4cba-a5c7-3b4704391855	DHCP agent	cmc	:-)	True	neutron-dhcp-agent
495feb13-d42b-4d96-bfe4-b4fcd7b7c632	DHCP agent	cc1	:-)	True	neutron-dhcp-agent
76029cdc-220c-4c28-800c-65faec106409	DHCP agent	cc2	:-)	True	neutron-dhcp-agent
7958e4c1-706f-4ded-b3a4-1d3658d98e63	L3 agent	cmc	:-)	True	neutron-l3-agent
7ec7caeb-bc53-45c0-bf46-19fb1e45ca30	Open vSwitch agent	cc1	:-)	True	neutron-openvswitch-agent
92e986b0-8171-4444-932b-c4661cac4095	Open vSwitch agent	cmc	:-)	True	neutron-openvswitch-agent
a48ce031-a4bc-40a2-98dc-31c173a2b166	Metadata agent	cmc	:-)	True	neutron-metadata-agent
b8c79f2e-d840-4b18-a8ec-2f1730f5a4a1	Metadata agent	cc2	:-)	True	neutron-metadata-agent
b9c36910-e9d1-4f9a-848a-cce14f13955f	L3 agent	cc1	:-)	True	neutron-l3-agent
d57707af-ff9d-4a70-93cd-678bbbb571bc	Open vSwitch agent	cc2	:-)	True	neutron-openvswitch-agent
ee649627-902d-4559-b9db-97daa4b8847a	L3 agent	cc2	:-)	True	neutron-l3-agent

HP Helion OpenStack

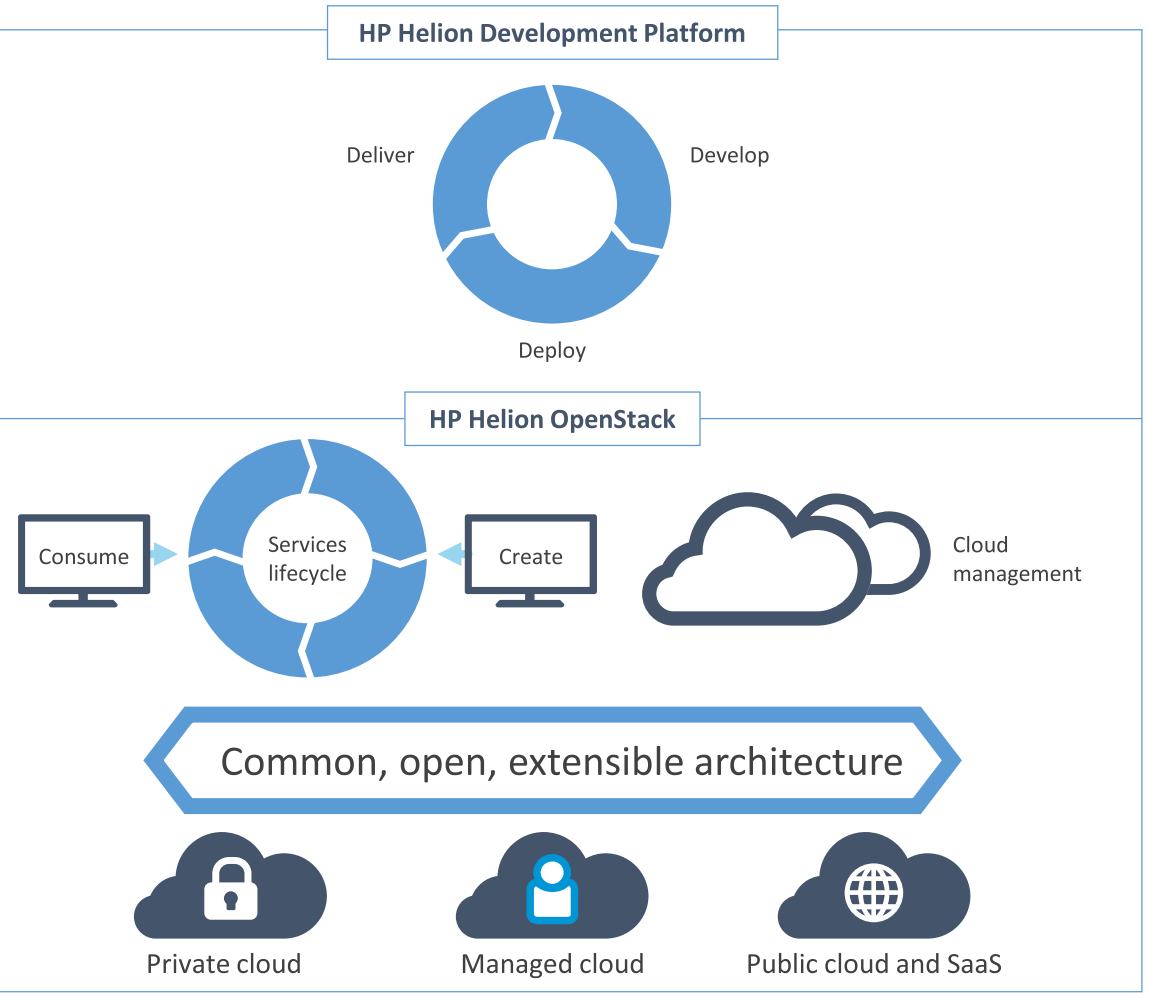
HP Helion OpenStack 1.1



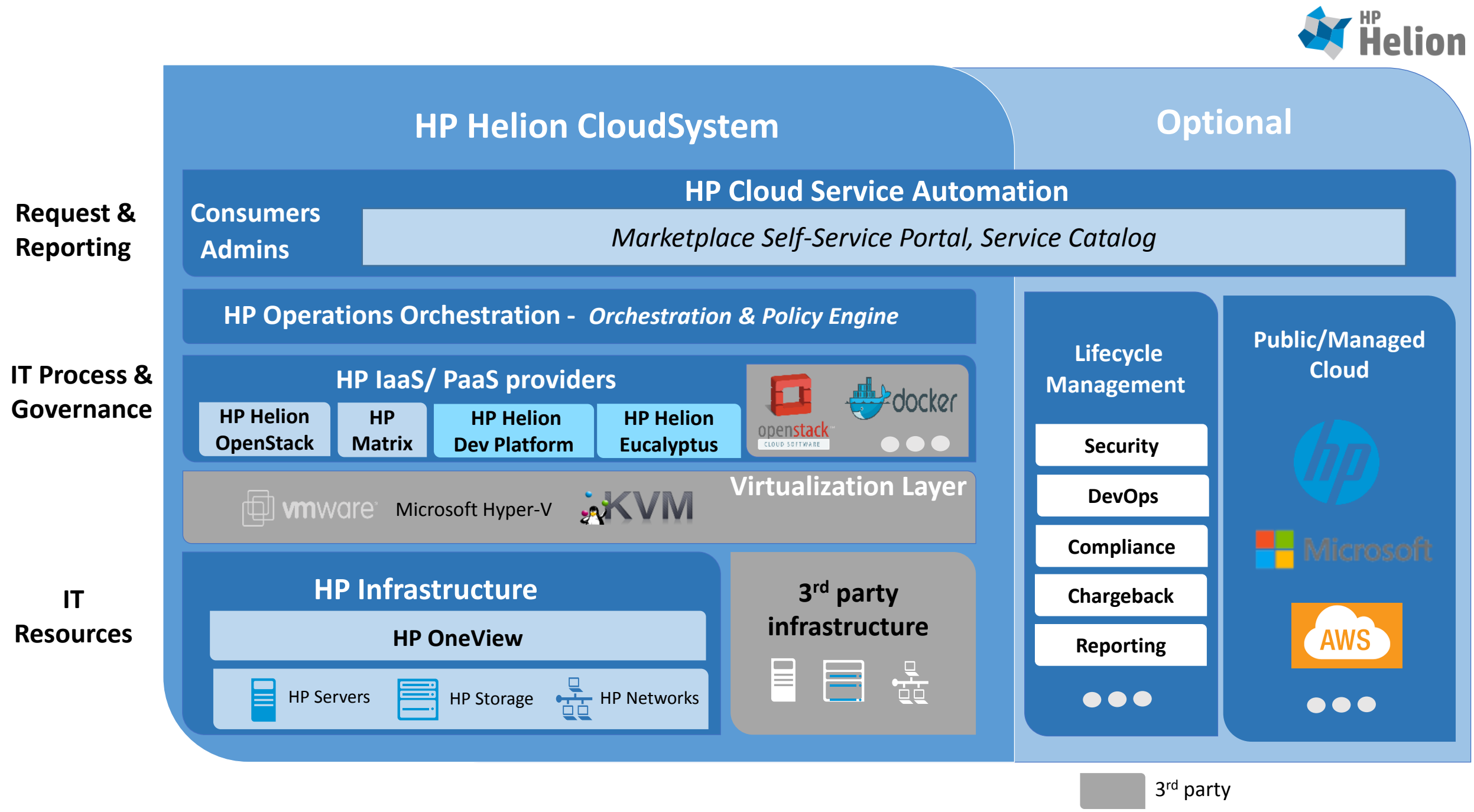
HP Helion Platform: Integrated IaaS and PaaS

HP Helion OpenStack (IaaS) + HP Helion Development Platform (PaaS) = better together

- **Flexible cloud-native infrastructure**
- **Application portability**
- **Control costs** and **avoid vendor lock-in**
- **Easier administration**
- **Visibility into resources**



HP Helion CloudSystem



Děkuji za pozornost ☺

Daniel Prchal

daniel.prchal@hpe.com