Operations Trend & OpenStack Administration Workshop
SMK Taruna Bhakti Depok, 11 Januari 2017

Utian Ayuba
utian@btech.id

Btech

About Me

- Executive Director of Btech

- Consultant for Networking and Security for SIKD Development – KOMPAK

- Consultant for System and Network of GAMBUT project – CCROM-SEAP IPB

- Member of Indonesia openSUSE Community

Keywords

DevOps, On-premise, Cloud, IaaS, Paas, SaaS, Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, Virtualization, Storage Cluster, SDN, Keystone, Glance, Nova, Neutron, Cinder, Swift, Horizon

References

- Linux Foudation Guide to the Open Cloud

  https://www.linux.com/publications/guide-open-cloud

- OpenStack Documentation
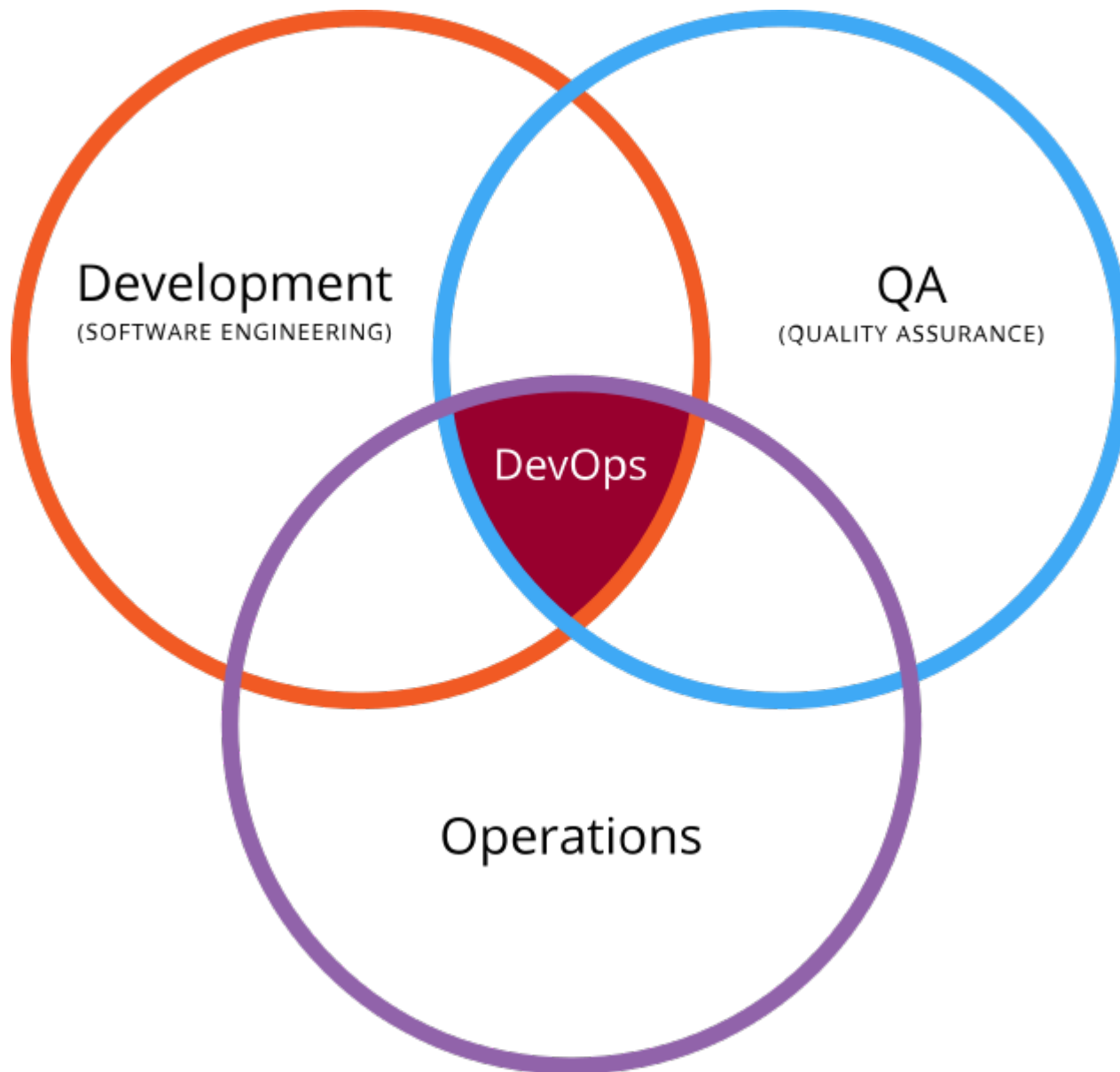 http://docs.openstack.org

DevOps

Development & Operations (DevOps)

"a set of processes and methods for thinking about communication and collaboration between development, QA, and IT operations"
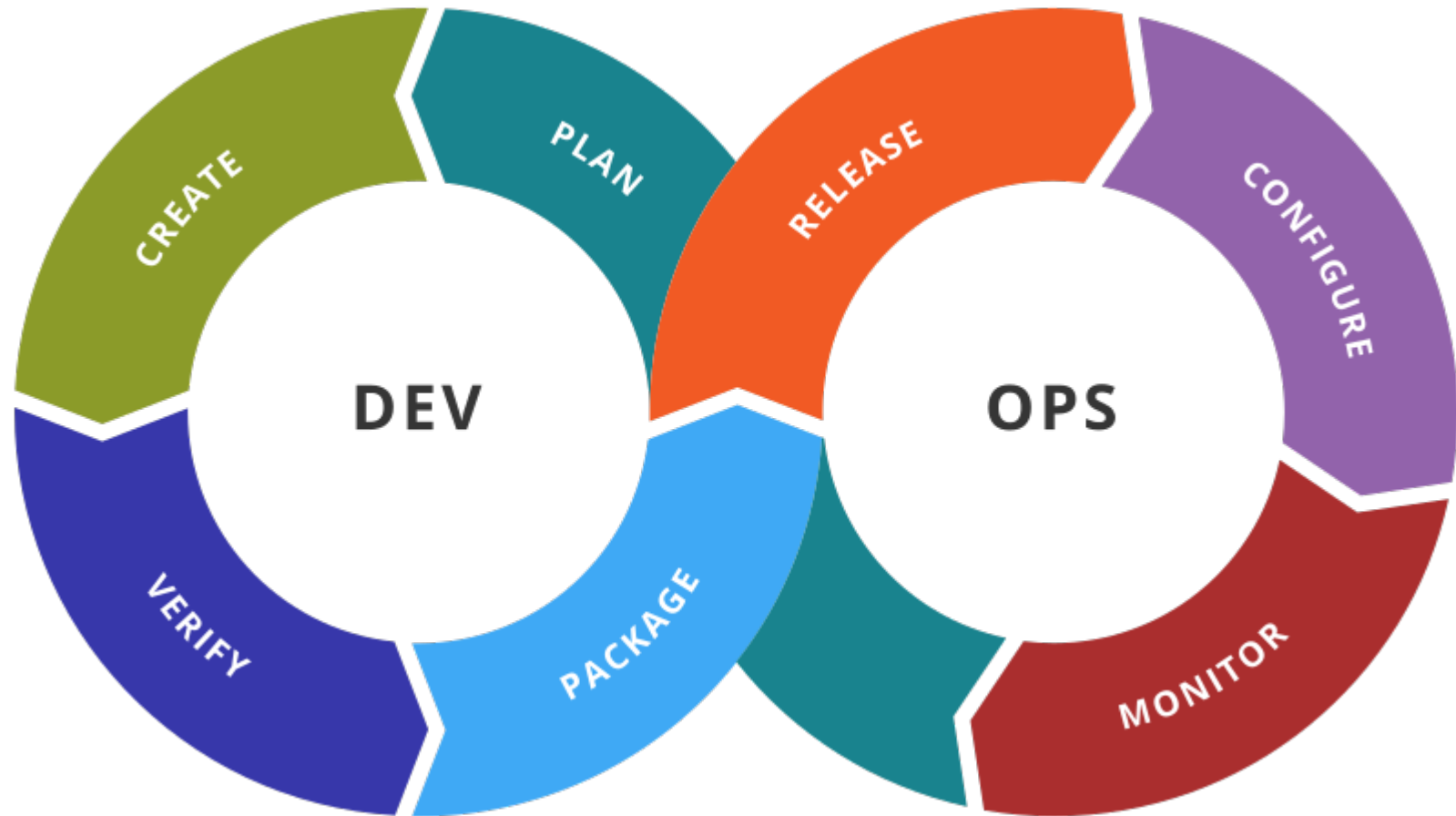
https://en.wikipedia.org/wiki/DevOps

DevOps Intersection

DevOps Stages

Operations Tools

Infrastructure as a Service (IaaS)
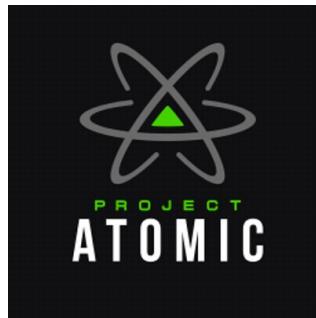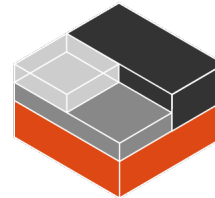
Platform as a Service (PaaS)
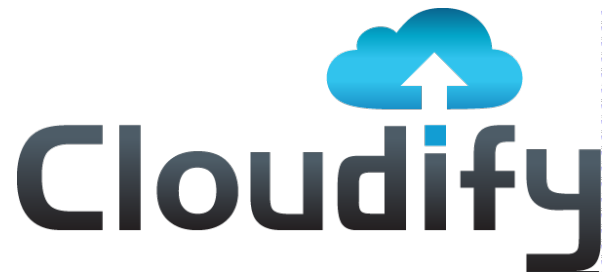
Cloud Operating System

Containers, Hypervisors, Virtualization Softwares

Management & Automation
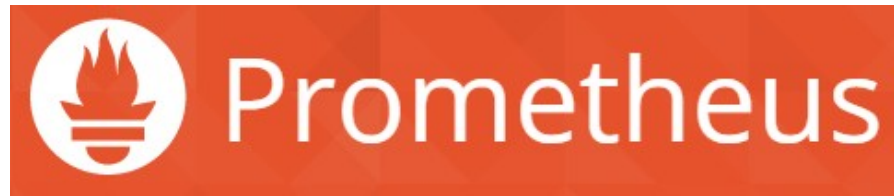
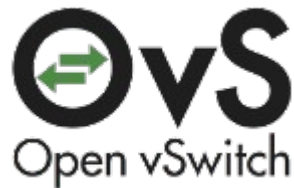# Continuous Integration/Delivery (CI/CD)

Configuration Management

Logging & Monitoring

Software-Defined Networking (SDN)

Software-Defined Storage (SDS)

Cloud Computing

On-Premise vs Cloud

Conventional Data Center

App 1 | App 2 | App 3 | App 4

CPU | MEM | CPU | MEM | CPU | MEM | CPU | MEM

OS1 | OS2 | OS3 | OS4
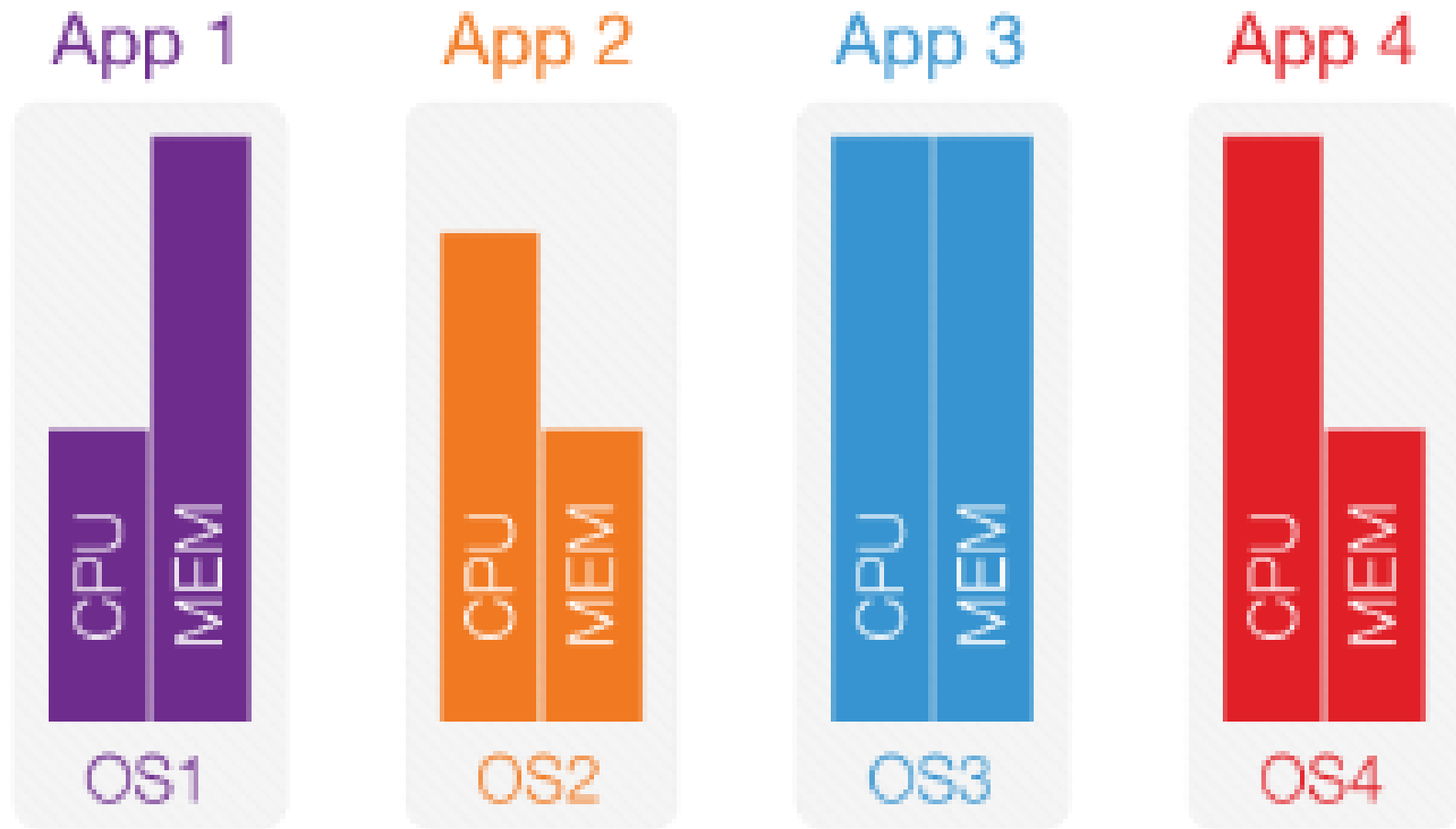
Cloud Characteristics

Cloud Types

Cloud Users

Cloud Deployment Model

Public Cloud
- Elasticity
- Utility Pricing
- Leverage Expertise

Private Cloud
- Total Control
- Regulation
- Flexibility

Community Cloud
- Meets shared concerns

Hybrid Cloud
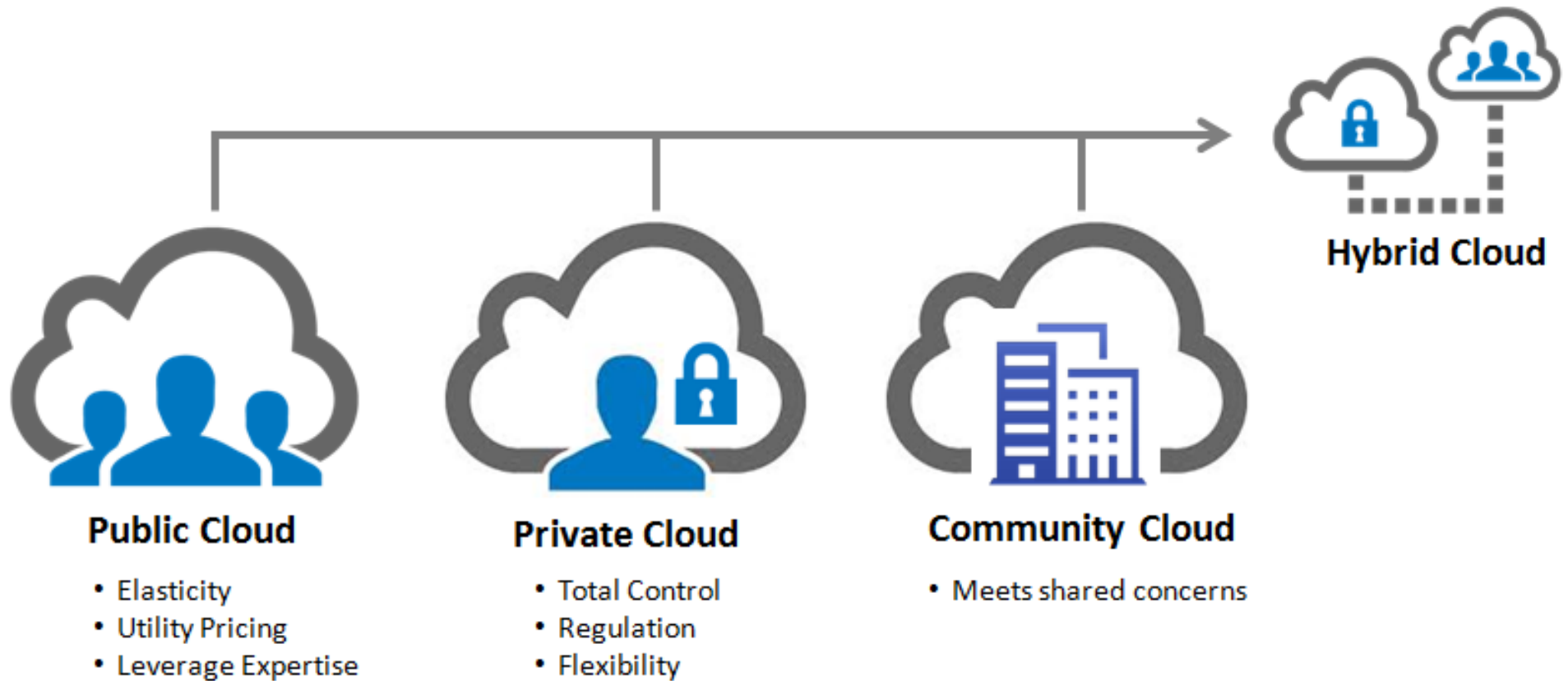
IaaS Public Cloud

Virtualization

Virtualization Types

- Hardware Level

  - Full Virtualization: Oracle VirtualBox, VMWare Workstation, Qemu

  - Bare Metal Virtualization: RedHat KVM, Citrix Xen, VMWare Vsphere, Microsoft HyperV

- Operating System Level (OS Container): OpenVZ, LXC

- Application Level (Application Container): Docker, rkt

Full Virtualization
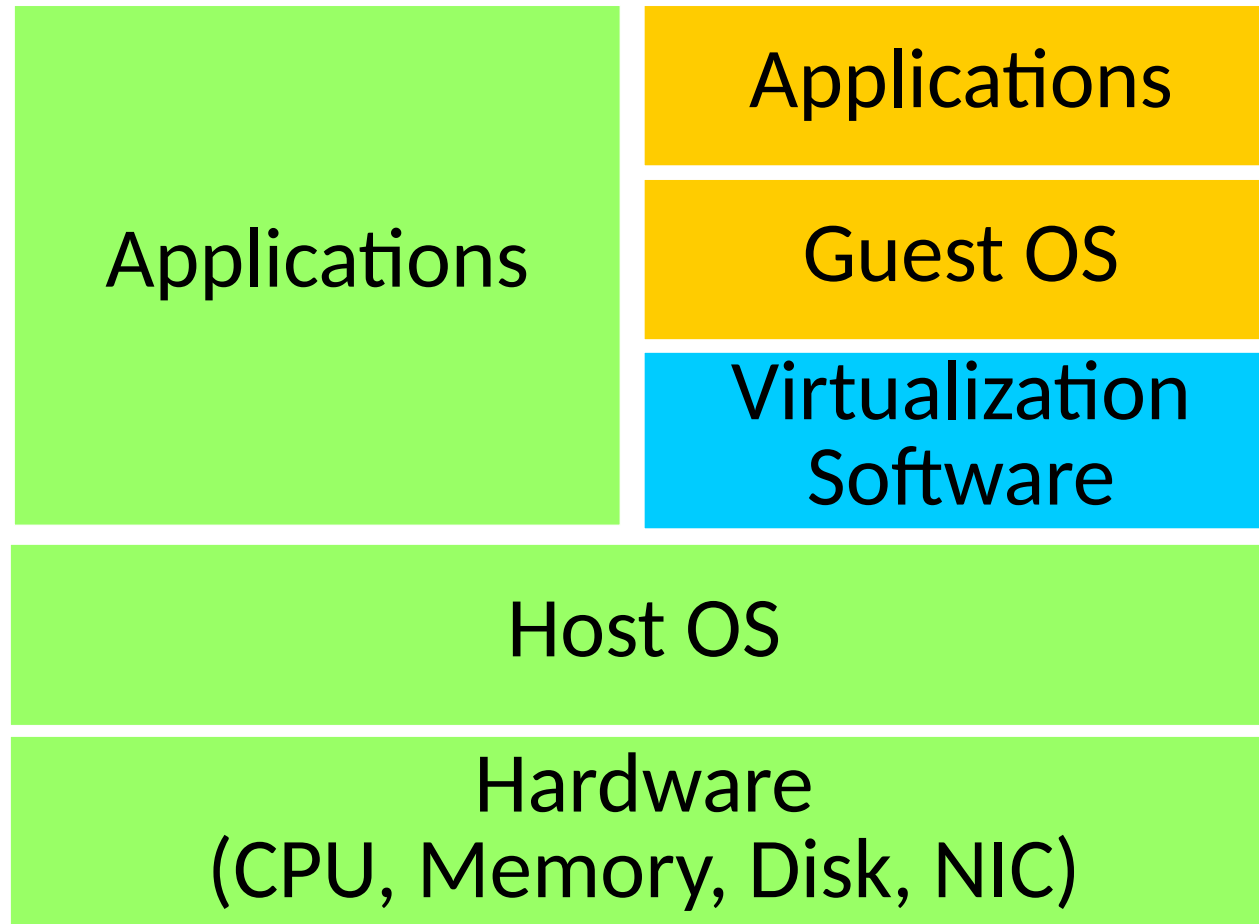
Applications

Applications

Guest OS

Virtualization Software

Host OS

Hardware
(CPU, Memory, Disk, NIC)

Bare Metal Virtualization

Apps	Apps	Apps
Guest OS	Guest OS	Guest OS

Hypervisor

Hardware
(CPU, Memory, Disk, NIC)

OS Container

Host OS		
OS Container	OS Container	OS Container

Container Engine & Management

Hardware
(CPU, Memory, Disk, NIC)

Application Container

Host OS

| Apps Container | Apps Container | Apps Container |

Container Engine & Management

Hardware
(CPU, Memory, Disk, NIC)
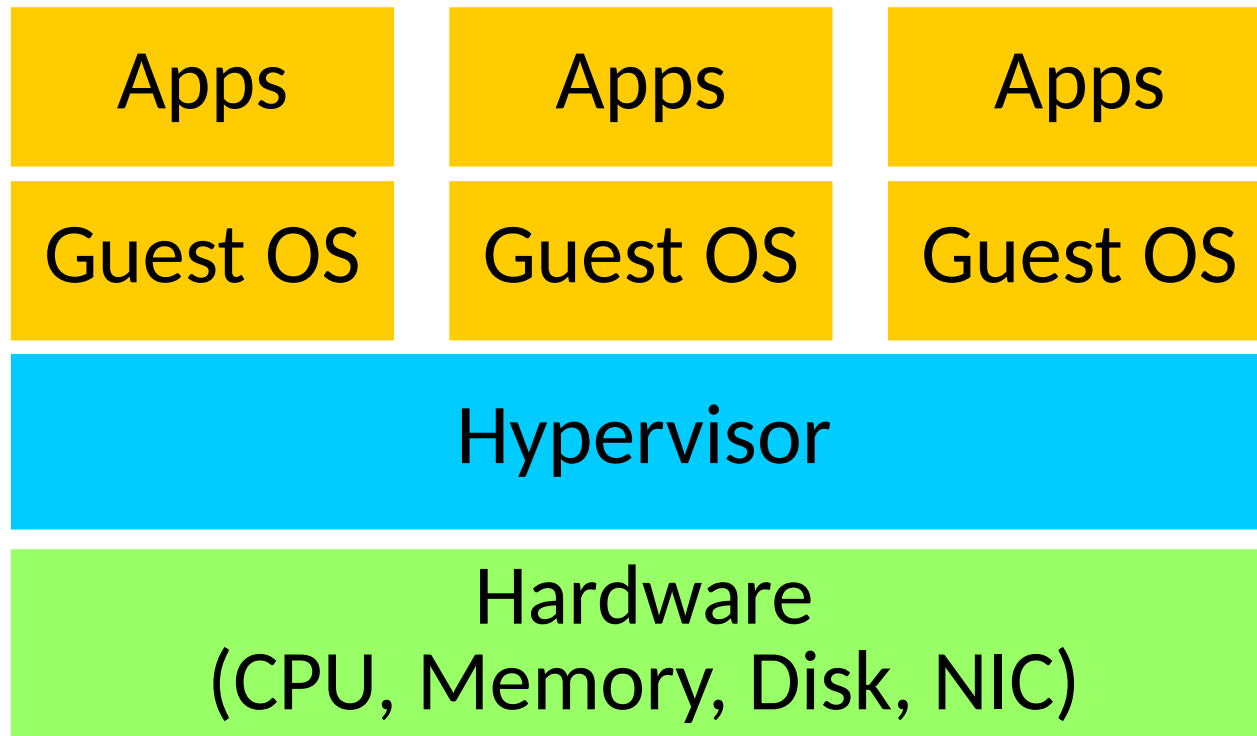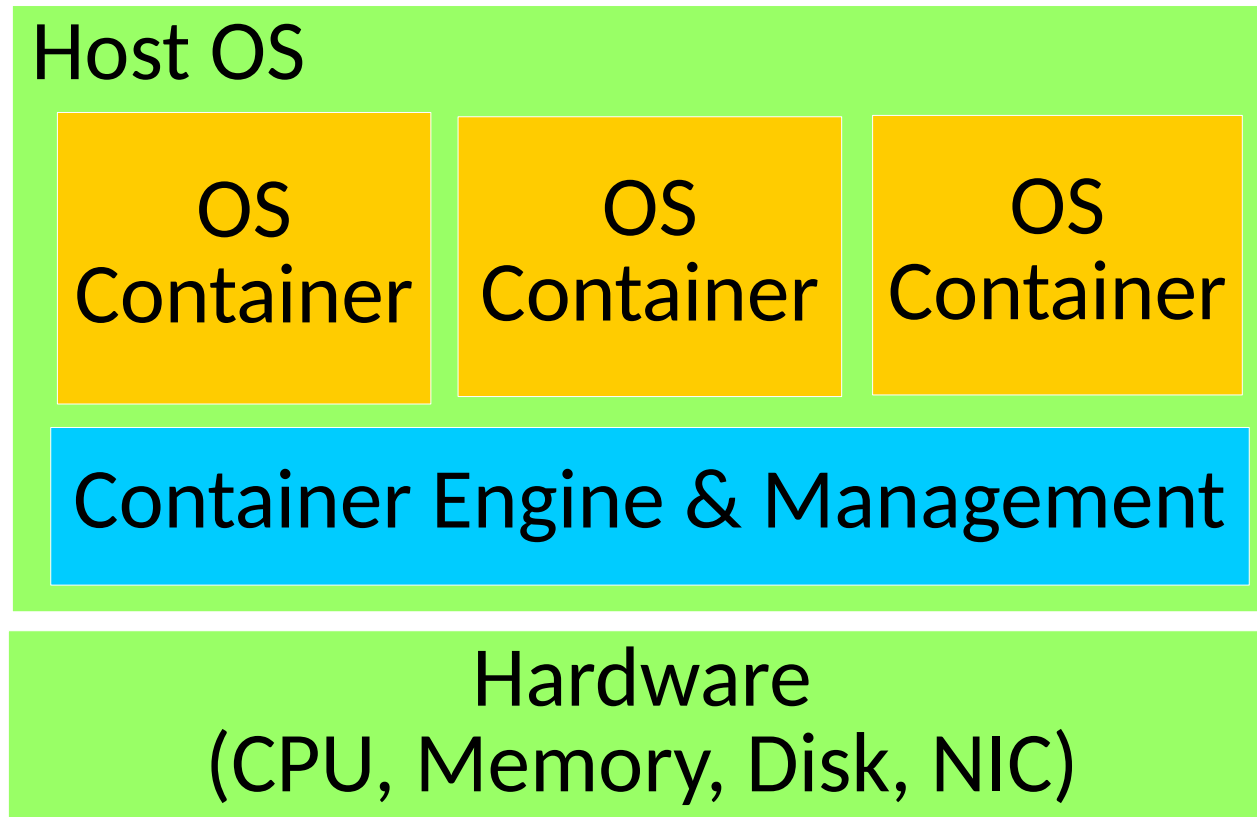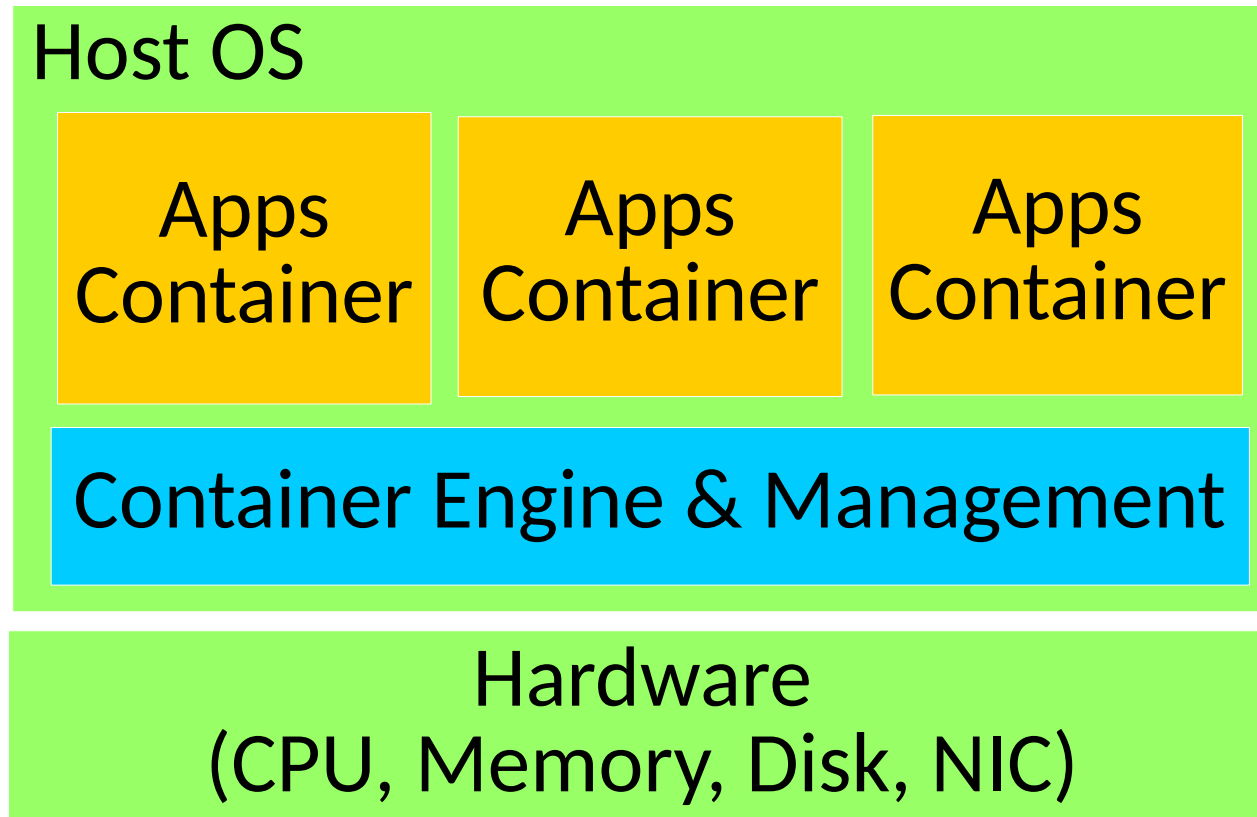
Software Defined Networking (1)

"an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow® protocol is a foundational element for building SDN solutions."

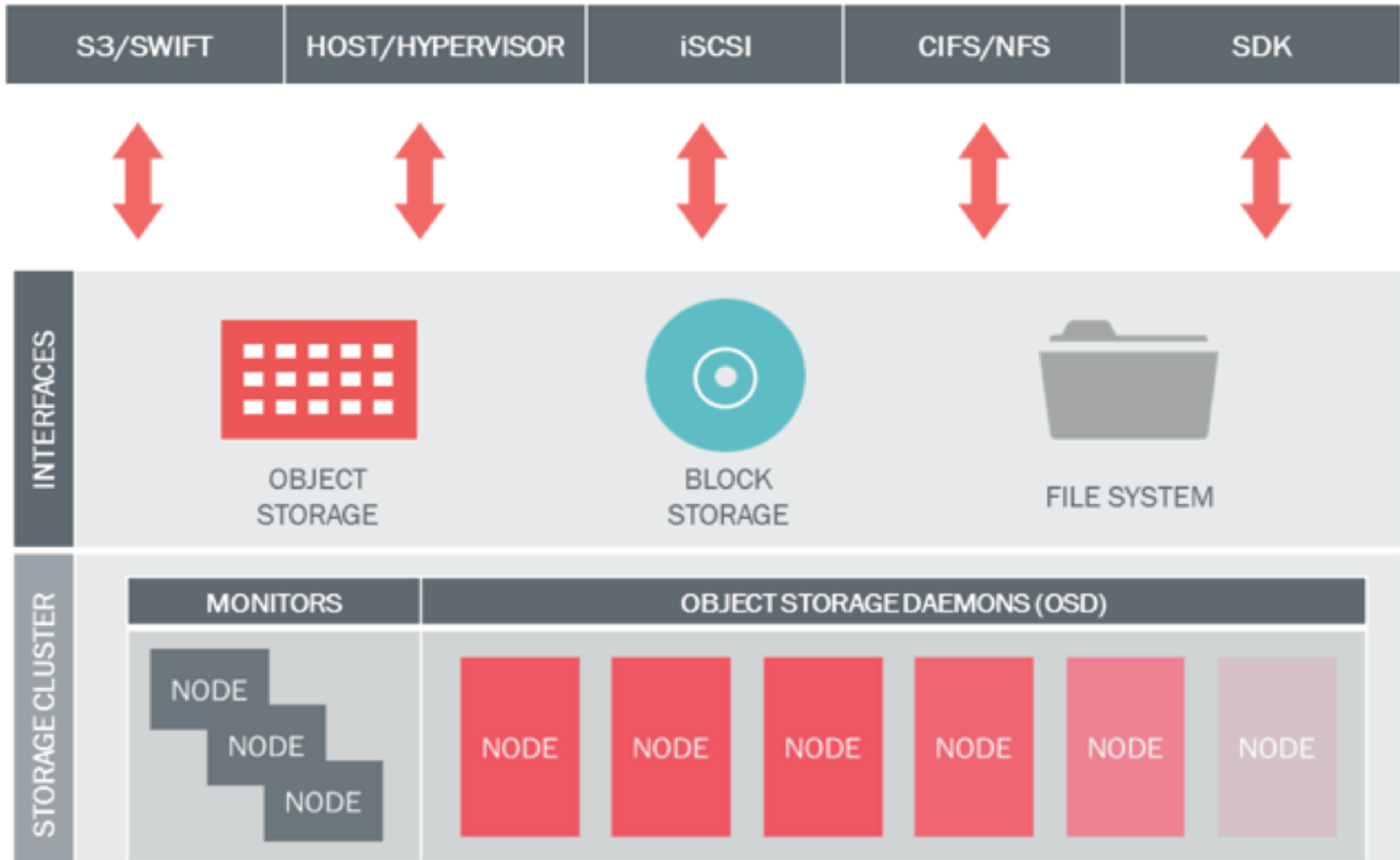https://www.opennetworking.org/sdn-resources/sdn-definition

Software Defined Networking (2)
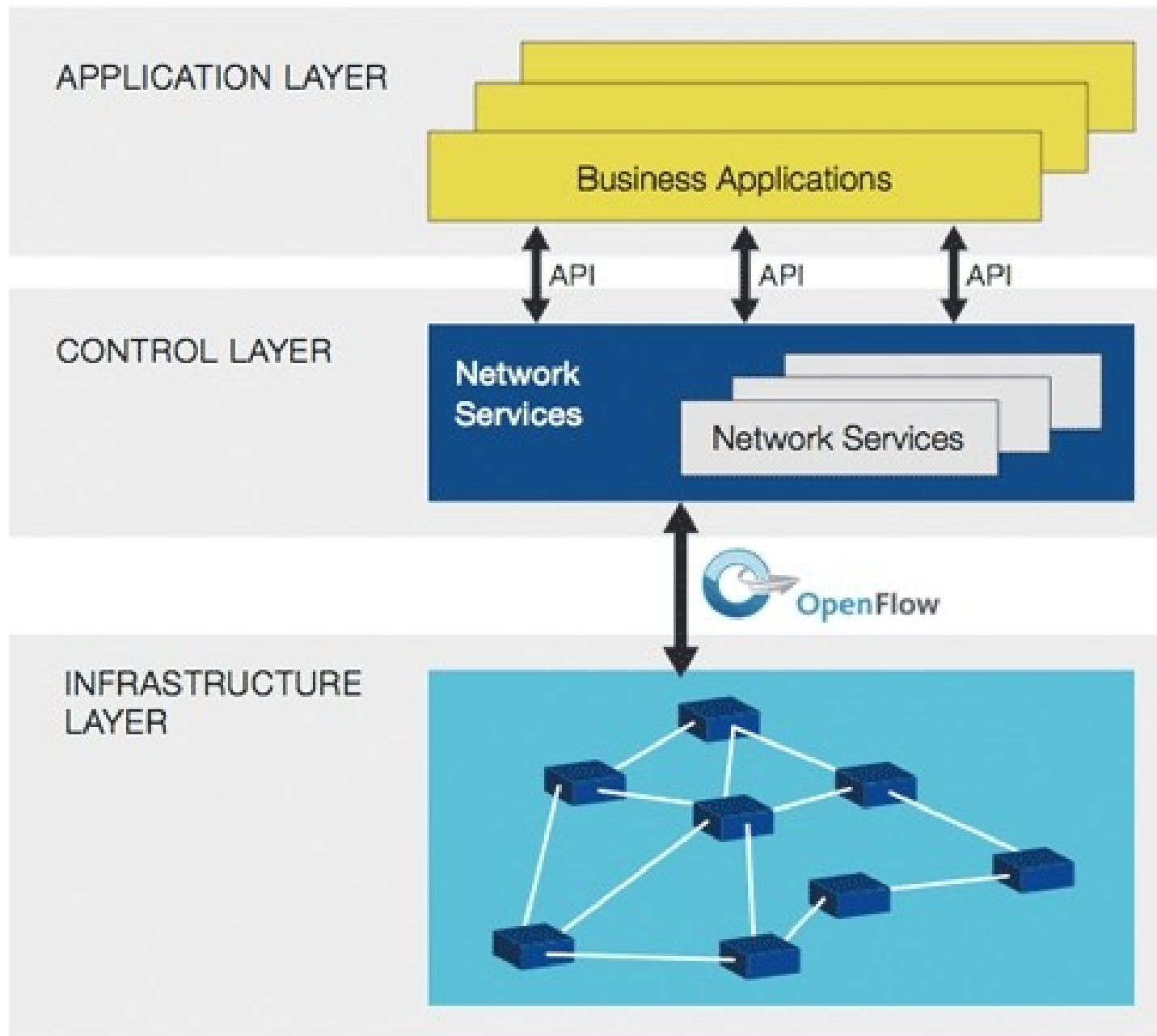
OpenFlow Based Plugin

- Open vSwitch
- Cisco UCS
- Linux Bridge
- Nicira NVP
- Ryu OpenFlow
- NEC OpenFlow
- Big Switch
- CloudBase Hyper-V
- Midionet
- Brocade VCS
- Juniper
- Mellanox
- ML2

Storage Clusters

OpenStack

OpenStack Platinum Members

AT&T

Canonical

Hewlett Packard Enterprise

IBM

Intel

Rackspace

Red Hat, Inc.

SUSE

OpenStack Gold Members

Aptira	CCAT	Cisco	Dell	DreamHost	EMC
Ericsson	Fujitsu	Hitachi	Huawei	inwinSTACK	Juniper Networks
Mirantis	NEC	NetApp	Symantec	Virtuozzo	Yahoo Inc.

OpenStack Core Services

SWIFT
Object Storage

KEYSTONE
Identity

NOVA
Compute

NEUTRON
Networking

CINDER
Block Storage

GLANCE
Image Service
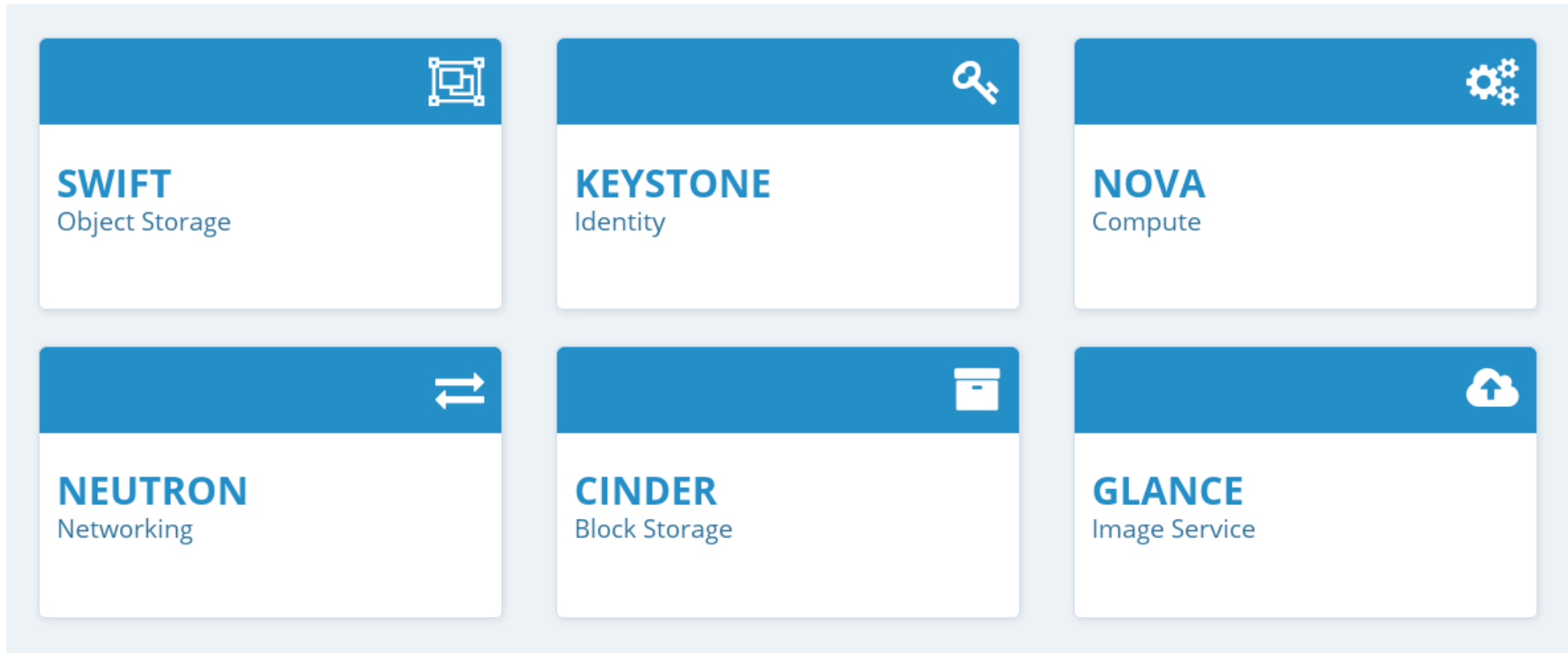
OpenStack Core Services (2)

- **Keystone (identity)**, centralized service for authentication and authorization of OpenStack services and for managing users, projects and roles

- **Neutron (networking)**, provide connectivity between the interfaces of OpenStack services

- **Glance (image)**, registry service that used to store resources such as VM images and volume snapshots

- **Nova (compute)**, manage and provisions Vms running on hypervisor nodes

- **Cinder (block storage)**, manage persistent block storage volumes for Vms

- **Swift (object storage)**, store and retrieve files and arbitrary data

OpenStack Optional Services

HORIZON
Dashboard

CEILOMETER
Telemetry

HEAT
Orchestration

TROVE
Database

SAHARA
Elastic Map Reduce

IRONIC
Bare-Metal Provisioning

ZAQAR
Messaging Service

MANILA
Shared Filesystems

DESIGNATE
DNS Service

BARBICAN
Key Management

MAGNUM
Containers

MURANO
Application Catalog

CONGRESS
Governance

OpenStack Optional Services (2)

- **Horizon (dashboard)**, web browser-based dashboard that used to manage OpenStack services

- **Ceilometer (telemetry)**, provides measurements of cloud resources

- **Heat (orchestration)**, template-based orchestration engine that supports automatic creation of resource stacks

- **Manila (shared FS)**, provides file storage to a VMs.

- **Ironic (bare metal provisioning)**, provision physical or bare metal machines.

- **Trove (DBaaS)**, allow users to select, provision, operate and administrate variety of relation and non-relation databases.

- **Sahara (data processing)**, provisioning and management of Hadoop clusters on OpenStack

OpenStack Version

Series	Status	Release Date	EOL
Pike	Future Development		
Ocata	Under Development	2017-02-22	
Newton	Stable	2016-10-06	
Mitaka	Security Supported	2016-04-07	2017-04-10

OpenStack Distribution
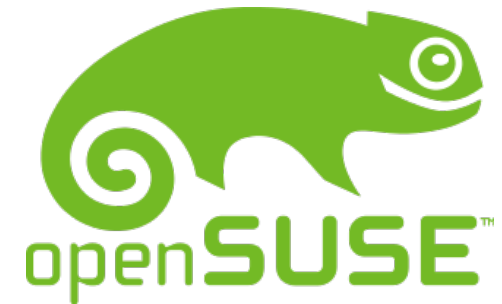
OpenStack Images

- Cirros: http://download.cirros-cloud.net

- CentOS: http://cloud.centos.org/centos/

- OpenSUSE: http://download.opensuse.org/repositories/Cloud:/Images:/

- Ubuntu: http://cloud-images.ubuntu.com

- Debian: http://cdimage.debian.org/cdimage/openstack/

- Windows Server: https://cloudbase.it/windows-cloud-images/

OpenStack Deployment Tools

- Devstack http://docs.openstack.org/developer/devstack/

- OpenStack Ansible https://github.com/openstack/openstack-ansible

- Packstack & Triple O: https://www.rdoproject.org/

- Juju OpenStack: https://jujucharms.com/openstack

- Crowbar: http://crowbar.github.io

- Fuel: https://www.fuel-infra.org

OpenStack Networking
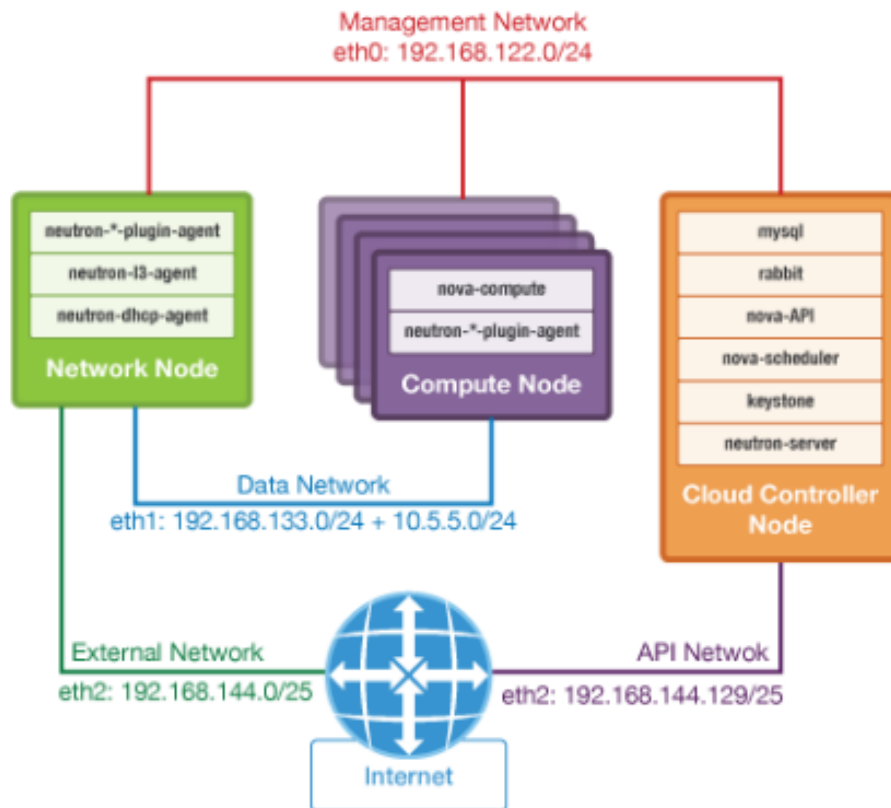
Next, we present a general overview of the networks present in **OpenStack Clouds**. We have:

- **Internal management network**: this is used by all the physical nodes to talk to each other.

- **Provider network**: this is GRE- or VLAN-based, used by VMs on different hosts to talk to each other.

- **External network**: the official, routable network to the Internet.

- **OAM network**: another official network for API access from external hosts; it can be the same as the External network.

Please note that **GRE** stands for **Generic Routing Encapsulation**. In contrast to other tunneling solutions, GRE does not offer any form of encryption. Don't confuse it with **IPsec** or other similar technologies.
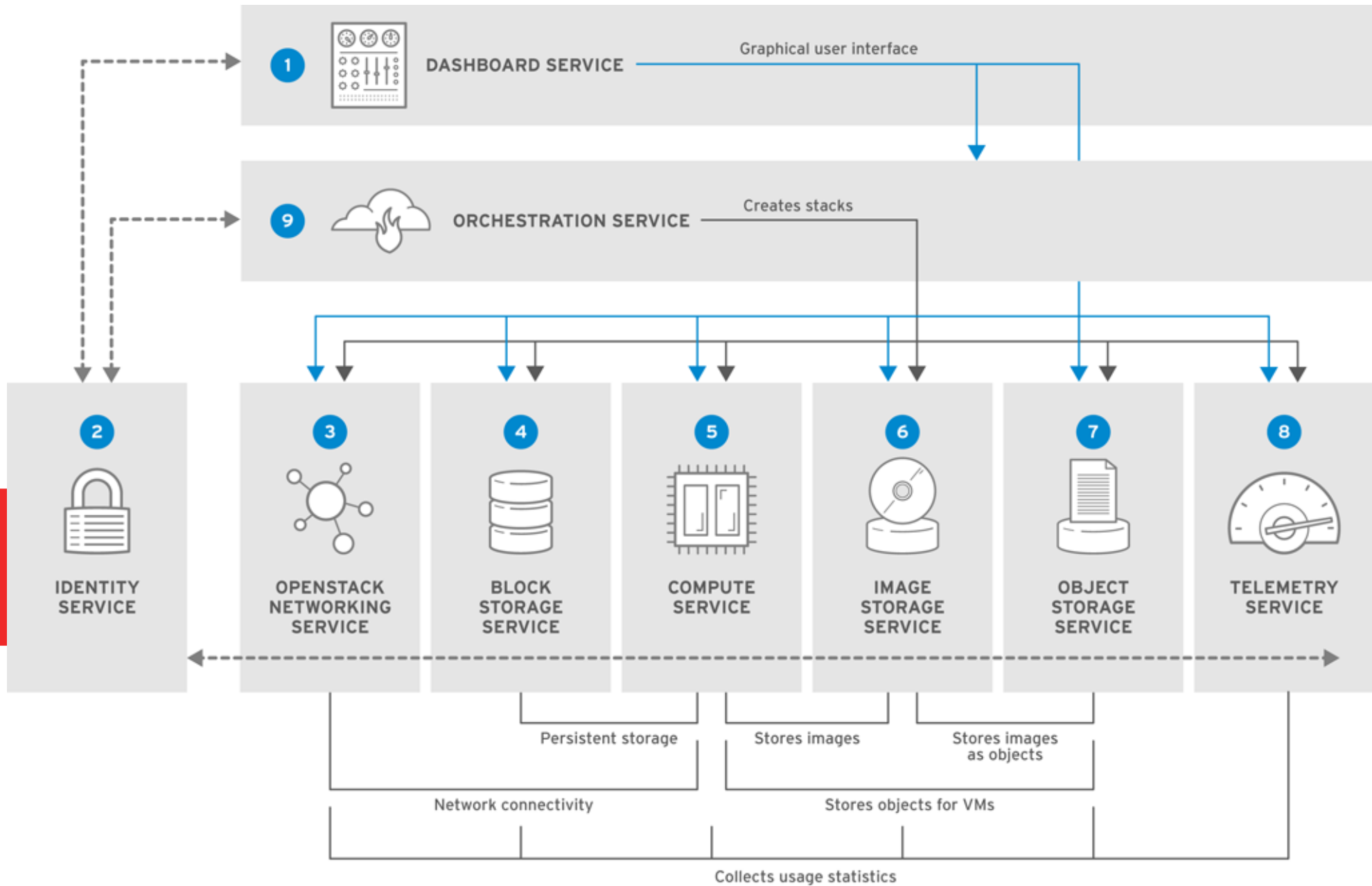
OpenStack Networking (2)
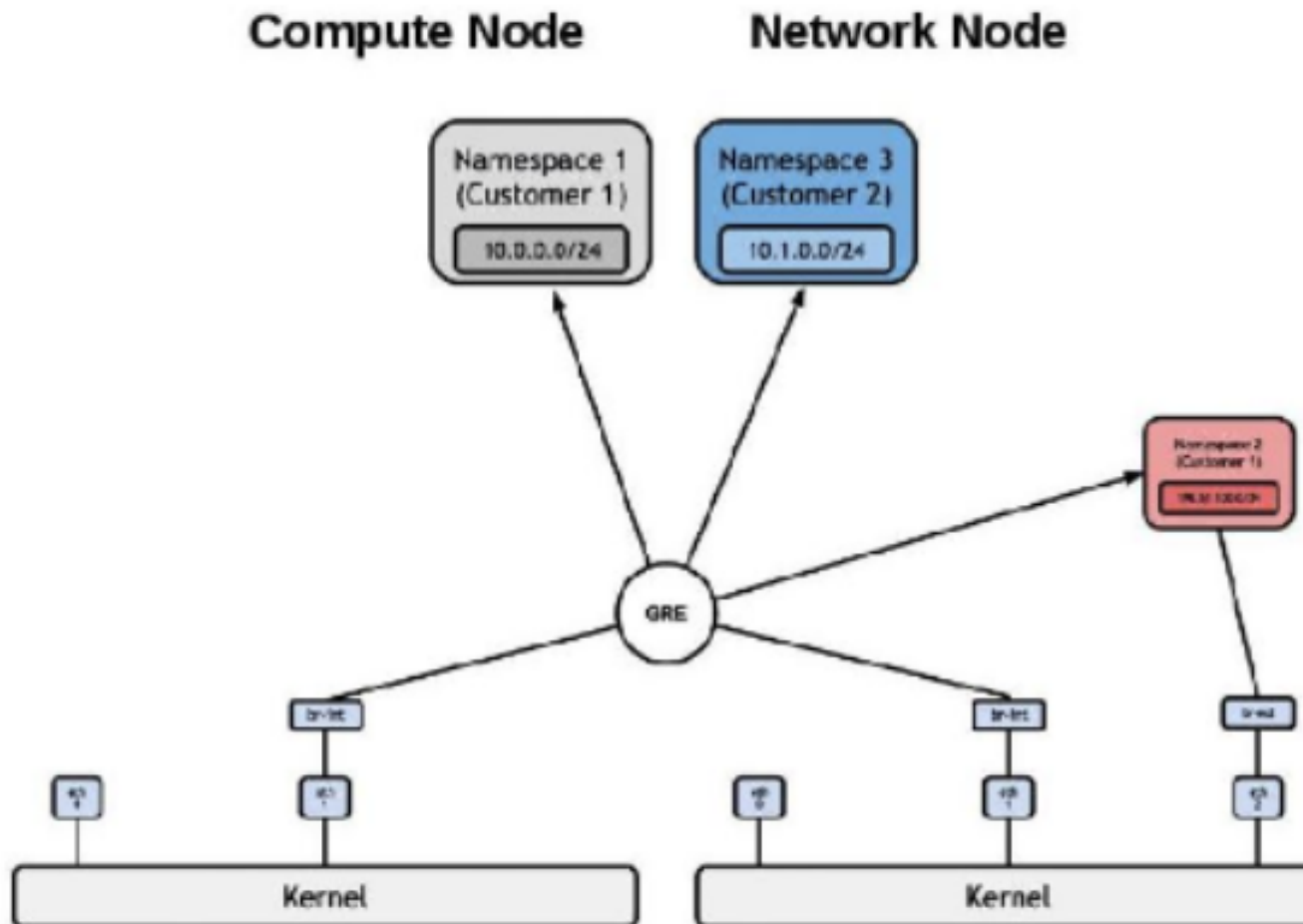
Prerequisite Services

- NTP: NTPD, Chrony

- MQ: RabbitMQ, zeroMQ

- SQL: MariaDB, MySQL, PostgreSQL

- NoSQL: MongoDB
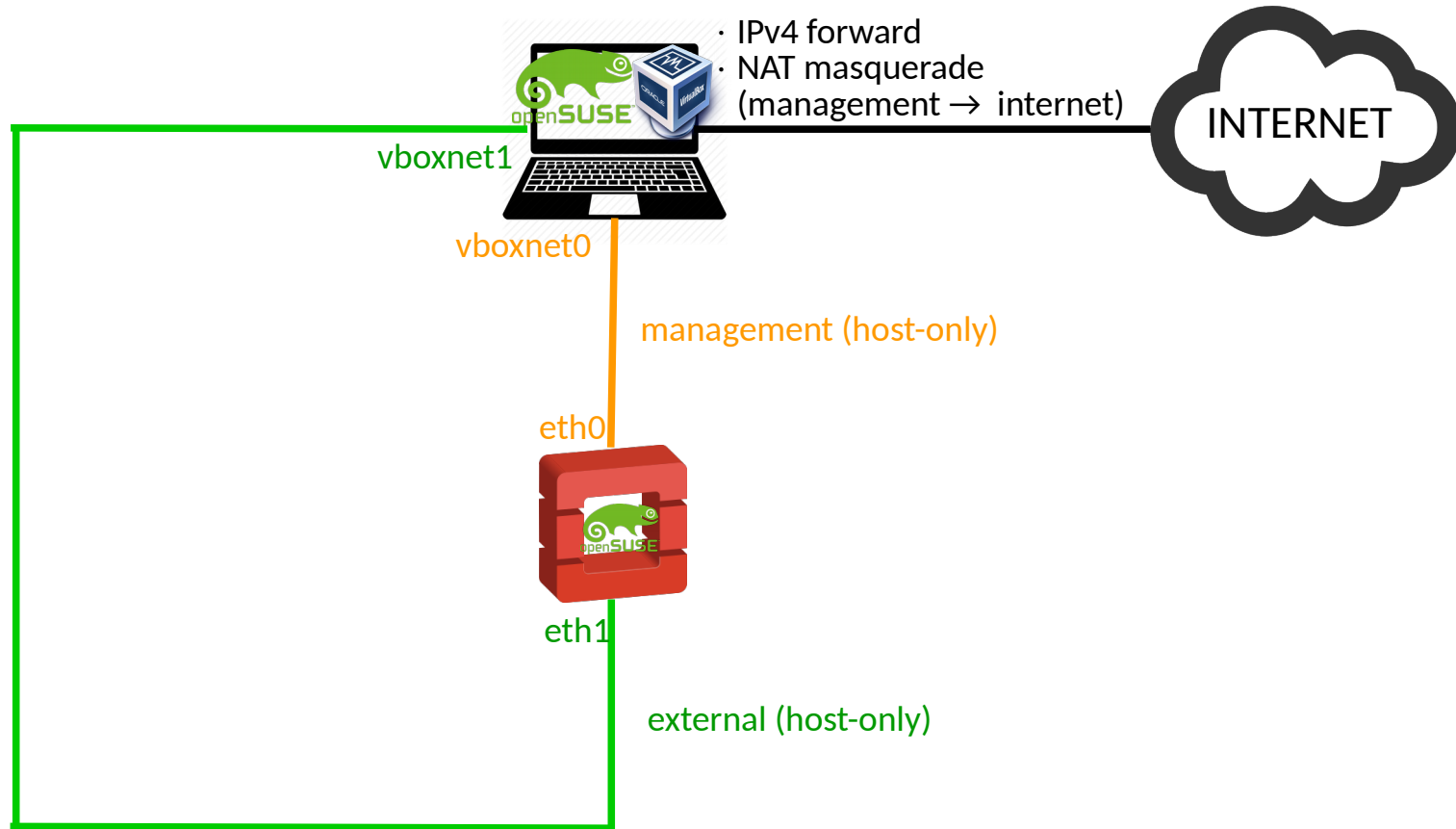
OpenStack Services Diagram

1 DASHBOARD SERVICE — Graphical user interface

9 ORCHESTRATION SERVICE — Creates stacks

2 IDENTITY SERVICE

3 OPENSTACK NETWORKING SERVICE

4 BLOCK STORAGE SERVICE

5 COMPUTE SERVICE

6 IMAGE STORAGE SERVICE

7 OBJECT STORAGE SERVICE

8 TELEMETRY SERVICE

Persistent storage

Stores images

Stores images as objects

Network connectivity

Stores objects for VMs

Collects usage statistics

RHELOSP_347192_1015

Lab I

Keystone, Neutron, Glance, Nova, Horizon

https://github.com/GLiBogor/leap42-newton-aio

Lab I Topology

- IPv4 forward
- NAT masquerade
  (management → internet)

INTERNET

vboxnet1

vboxnet0

management (host-only)

eth0

eth1

external (host-only)
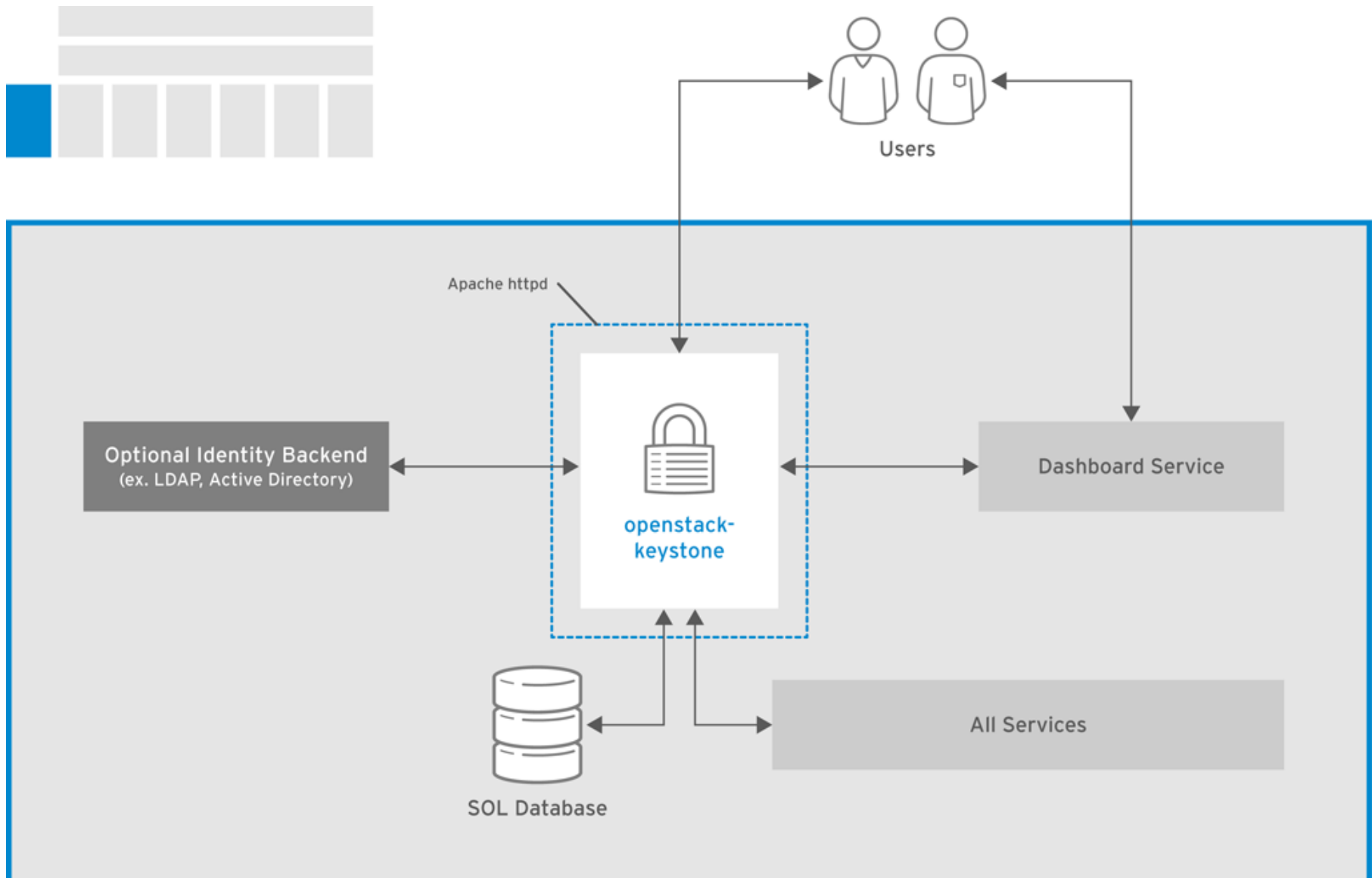
Keystone Components

- **Keystone server**, centralized server provide authentication and authorization services using RESTful interface.

- **Keystone driver**, accessing identity information in repositories external to OpenStack (SQL DB, LDAP, AD).

- **Keystone modules**, middleware modules run in the address space of the OpenStack component that is using the identity service.

Keystone Flow Diagram

Users

Apache httpd

openstack-keystone

Optional Identity Backend
(ex. LDAP, Active Directory)

Dashboard Service

SOL Database

All Services

OPENSTACK IDENTITY SERVICE

RHELOSP_347192_1015

Neutron Components

- **Neutron servers**, python daemon that manages user request and expose the networking API.

- **Neutron plugins**, specific set of networking technology/mechanisms to implement the networking API.

- **Neutron agents**, service that runs on each OpenStack node to perform local networking configuration for the node virtual machines and for networking services such as Open vSwitch.

Neutron Configuration Example
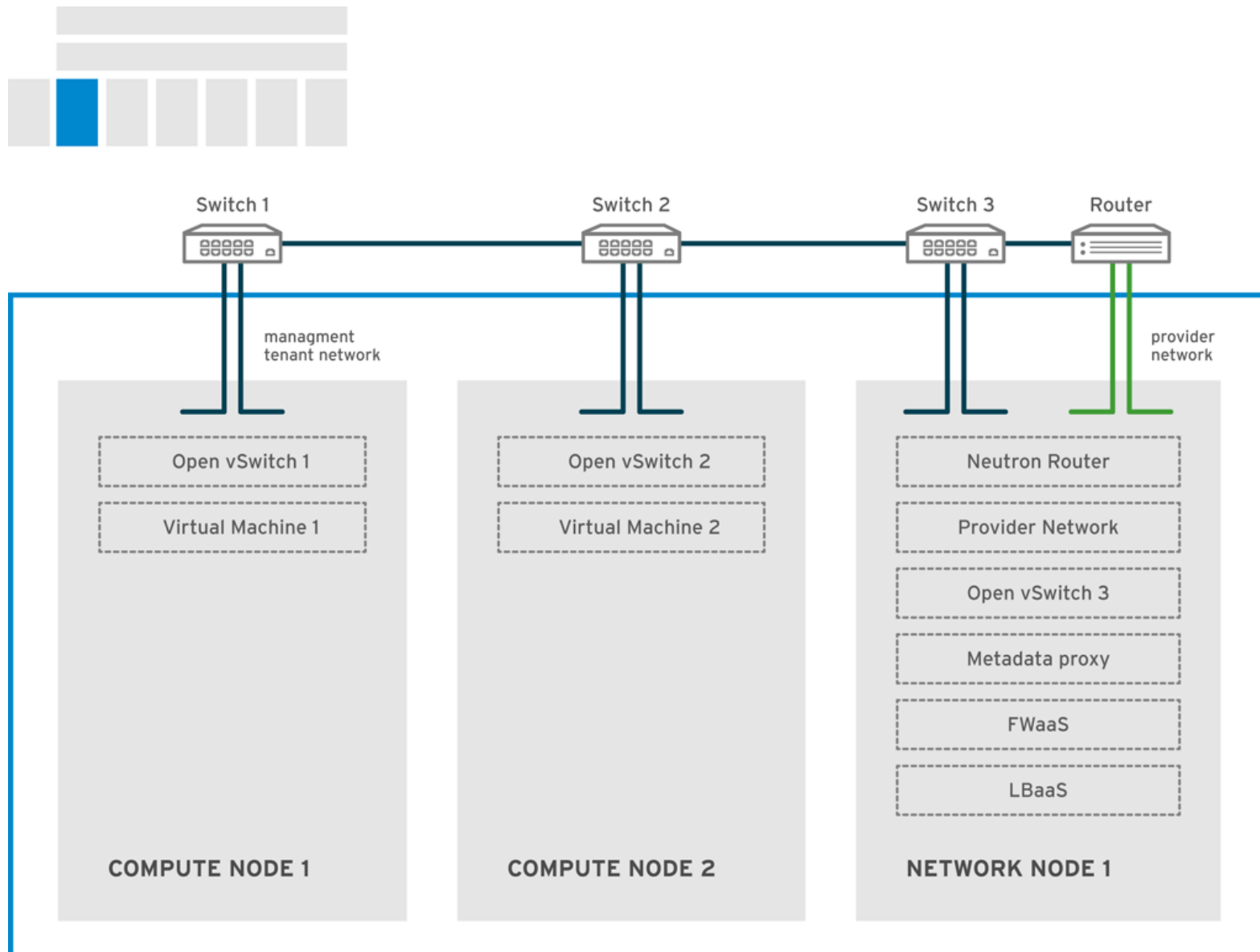
Glance Components

- **Glance API**, interacts with storage backends to handle requests for image retrieval and storage.

- **Glance registry**, manage all metadata for each image.

Glance Components Diagram
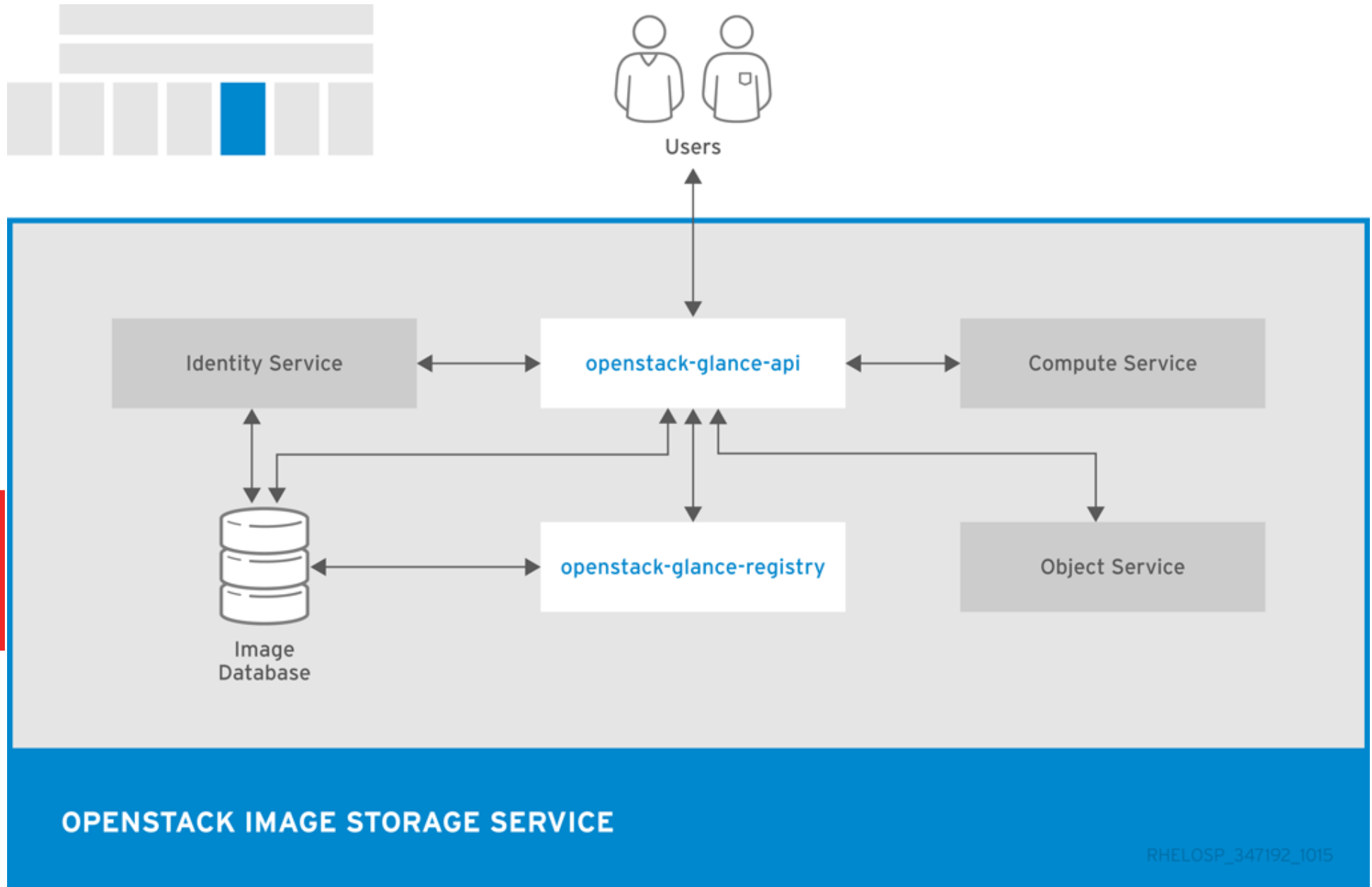

RHELOSP_347192_1015

Image Disk Formats

- aki/ami/ari, amazon kernel/machine/ramdisk image.

- iso, archive format for optical discs.

- qcow2, qemu/kvm support copy on write.

- raw, unstructed format

- vhd, hyper-v

- vdi, virtualbox

- vmdk, vmware

- bare, no metadata

- ova

- ovf

Nova Components

- **Nova API**, handles requests and provides access to the compute services.

- **Nova cert**, provide the certificate manager.

- **Nova compute**, run on each compute node to create and terminate instances.

- **Nova conductor**, provides database-access support for compute nodes to reduce security risks.

- **Nova consoleauth**, handles console authentication.

- **Nova novncproxy**, provides a VNC proxy for browser to enable consoles to access instances.

- **Nova scheduler**, dispatches requests for new instances to the correct node based on configured weights and filters/

Nova Components Diagram
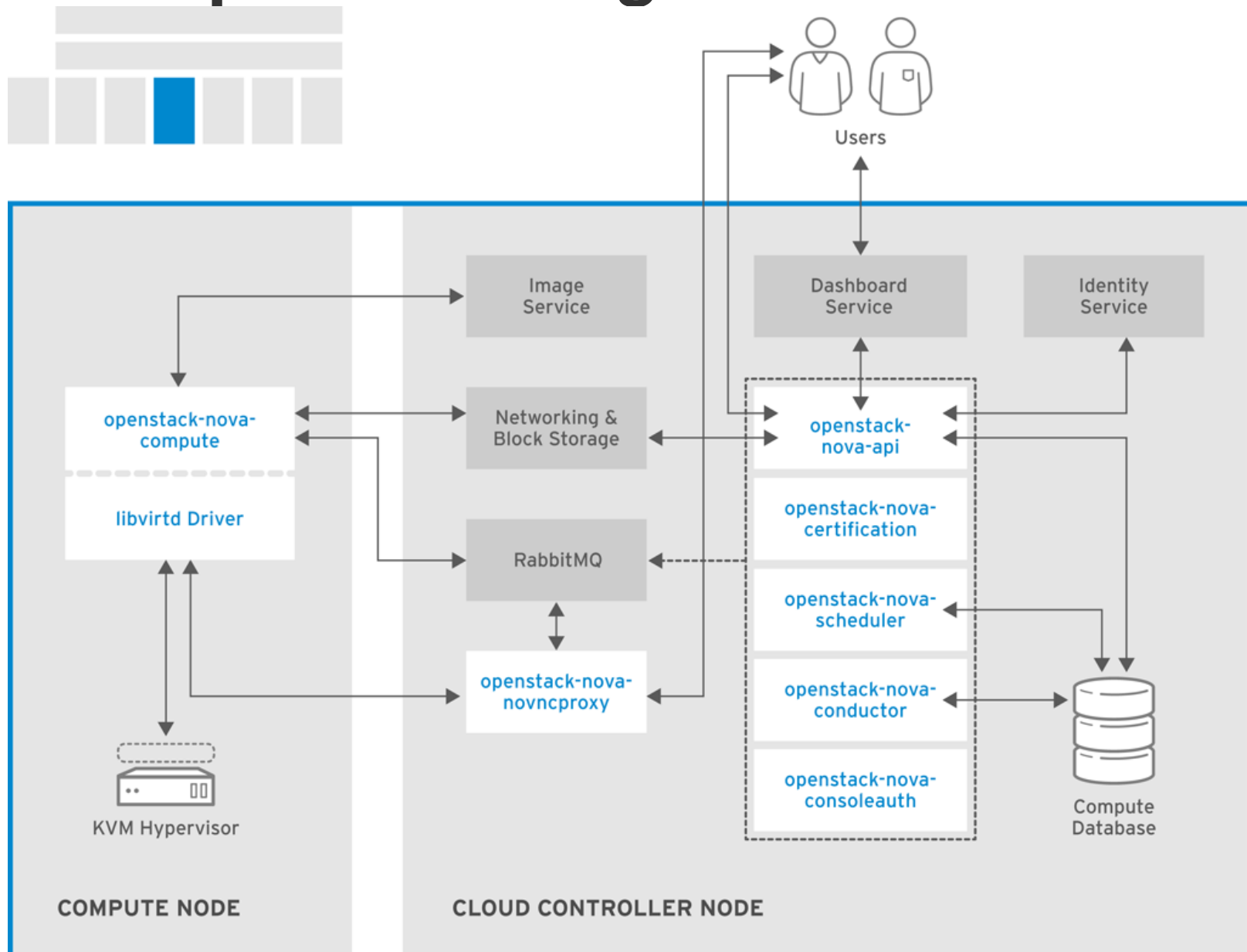
Horizon Interactions Diagram
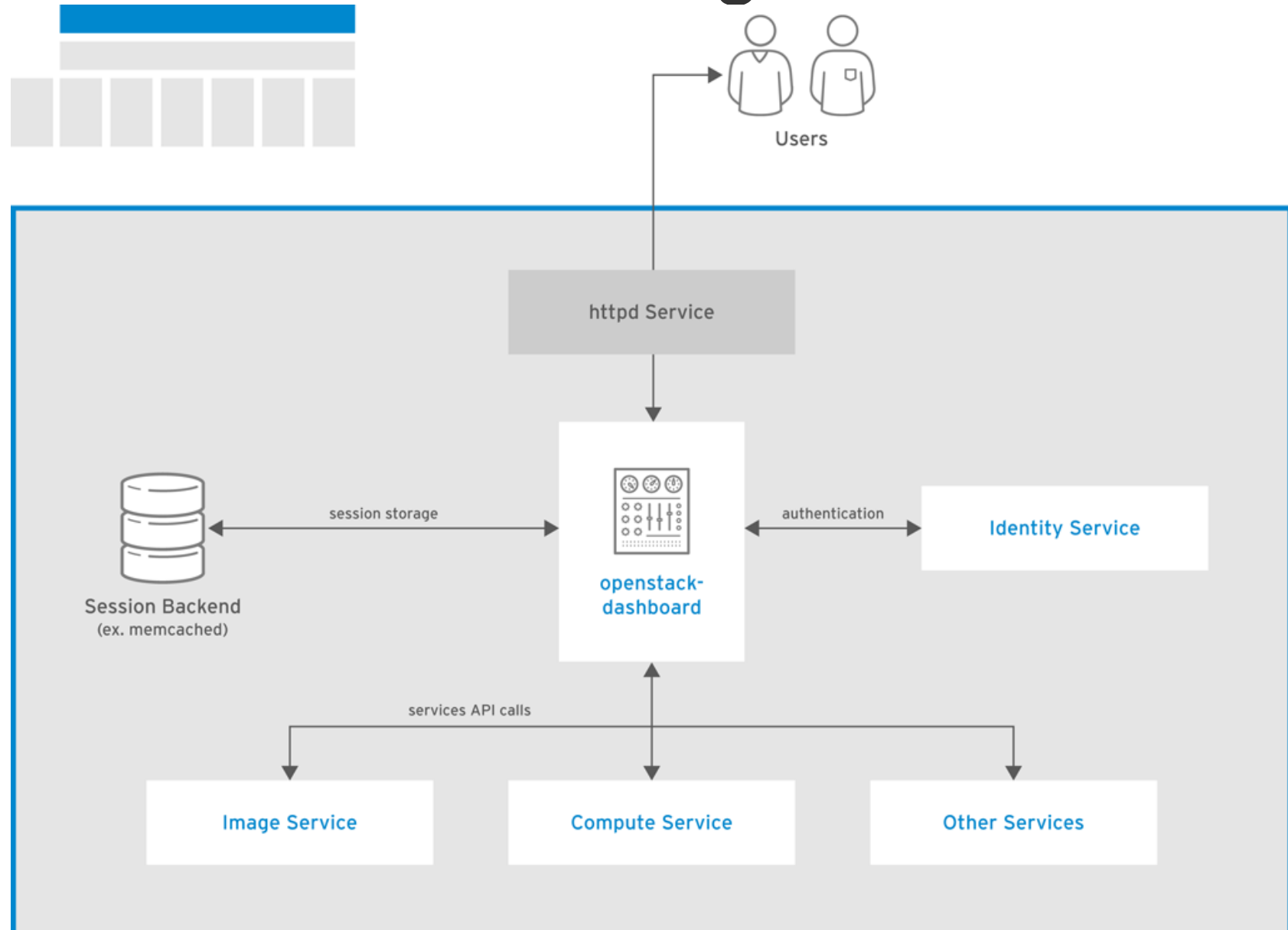
Horizon Tabs

- Project tab, view and manage the resources in a selected project

- Admin tab, administration tab to view usage, manage instances, volumes, flavors, images, networks and so on.

- Identity tab, view and manage projects and users.

- Settings tab, view and manage dashboard settings.

Horizon Project Tab

Horizon Admin Tab

Horizon Identity Tab

Horizon Settings Tab

Lab II

Cinder, Swift

https://github.com/GLiBogor/leap42-newton-aio

Lab II Topology

- IPv4 forward
- NAT masquerade
  (management → internet)

INTERNET

vboxnet1

vboxnet0

management (host-only)

eth0

eth1

external (host-only)
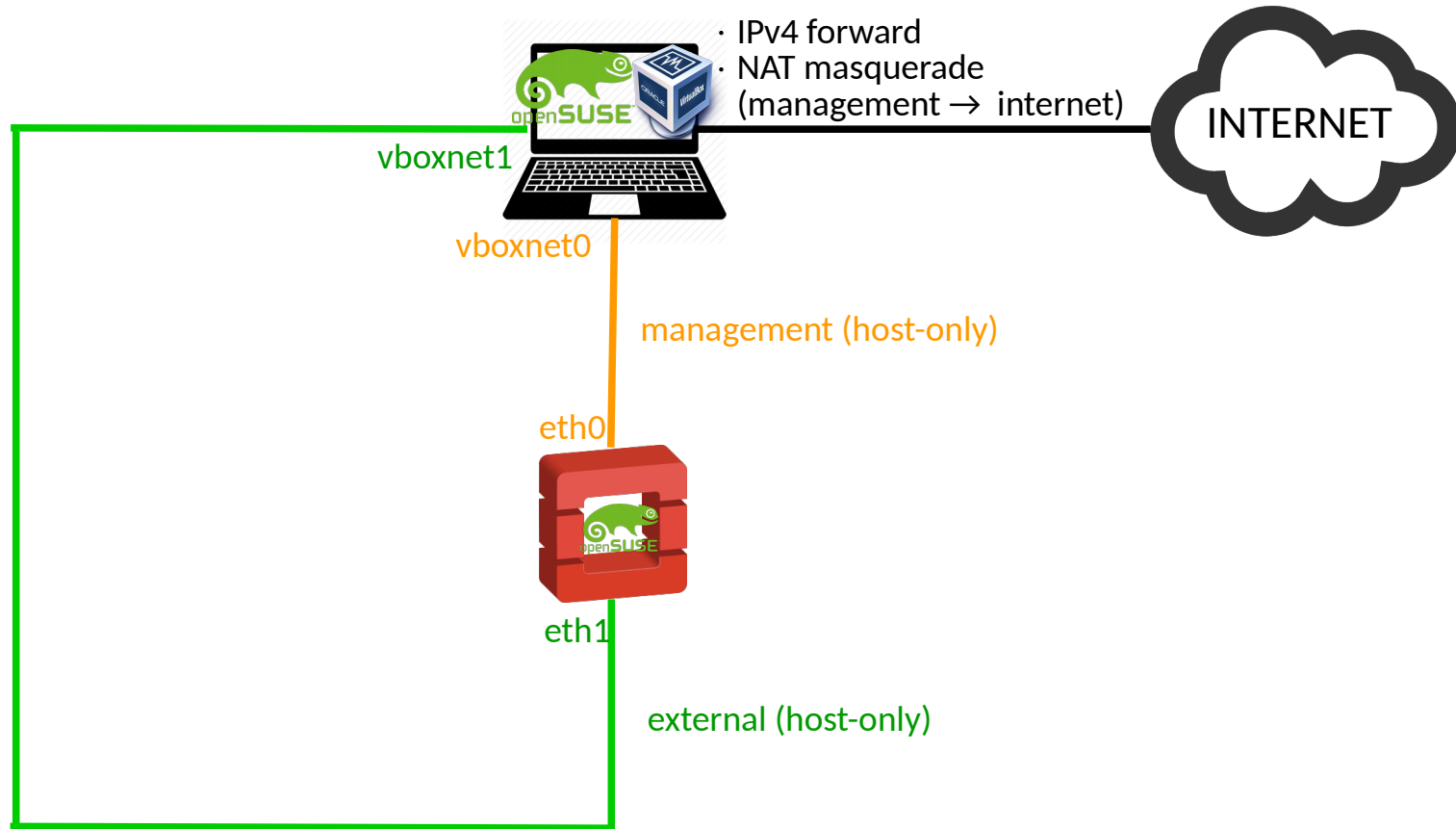
Cinder Components

- **Cinder API**, responds to request and places them in the message queue.

- **Cinder backup**, backup a block storage volume to an external storage repository.

- **Cinder scheduler**, assigns tasks to the queue and determines the provisioning volume server.

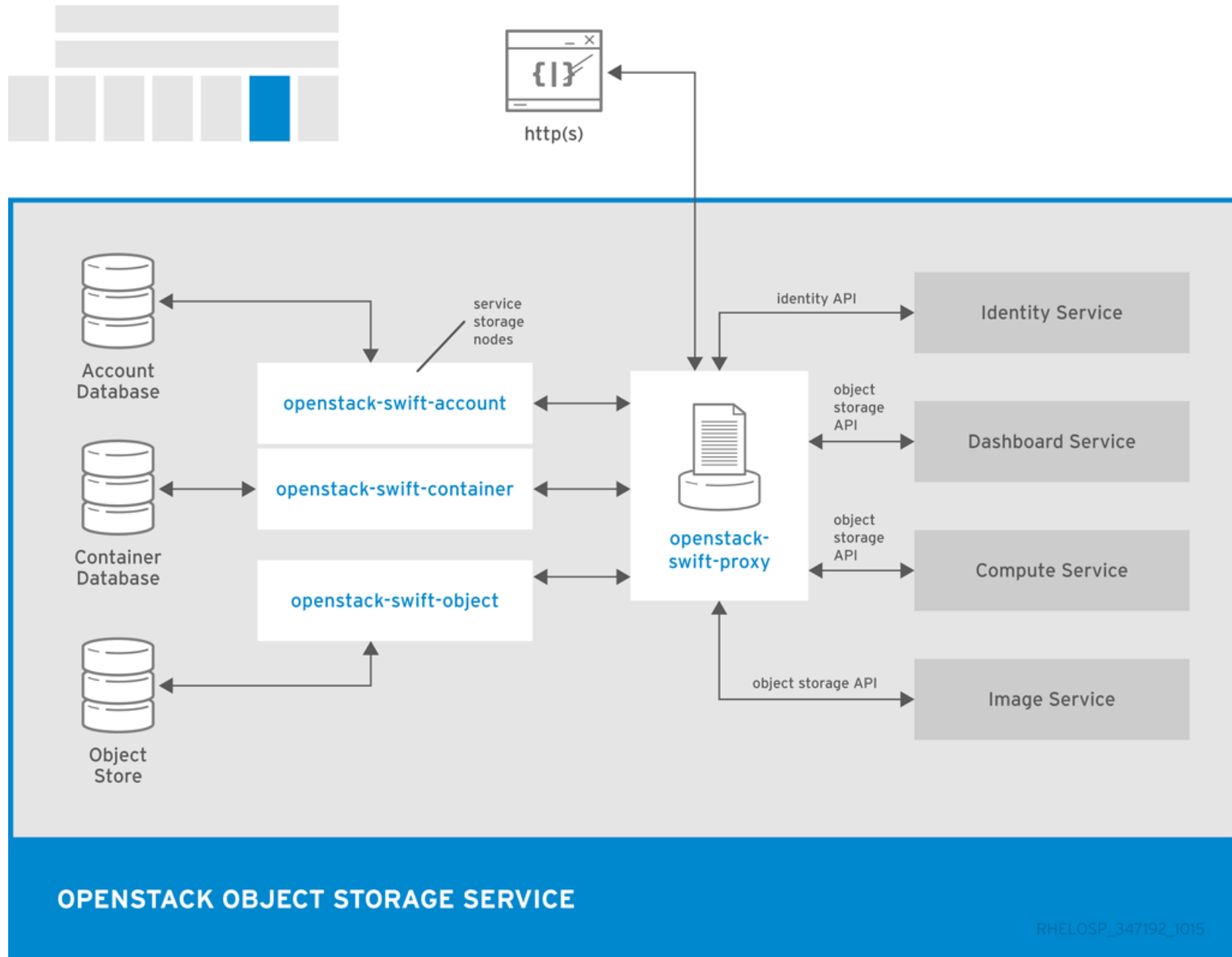- **Cinder volume**, designates storage for VMs.

Cinder Components Diagram

OPENSTACK BLOCK STORAGE SERVICE

RHELOSP_347192_1015
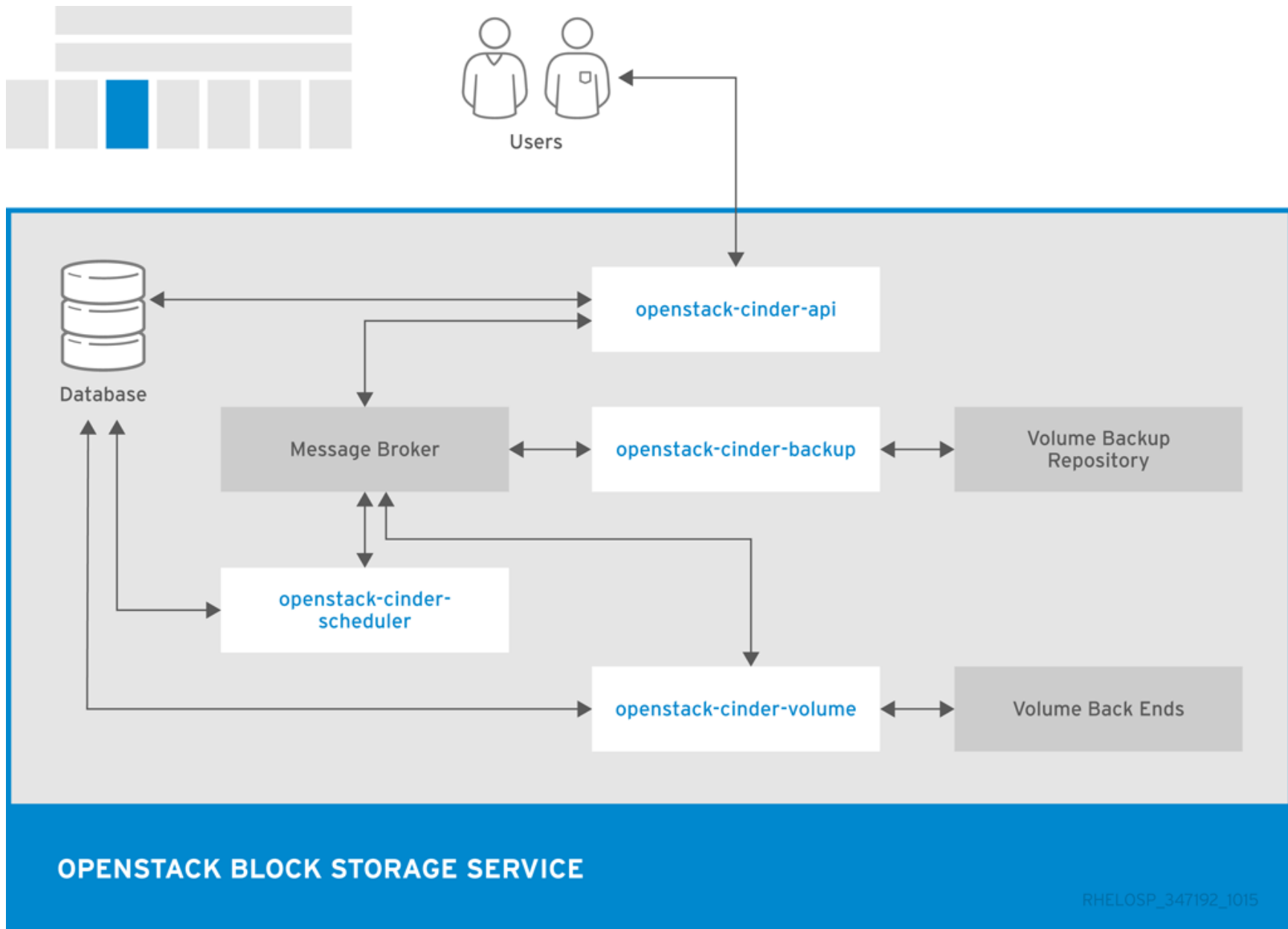
Swift Components

- **Swift account**, handles listing of containers with the account database.

- **Swift container**, handles listing of objects that are included in a specific container with the container database.

- **Swift object**, stores, retrieves, and delete objects.

- **Swift proxy**, expose the public API, provides authentication, and route requests.

- **Swift auditor**, verifies the integrity of accounts, containers and objects and protect against data corruption.

- **Swift replicator**, ensures consistent and available replication throughout the swift cluster including garbage collection

- **Swift updater**, identifies and retries failed updates.

Swift Components Diagram

https://www.linkedin.com/in/utianayuba
https://twitter.com/utianayuba
https://www.facebook.com/utianayuba