Cloud on TEIN
Part I: OpenStack Cloud Deployment

Vasinee Siripoonya
Electronic Government Agency of Thailand
Kasidit Chanchio
Thammasat University

Outline

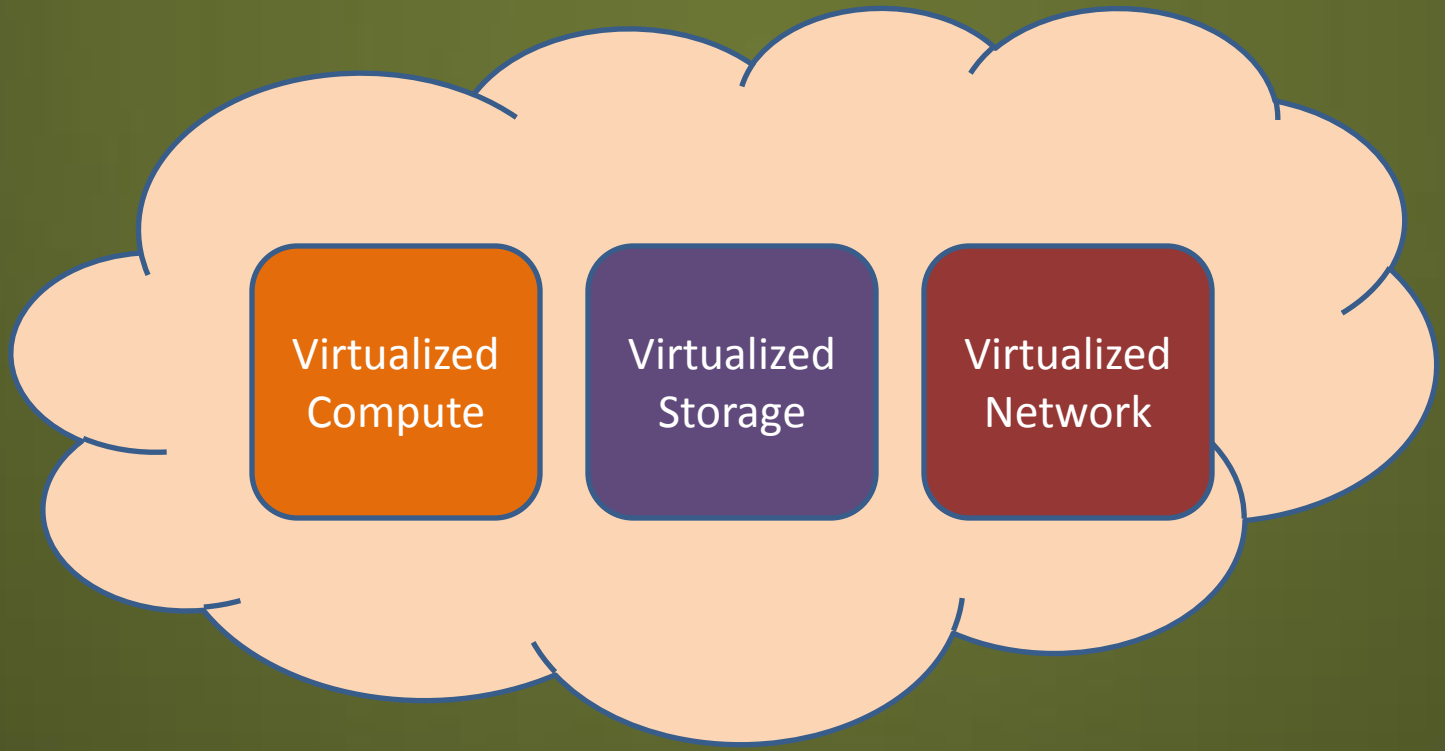
- Objectives
- Part I: OpenStack
  - Overview
  - How OpenStack components work
    - Keystone
    - Nova
    - Glance
- Part II: Demo
  - Use Cases

Objectives to build our private cloud

- Create a Cloud Computing Platform to support research at Thammasat University and partner organizations
- Accumulate practical knowledge and experiences on Cloud deployment and operations
- Study OpenStack Cloud OS in order to integrate our advanced Fault Resilient and Cloud management mechanisms to it

Cloud

- Distributed Systems that provide **Services** to users “on-demand”
- Focus on “Infrastructure As A **Service**” Cloud



Public and Private Cloud

Public Cloud:
- Available over Internet
- "Pay-per-use" basis
- Resources are shared by users from anywhere

Private Cloud:
- Available over organization's IT infrastructure
- Pay by organization
- Resources are shared by users in same organization

Cloud Layers

Applications

cloudstack
open source cloud computing
OpenNebula.org
The Open Source Solution for Data Center Virtualization

Cloud OS

openstack
CLOUD SOFTWARE

vmware
Xen

Virtualization/OS

KVM

Hardware/Storage/Network

Which Cloud OS should I use?

- Compatibility with your hypervisor/OS
  - Cloudstack comes from Citrix
  - OpenStack uses KVM by default. It has good support and documentation on Ubuntu
  - vCloud is definitely for vmware
- Maintainability
  - Provide means to fix the system when things go wrong
- Community Supports
- Etc.

Major OpenStack and CloudStack Supporters

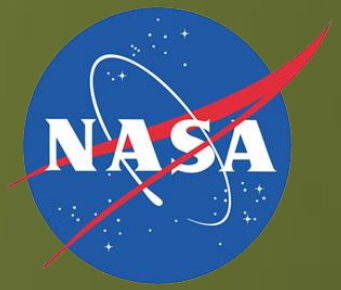
IT Vendors	OpenStack	CloudStack
Alcatel-Lucent		X
AMD	X	
Broadcom	X	
Brocade	X	X
Cisco	X	
Dell	X	
F5	X	
HP	X	
IBM	X	
Intel	X	X
Juniper	X	X
NEC	X	
NetApp	X	X
Red Hat	X	
Suse	X	
TrendMicro		X

Communications Service Providers	OpenStack	CloudStack
Akamai	X	
AT&T	X	
BT (British Telecom)		X
Deutsche Telekom	X	
Go Daddy		X
Internap	X	
KT (Korea Telecom)	X	X
NTT	X	X
Yahoo	X	

Source: DOMICITY LTD. – www.domicity.com

OpenStack® is an open and scalable cloud computing platform for building private and public clouds.

Invented by Rackspace and NASA.



The OpenStack project is provided under the Apache 2.0 license.

Participating Companies

Main Components

- OpenStack **Compute (Nova)**: Provision and manage large networks of virtual machines
- OpenStack **Object Storage (Swift)**: Create petabytes of secure, reliable storage using standard hardware
- OpenStack **Image Service (Glance)**: Catalog and manage massive libraries of server images

Main Components

- OpenStack **Dashboard (Horizon)** : a modular web-based user interface for all the OpenStack services.

- OpenStack **Identity Service (Keystone)** : authentication and authorization for all the OpenStack services.

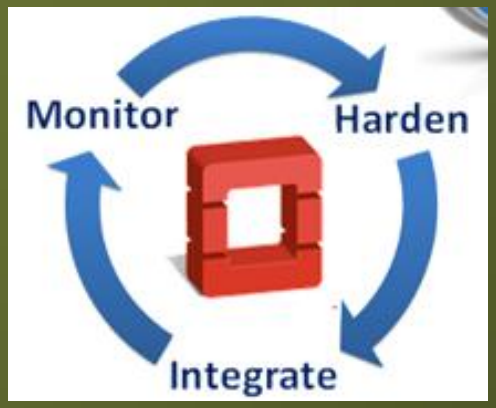
OpenStack Releases

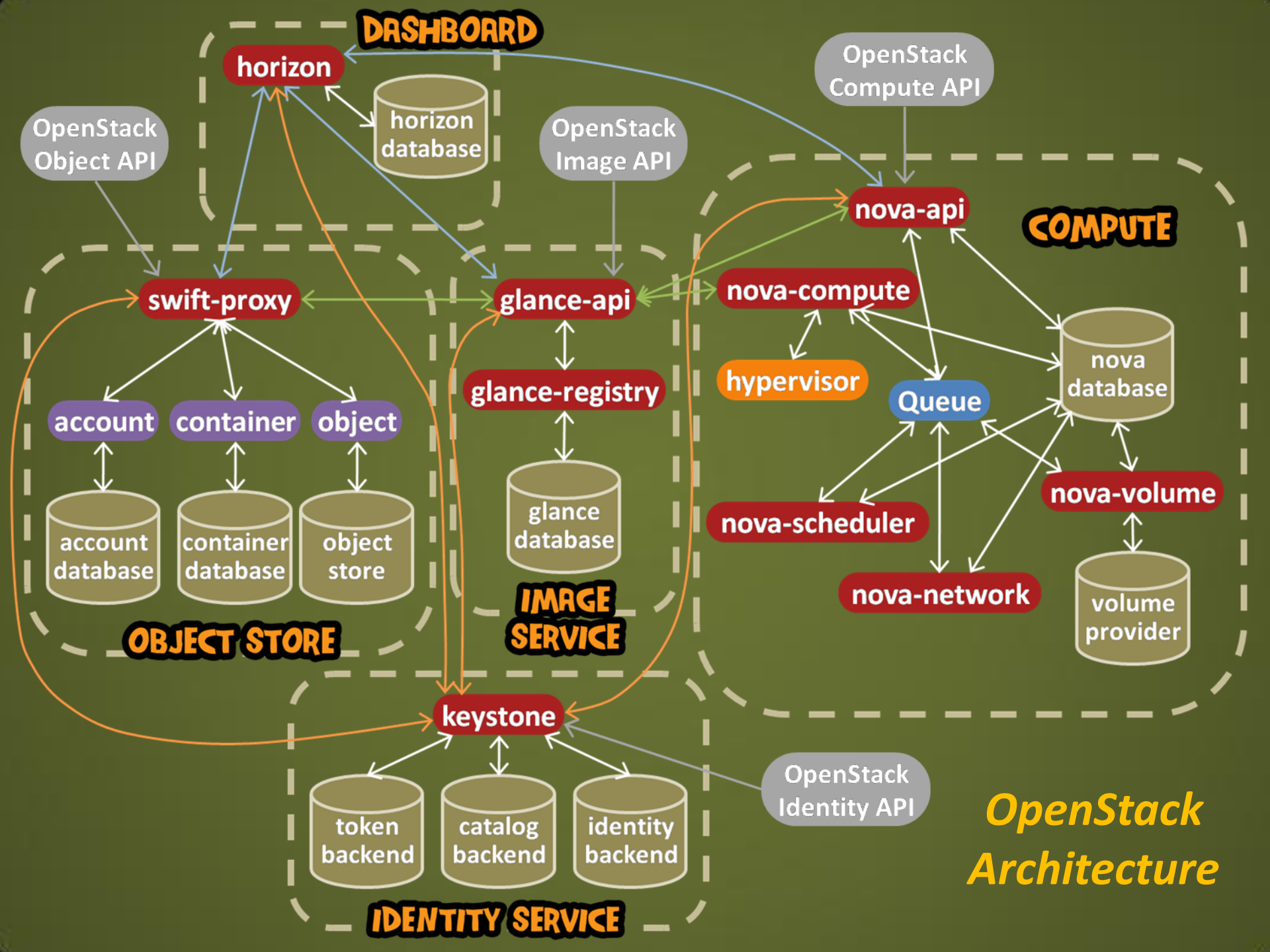
OpenStack isn't everything

Strategic Planning	Consultants, Business Process Automation
Operations	Engineers, Technicians, IT professionals, Network Experts
Systems	Servers, Firewall, Load-balancer, Operating Systems **OpenStack → Management Tools, Storage, Virtualization**
Facilities	Data Center, Network, Storage

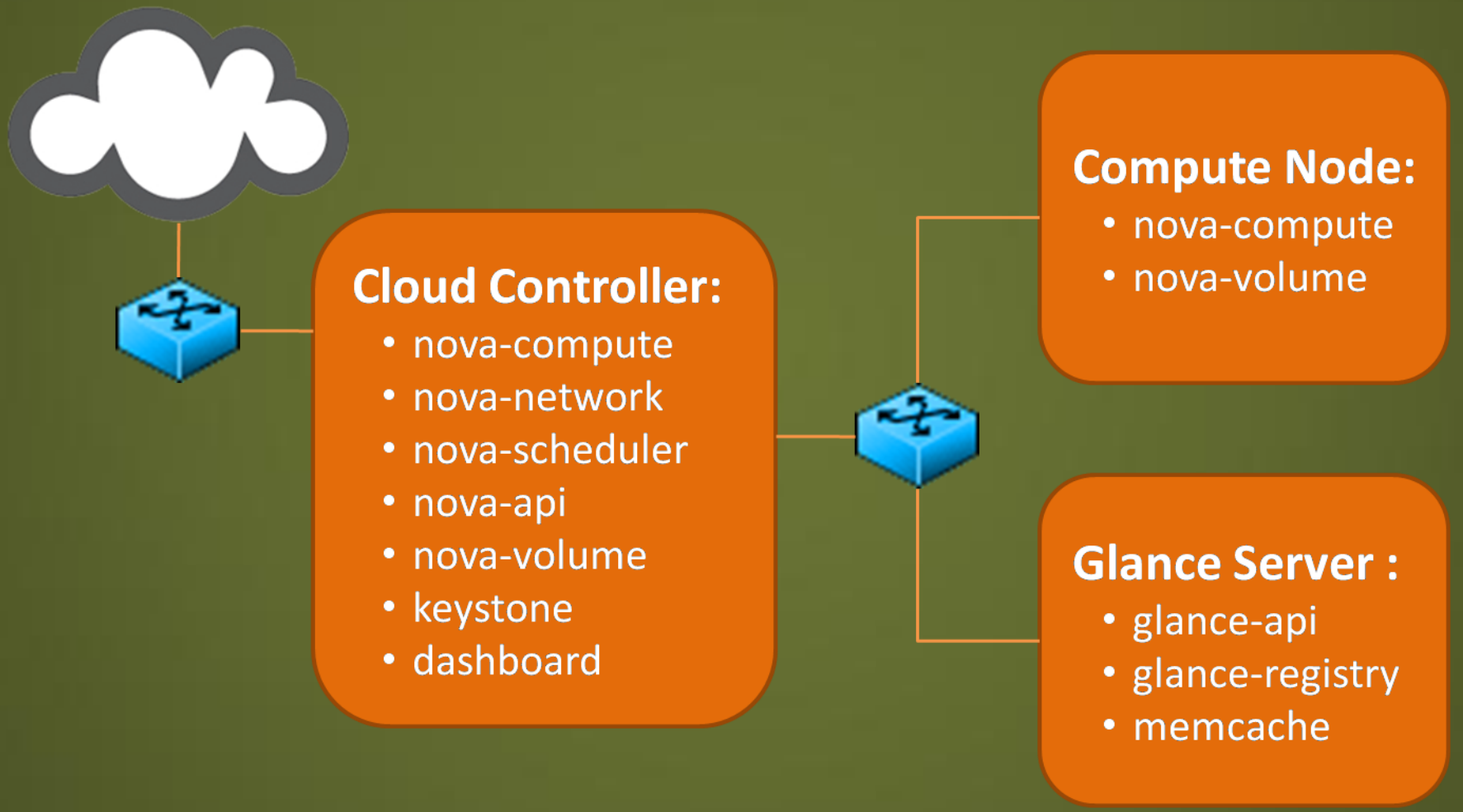
Hardening OpenStack Environments

- Restrict network and data access to least privilege
- Enable security features of underlying software
- Configure security features of underlying OS
- Harden the Hypervisor
- Use PKI for SSL
- Implement database security



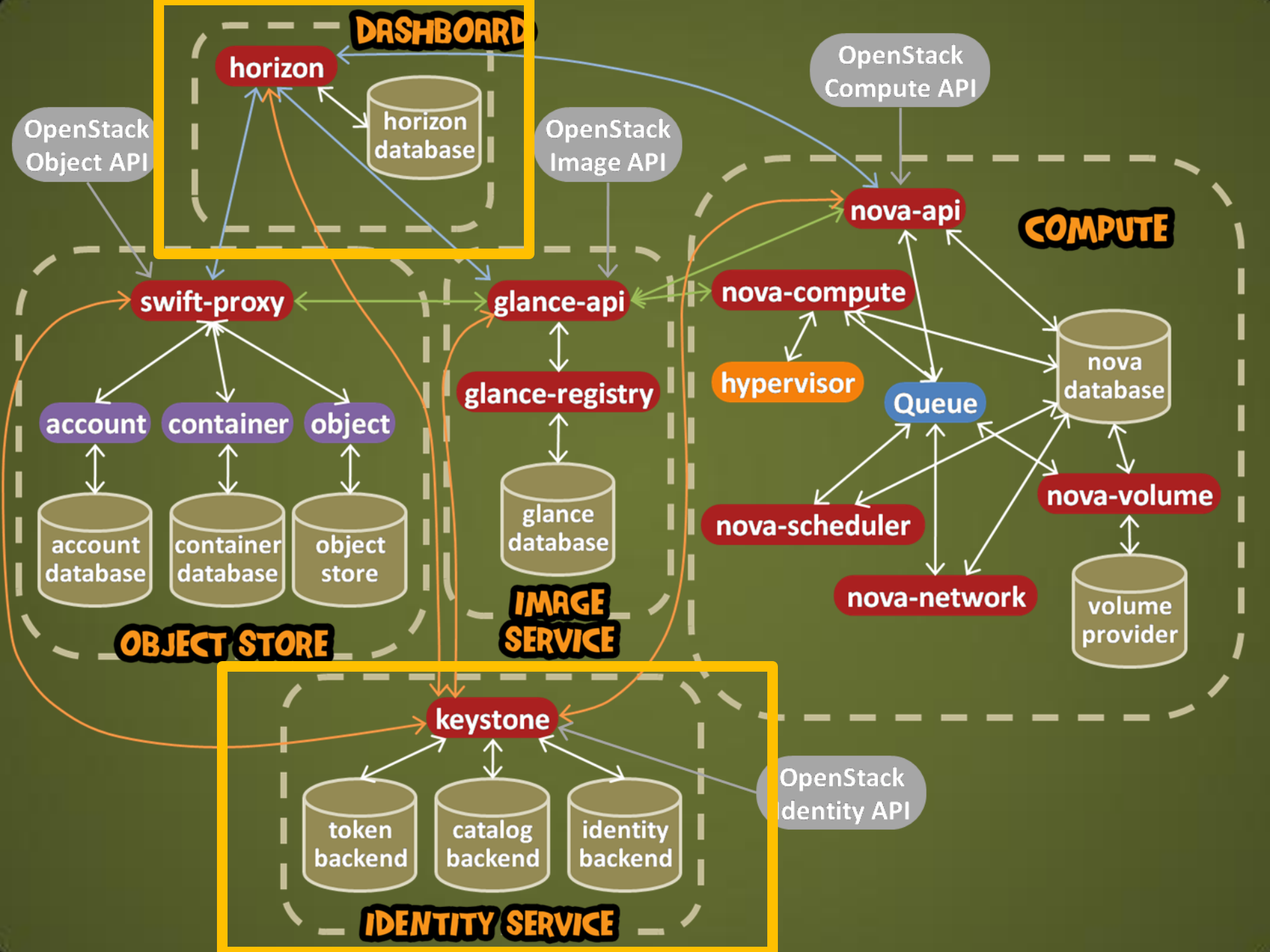

DASHBOARD
horizon
horizon database
OpenStack Object API
OpenStack Image API
OpenStack Compute API
nova-api
COMPUTE
swift-proxy
glance-api
nova-compute
hypervisor
Queue
nova database
nova-volume
volume provider
account
container
object
account database
container database
object store
OBJECT STORE
glance-registry
glance database
IMAGE SERVICE
nova-scheduler
nova-network
keystone
OpenStack Identity API
token backend
catalog backend
identity backend
IDENTITY SERVICE
OpenStack Architecture

SushiCloud's System Architecture



How OpenStack Components work

- Components in our focuses:
  - Keystone
  - Nova
  - Glance
- Networking Model
- Not currently cover
  - Swift


DASHBOARD
horizon
horizon database
OpenStack Object API
OpenStack Image API
OpenStack Compute API
nova-api
COMPUTE
swift-proxy
glance-api
nova-compute
hypervisor
Queue
nova database
glance-registry
account
container
object
account database
container database
object store
glance database
nova-volume
nova-scheduler
nova-network
volume provider
IMAGE SERVICE
OBJECT STORE
keystone
token backend
catalog backend
identity backend
OpenStack Identity API
IDENTITY SERVICE

Keystone

- A central authentication and authorization
- User represents someone or something that can gain access through Keystone. Users come with credentials that can be checked like passwords or API keys.
- Tenant represents what is called the project in Nova. Users are bound to a tenant by assigning them a role on that tenant.
- Role represents a number of privileges or rights a user has or actions they are allowed to perform.
- To access a service, we have to know its endpoint. So there are endpoint templates in Keystone that provide information about all existing endpoints of all existing services.

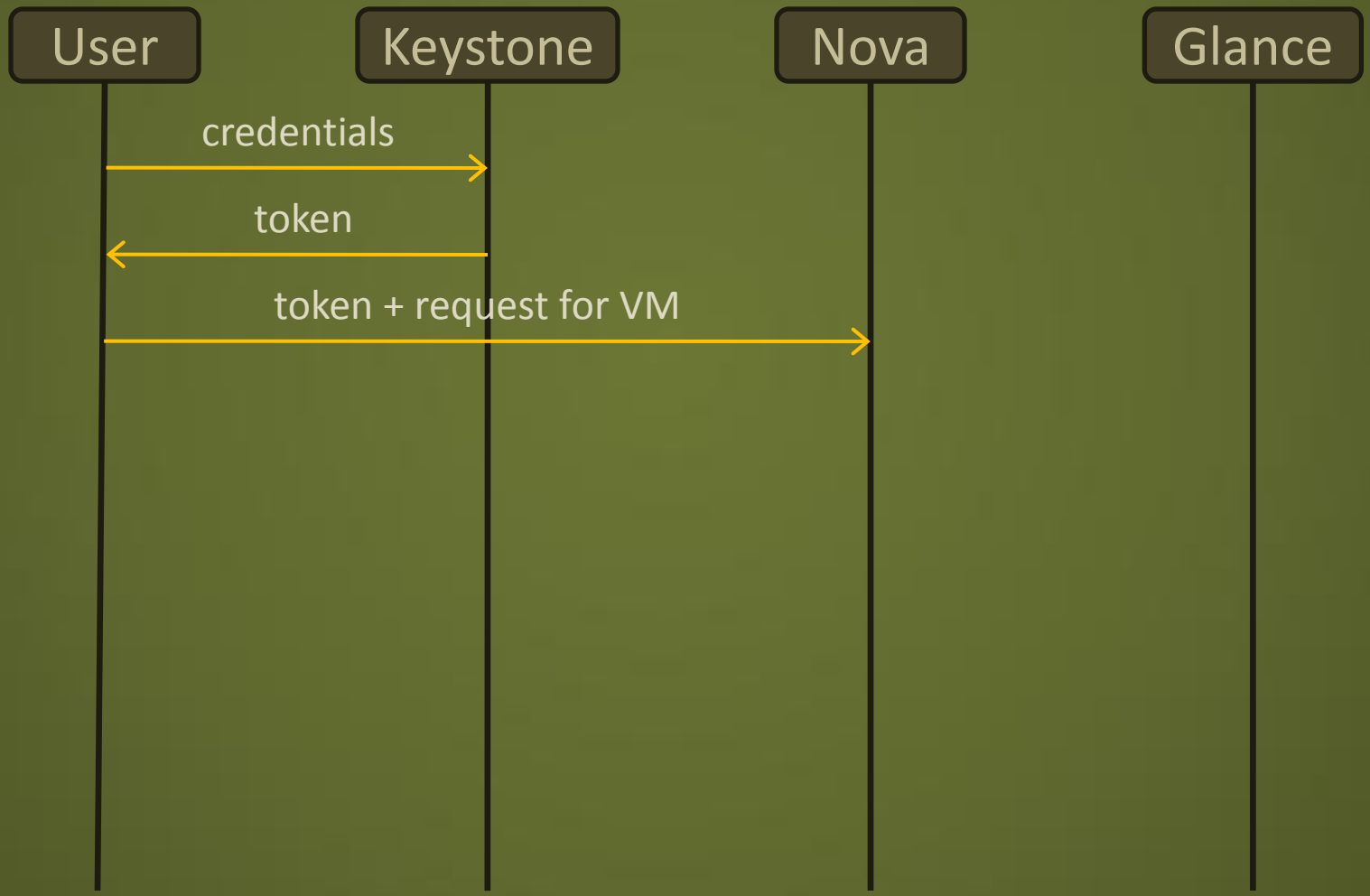
Keystone

- To access some service, users provide their credentials to Keystone and receive a token.
- If the user, for example, wants to spawn a new VM instance in Nova, one can find an URL to Nova in the list of endpoints provided by Keystone and send an appropriate request.
- After that, Nova verifies the validity of the token in Keystone and should create an instance from some image by the provided image ID and plug it into some network.
- All the way this token travels between services so that they can ask Keystone or each other for additional information or some actions.

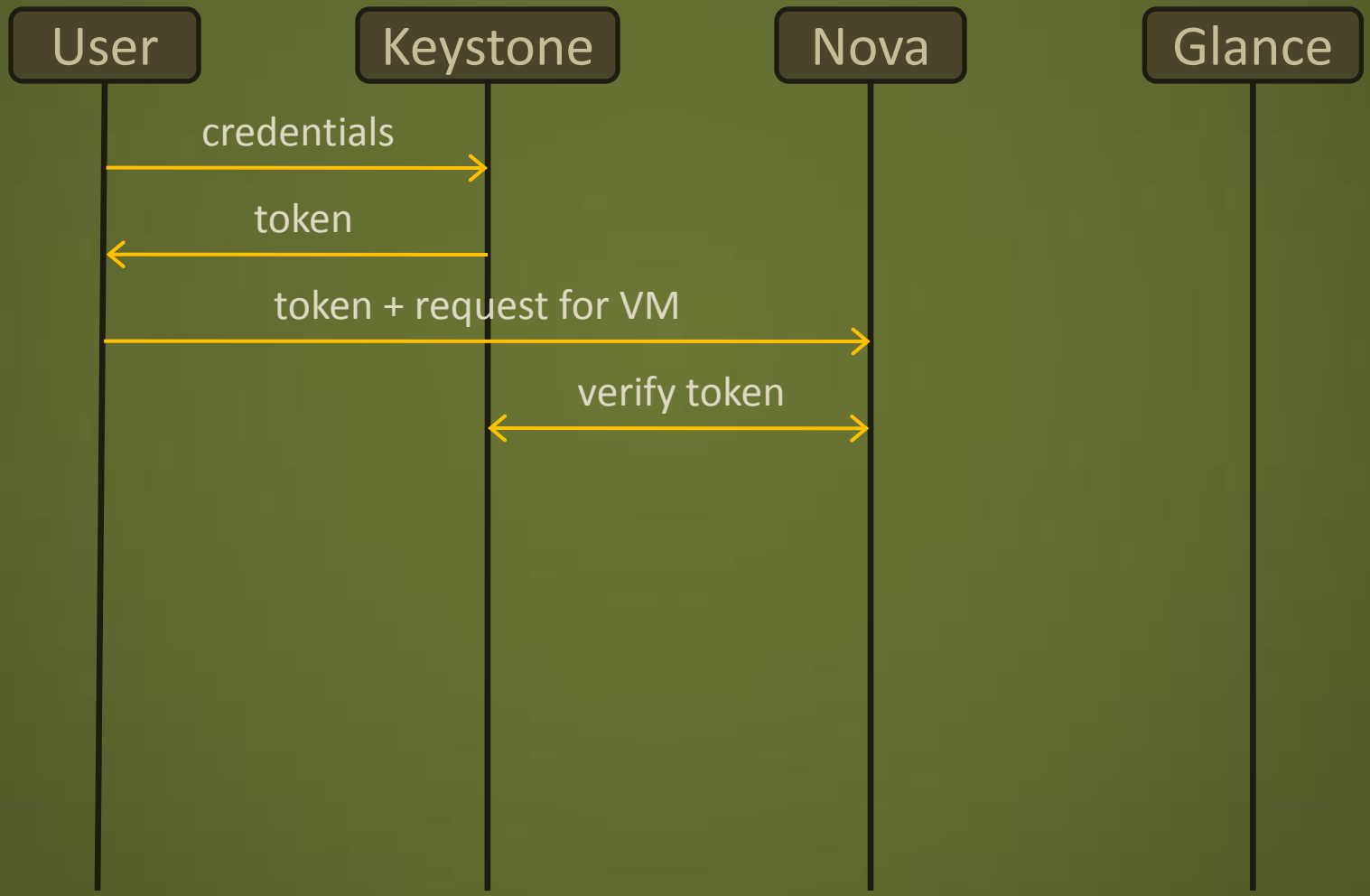
Keystone Control Flow

Keystone Control Flow

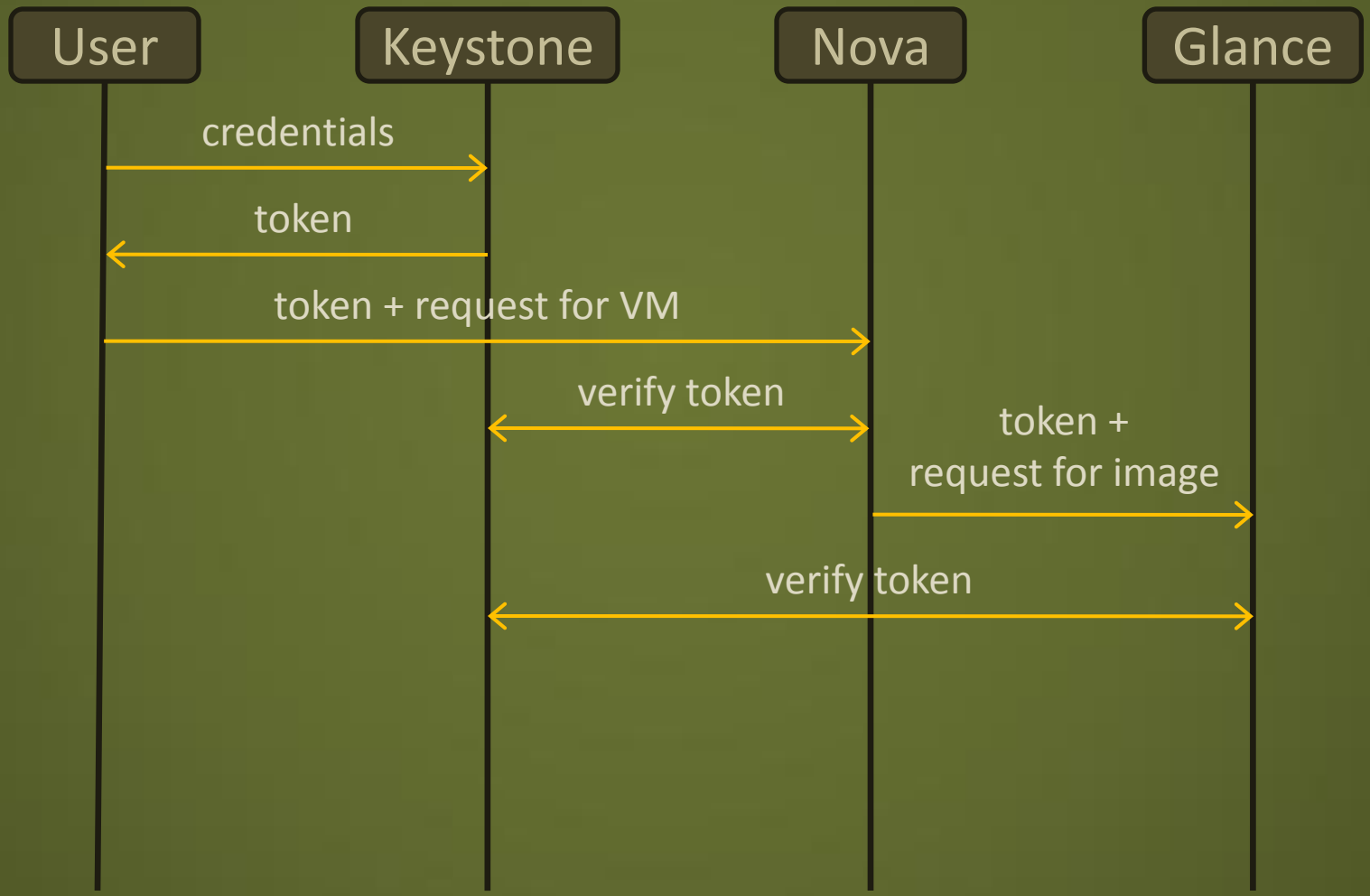
Keystone Control Flow



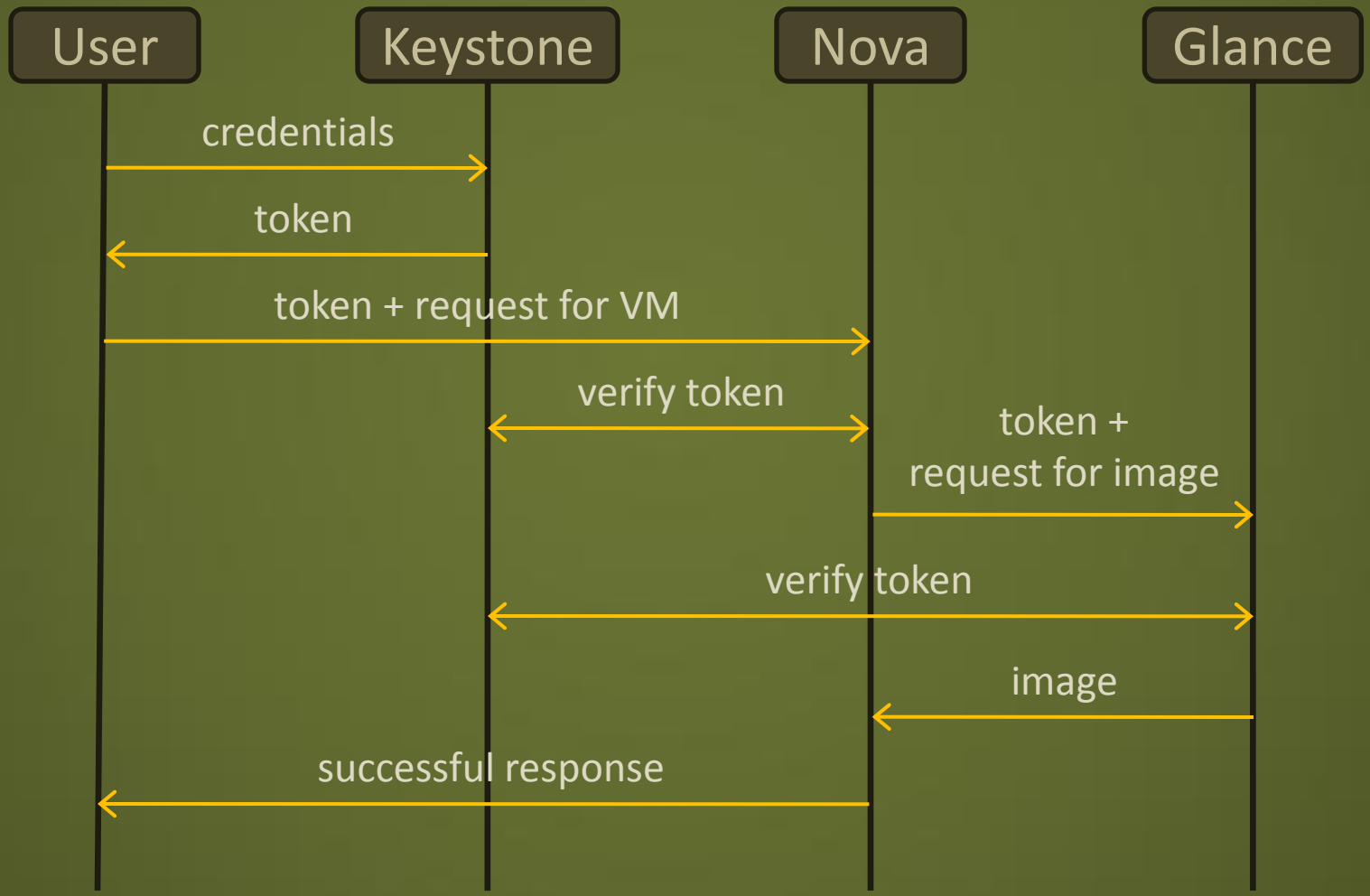
Keystone Control Flow

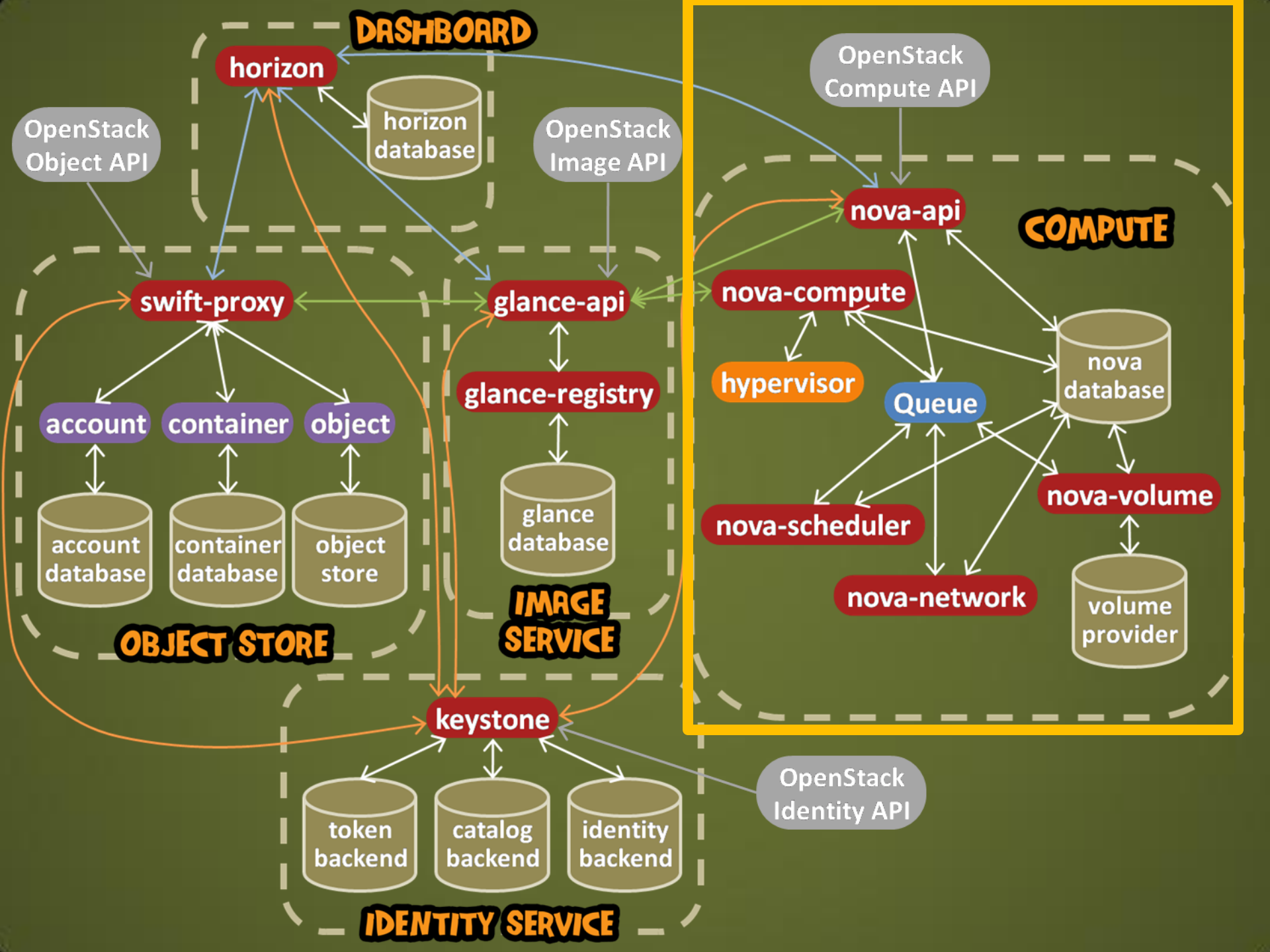


Keystone Control Flow



Keystone Control Flow



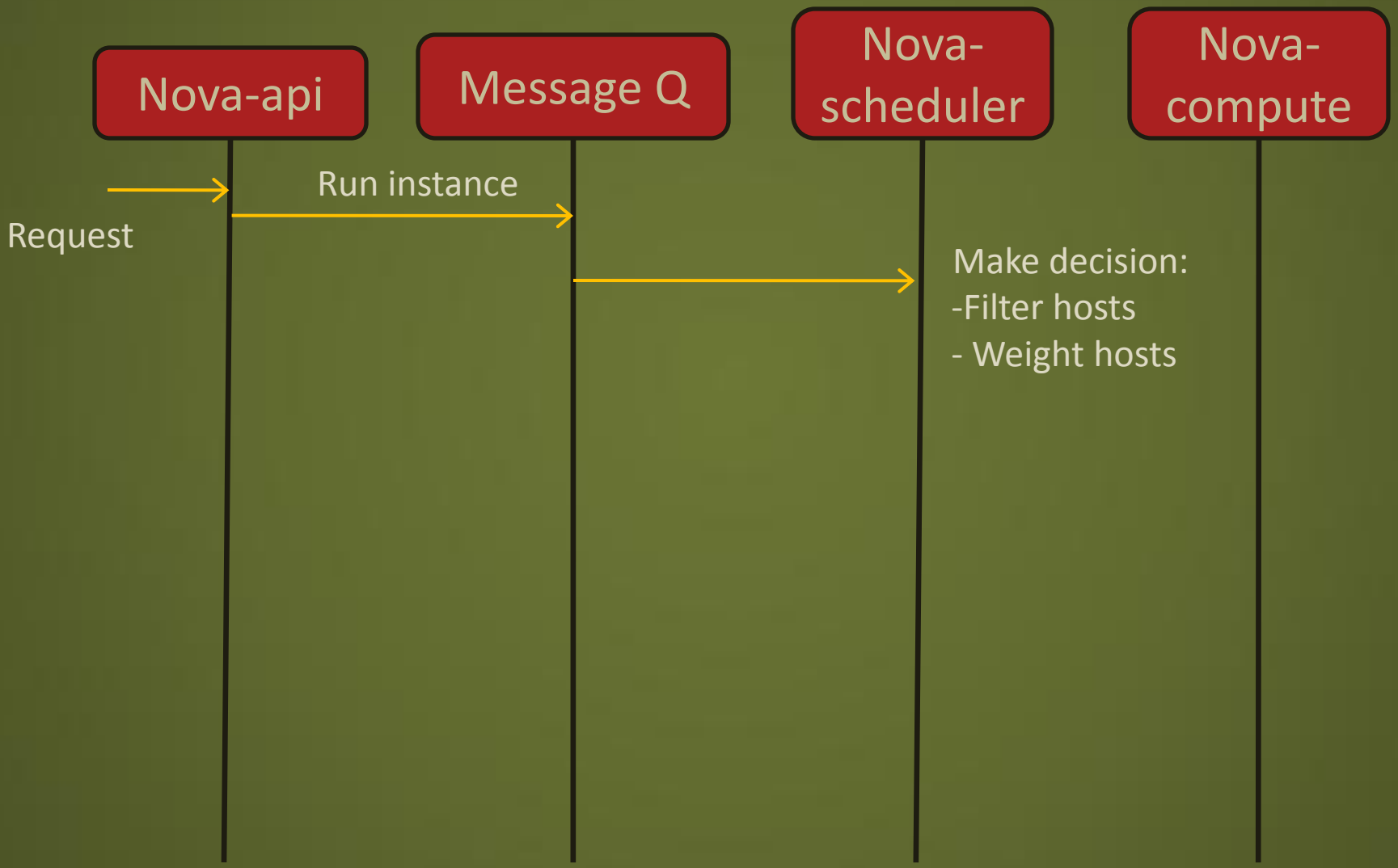

DASHBOARD
horizon
horizon database
OpenStack Object API
OpenStack Image API
OpenStack Compute API
COMPUTE
nova-api
swift-proxy
glance-api
nova-compute
hypervisor
Queue
nova database
nova-volume
nova-scheduler
nova-network
volume provider
glance-registry
account
container
object
account database
container database
object store
glance database
OBJECT STORE
IMAGE SERVICE
keystone
OpenStack Identity API
token backend
catalog backend
identity backend
IDENTITY SERVICE

Nova

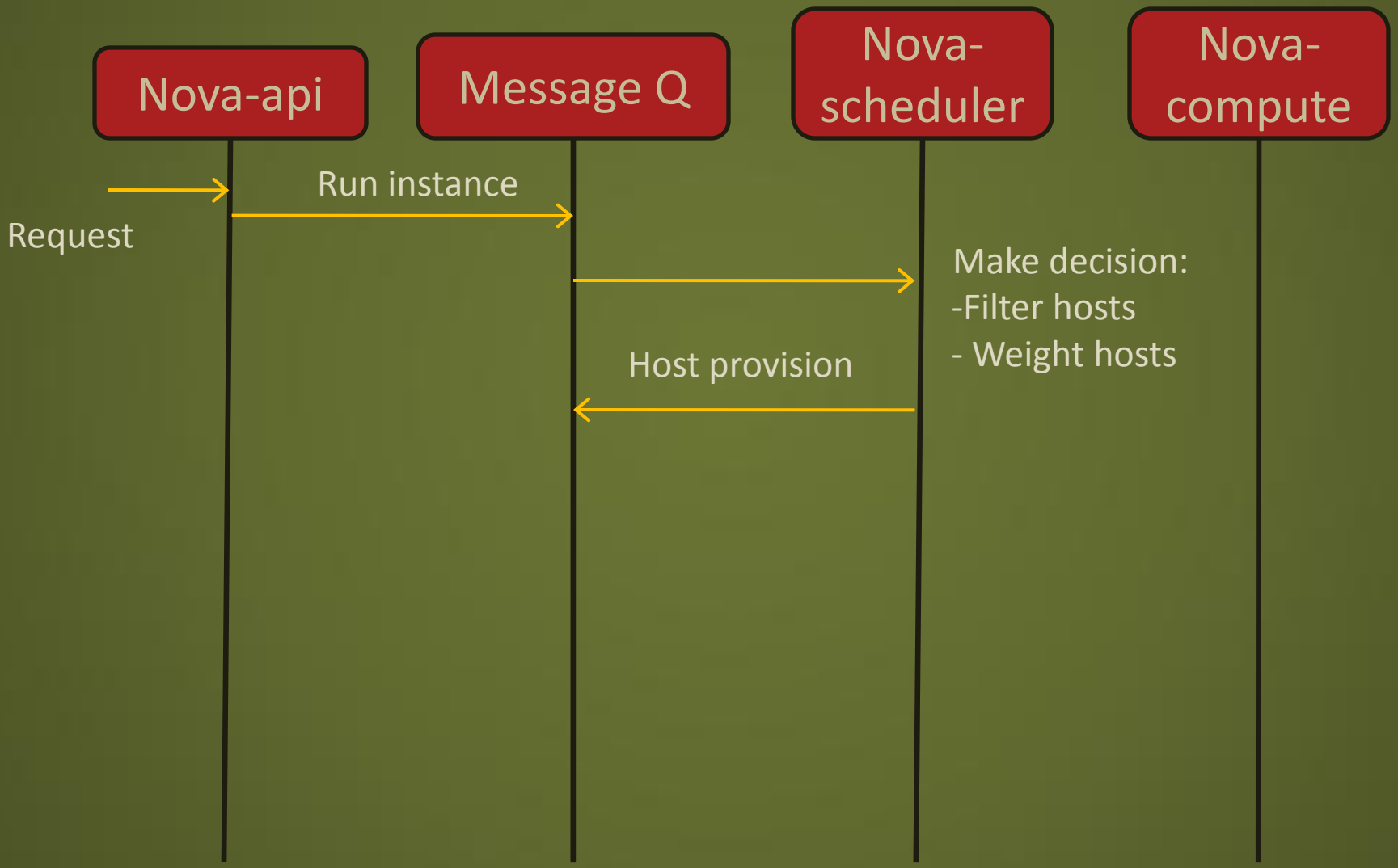
- Nova handles instances provisioning on compute resources.
- Nova-api initiates most activities
- Nova components communicate via queue and nova database
- Nova-scheduler decides where to launch instances
- Nova-compute launches instances
- Nova-compute periodically report host and network capabilities to Nova-scheduler

Nova Control Flow

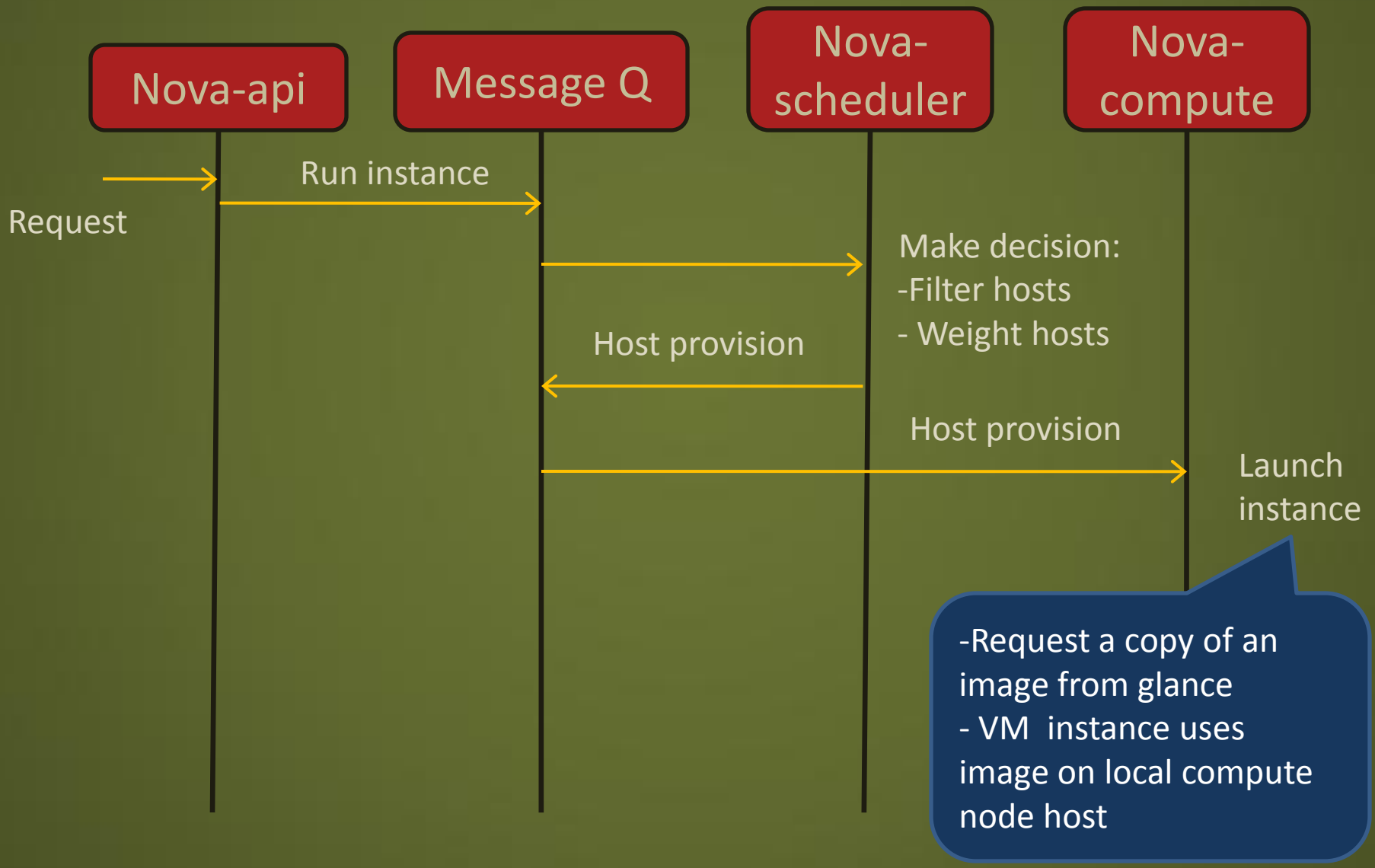
Nova Control Flow



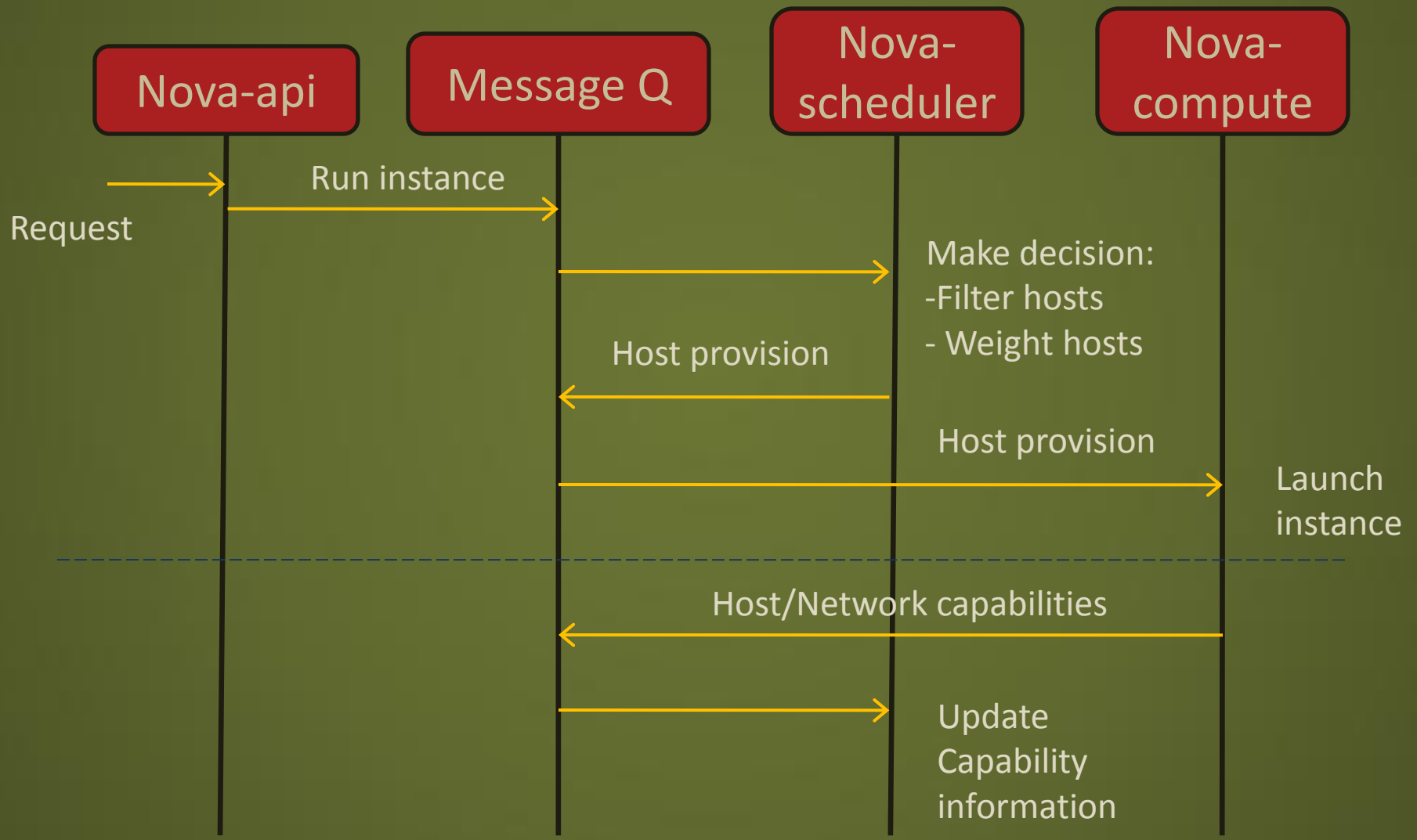
Nova Control Flow

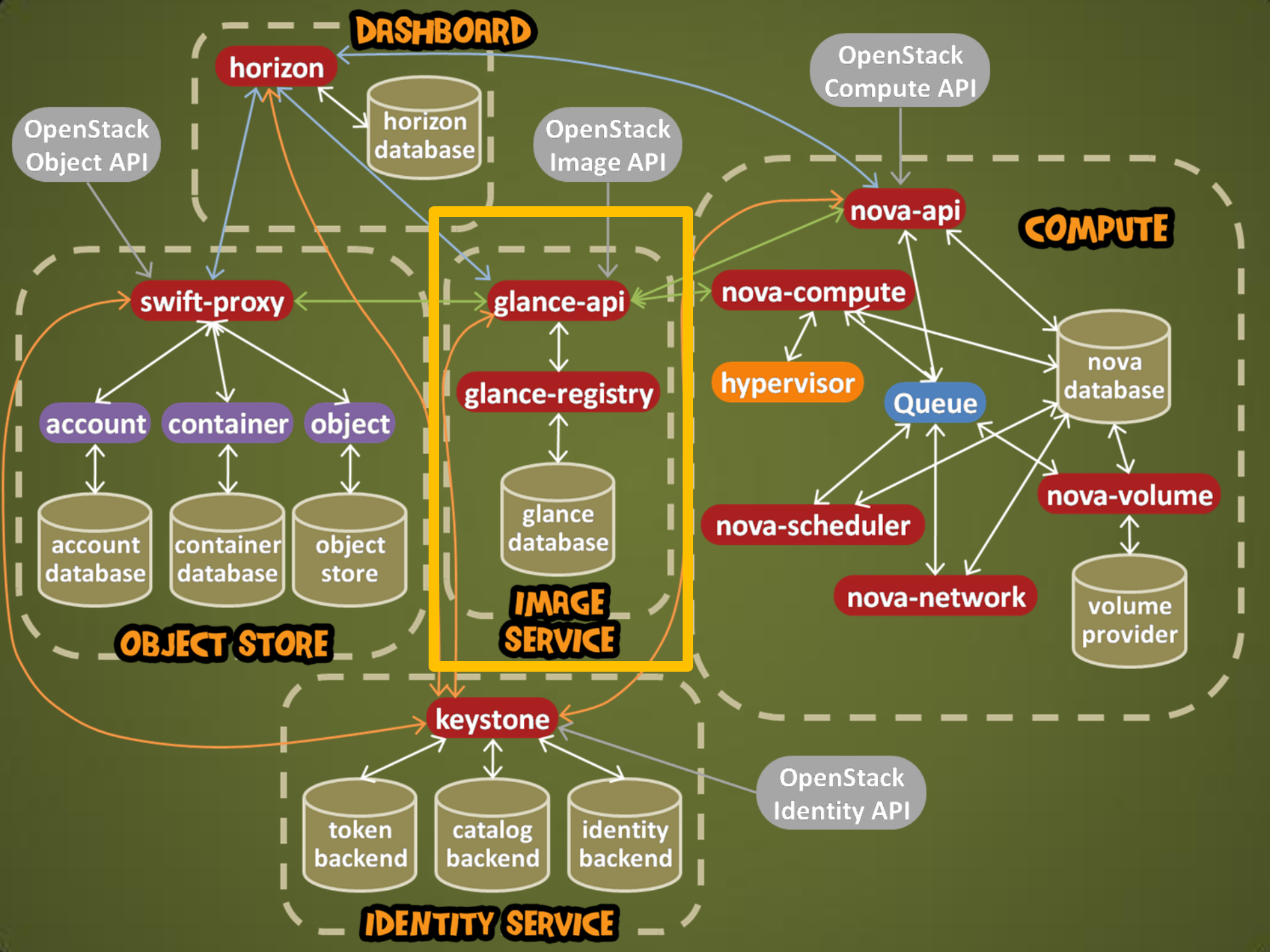


Nova Control Flow



Nova Control Flow

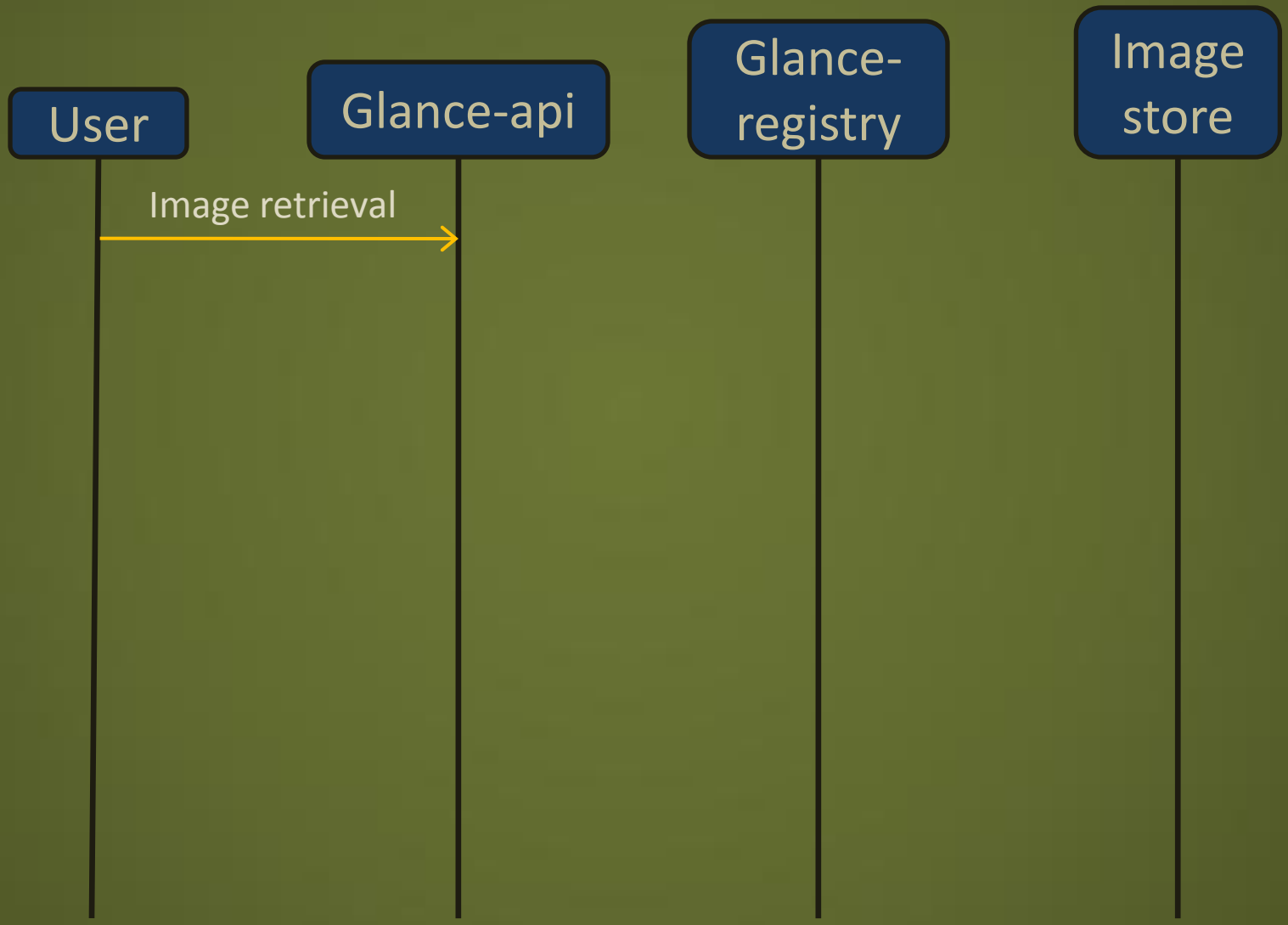



DASHBOARD
horizon
horizon database
OpenStack Compute API
OpenStack Object API
OpenStack Image API
nova-api
COMPUTE
swift-proxy
glance-api
nova-compute
glance-registry
hypervisor
nova database
Queue
account
container
object
account database
container database
object store
glance database
nova-volume
nova-scheduler
nova-network
volume provider
IMAGE SERVICE
OBJECT STORE
keystone
OpenStack Identity API
token backend
catalog backend
identity backend
IDENTITY SERVICE

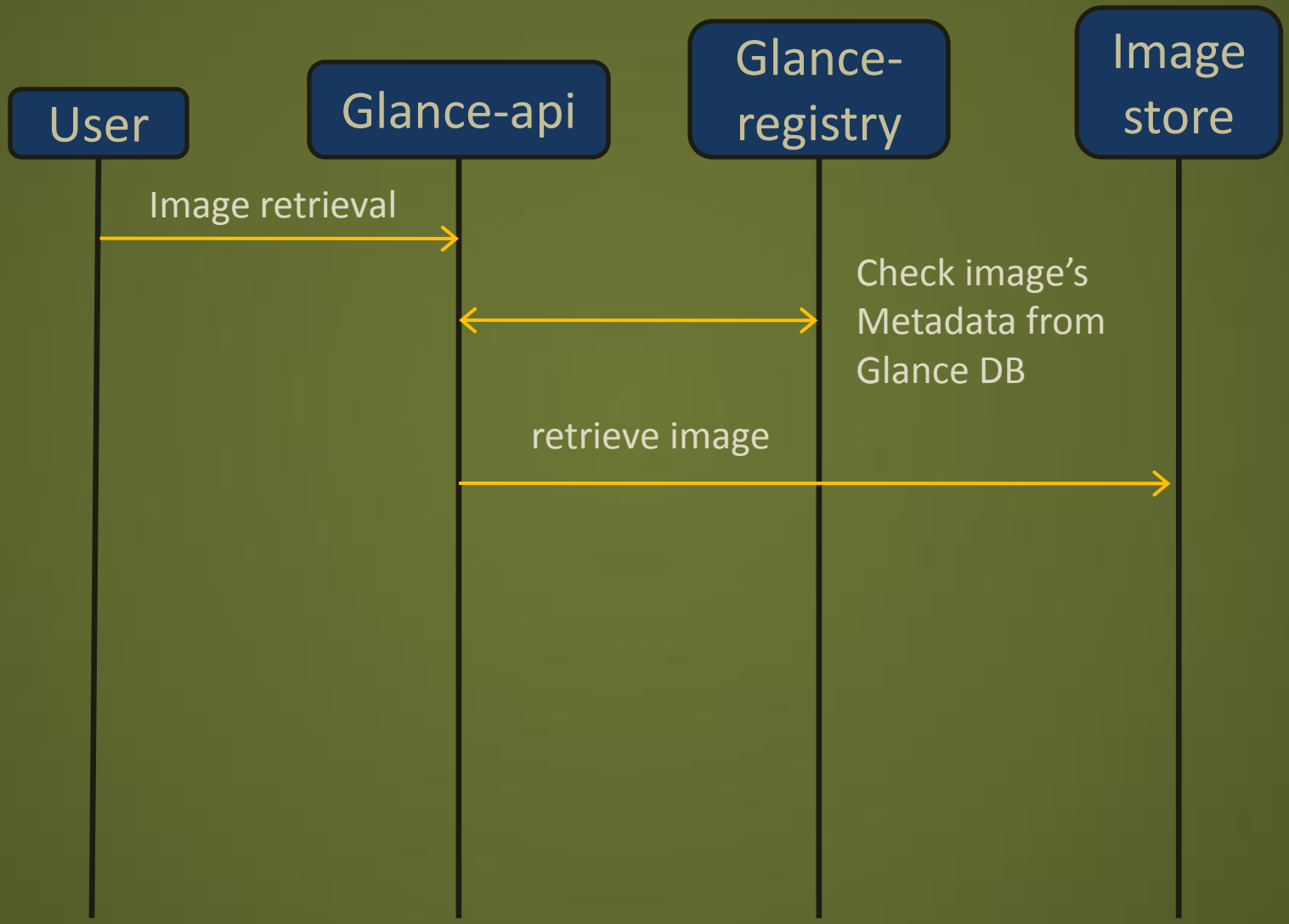
Glance

- Glance manage all kinds of images to instantiate VM instances
- Glance-api takes image retrieval requests from nova-compute and pass them to glance-registry
  - OpenStack create **a new copy** of the image on a host where the VM instance runs
- Glance-registry check image metadata from database
- Glance stores Image data in its image store (S3, HTTP, Local, Swift)

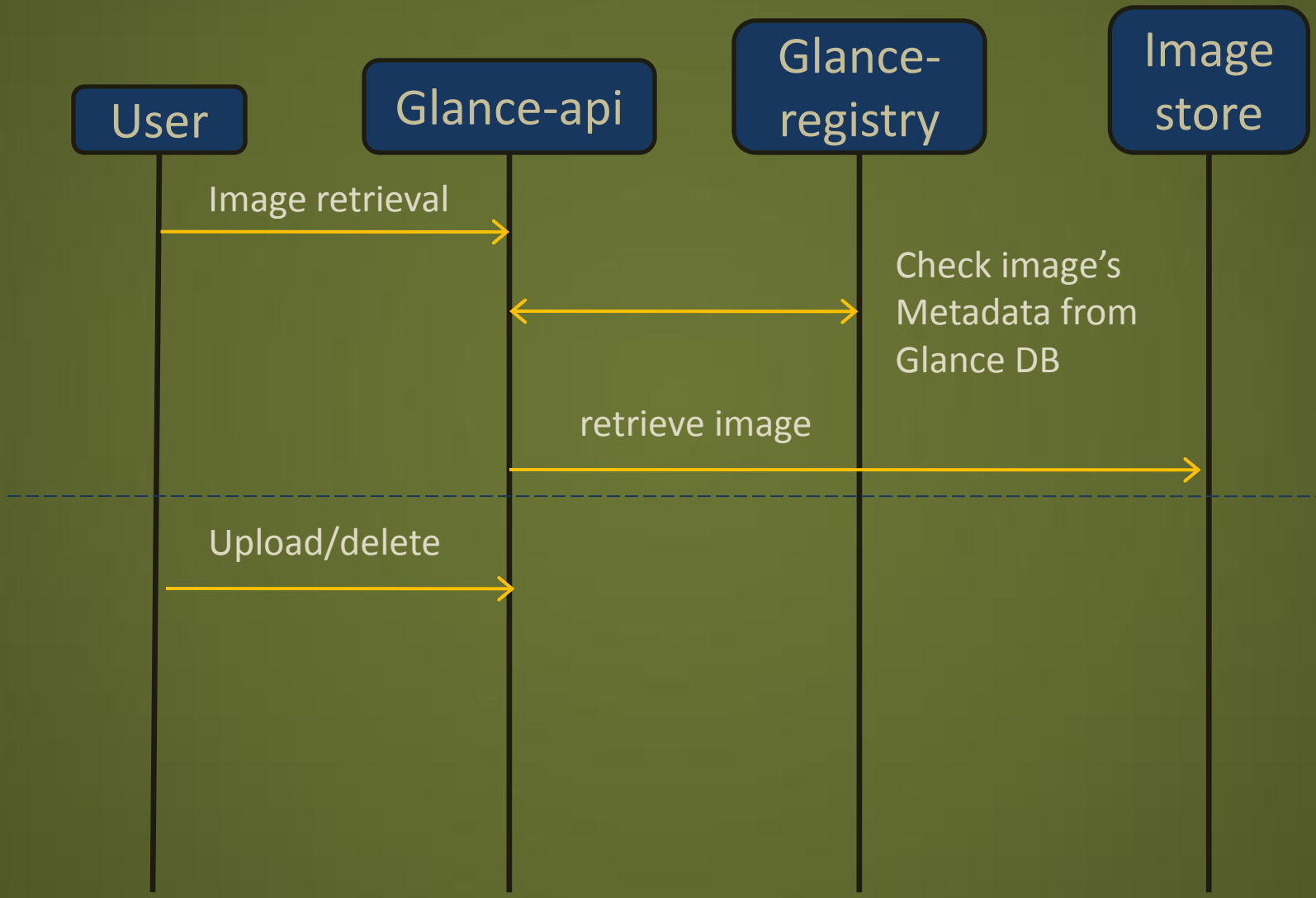
Glance Control Flow



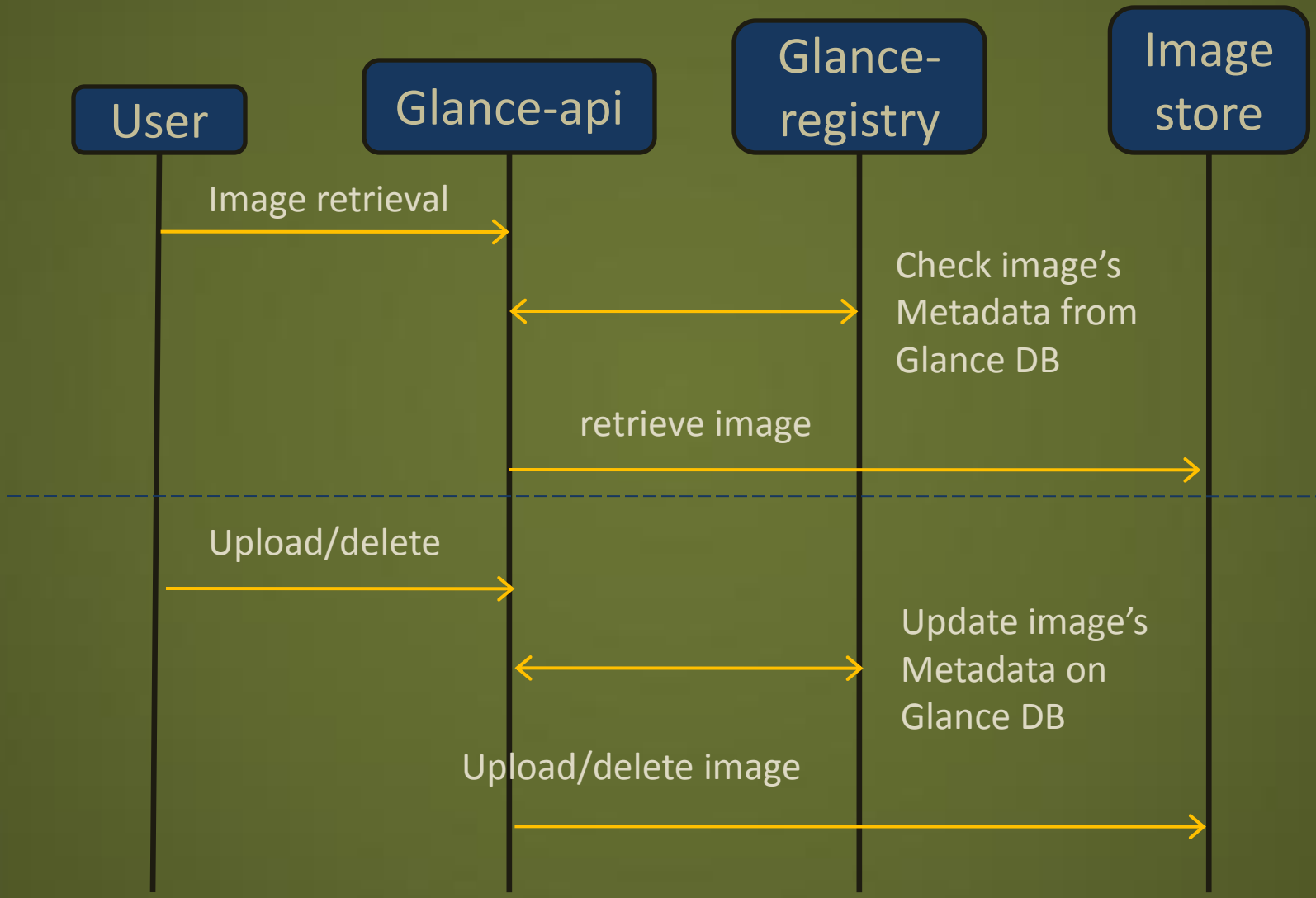
Glance Control Flow



Glance Control Flow



Glance Control Flow



How OpenStack Components work

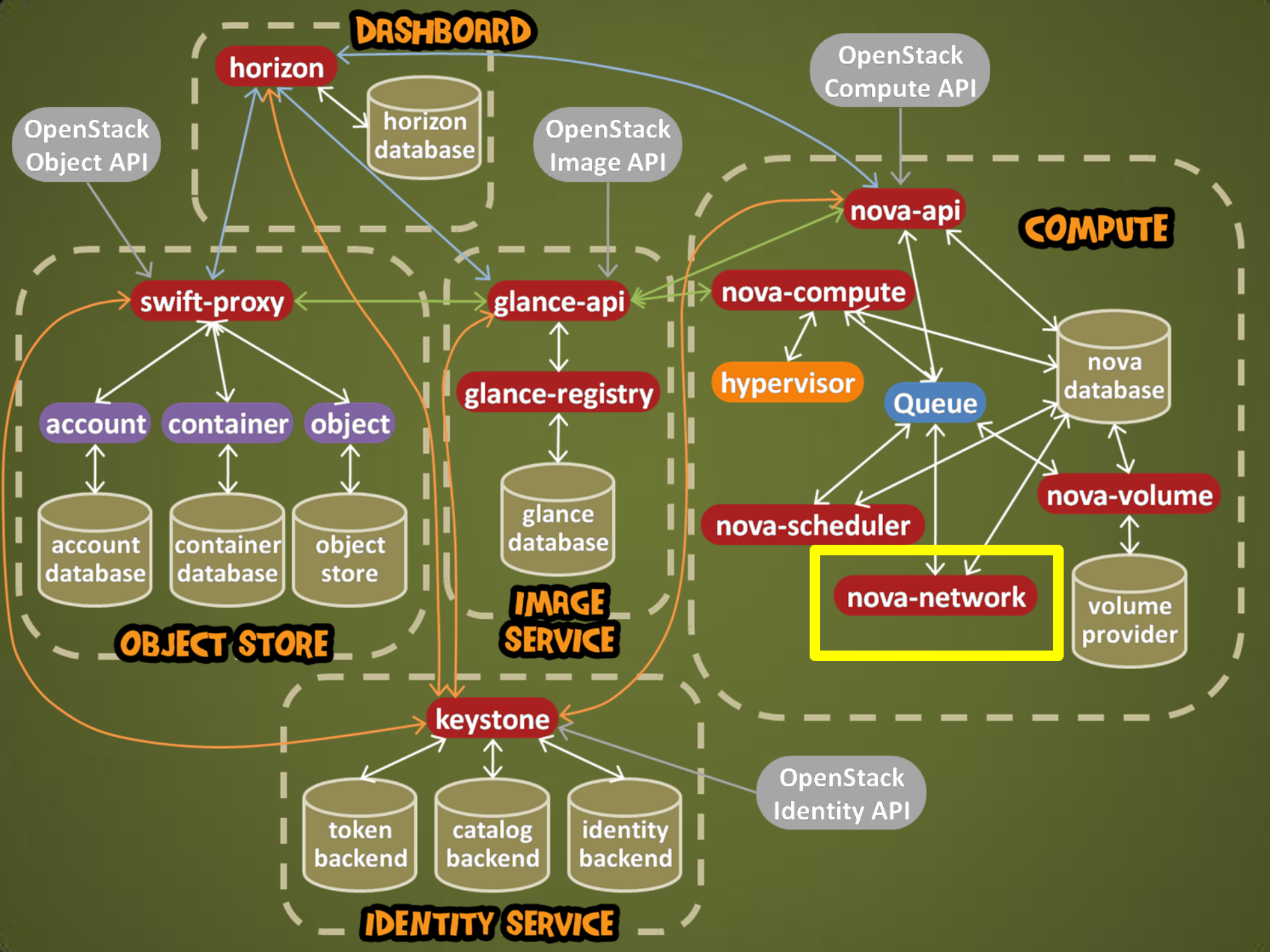
- Components in our focuses:
  - Keystone
  - Nova
  - Glance
- Networking Model
- Not currently cover
  - Swift

OpenStack Network Model

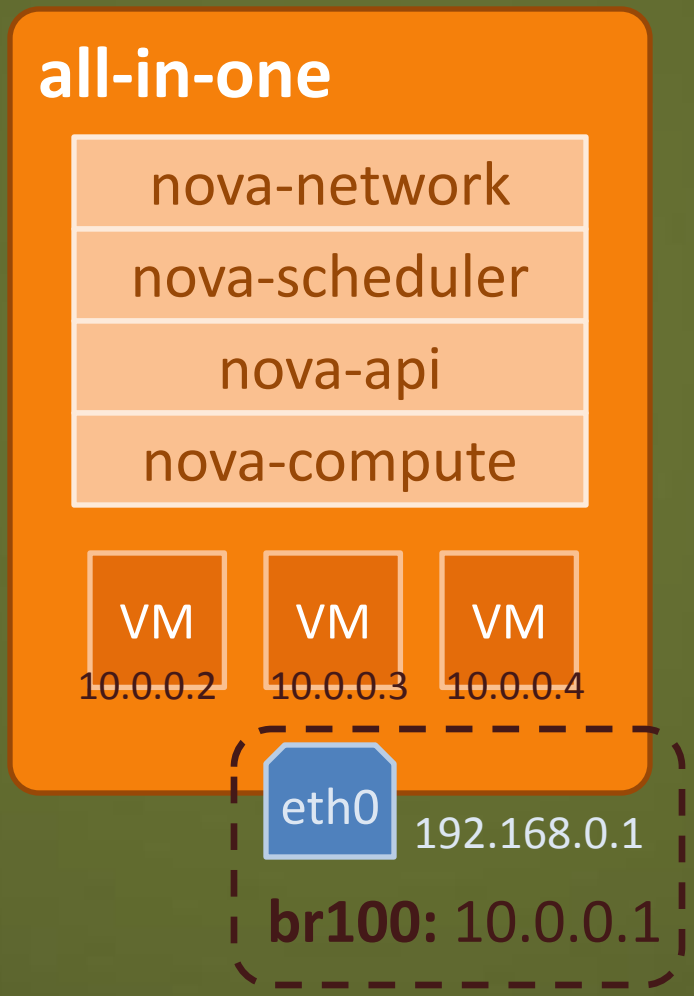
- Flat Network: A network administrator specifies a subnet from which all the virtual machines pulls IP addresses from a pool of available fixed addresses.
- Flat DHCP Network: The server that runs nova-network is a gateway to the compute nodes running virtual machines. Instances receive their fixed IPs by doing a dhcpdiscover. Like Flat Mode, all instances are attached to a single bridge on the compute node.
- VLAN Network: Compute creates a VLAN and bridge for each project. The project gets a range of private IPs that are only accessible from inside the VLAN. In this mode, each project gets its own VLAN, Linux networking bridge, and subnet.

IP address

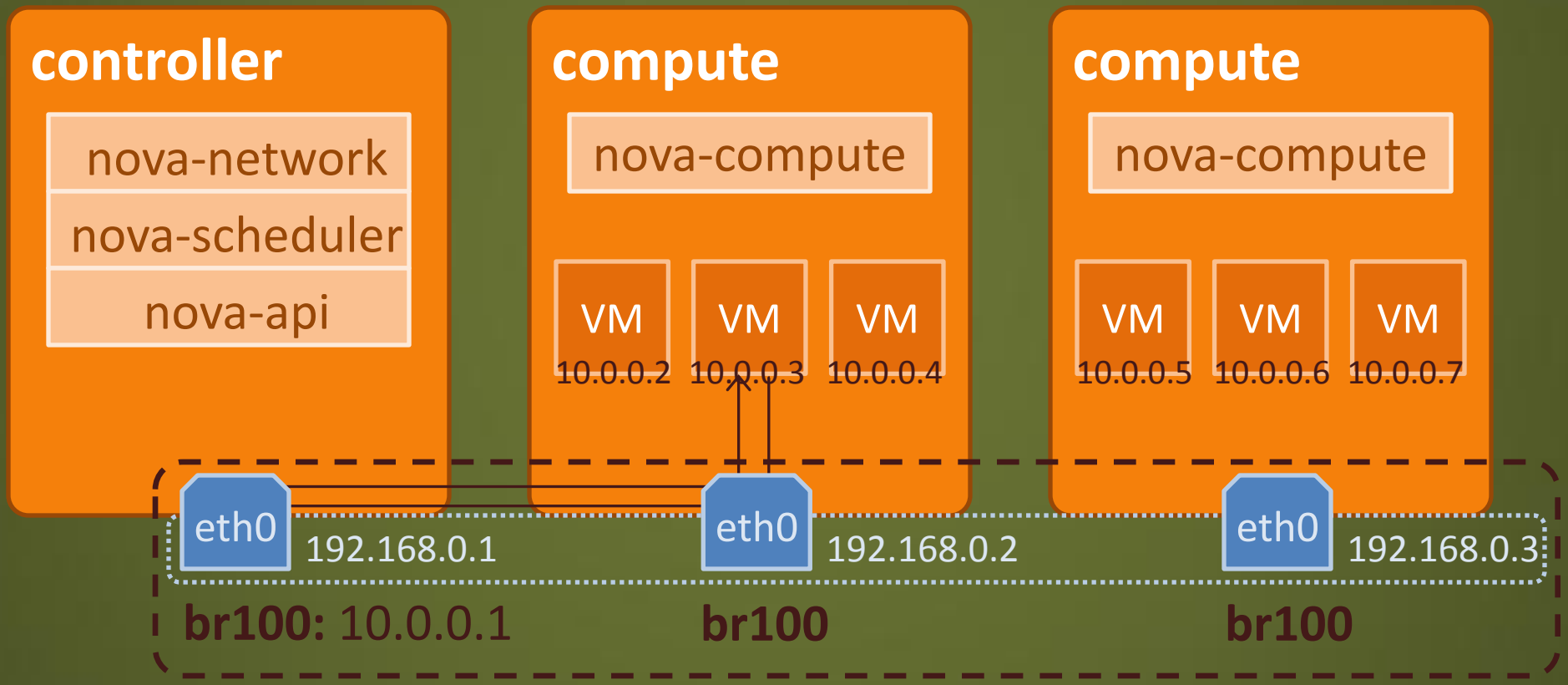
- Fixed IPs are IP addresses that are assigned to an instance on creation and stay the same until the instance is explicitly terminated.
- Floating IPs are addresses that can be dynamically associated with an instance. A floating IP address can be disassociated and associated with another instance at any time.


DASHBOARD
horizon
horizon database
OpenStack Compute API
OpenStack Object API
OpenStack Image API
nova-api
COMPUTE
swift-proxy
glance-api
nova-compute
hypervisor
Queue
nova database
glance-registry
account
container
object
account database
container database
object store
glance database
nova-volume
nova-scheduler
nova-network
volume provider
IMAGE SERVICE
OBJECT STORE
keystone
OpenStack Identity API
token backend
catalog backend
identity backend
IDENTITY SERVICE

Flat network, all-in-one server installation for development setup

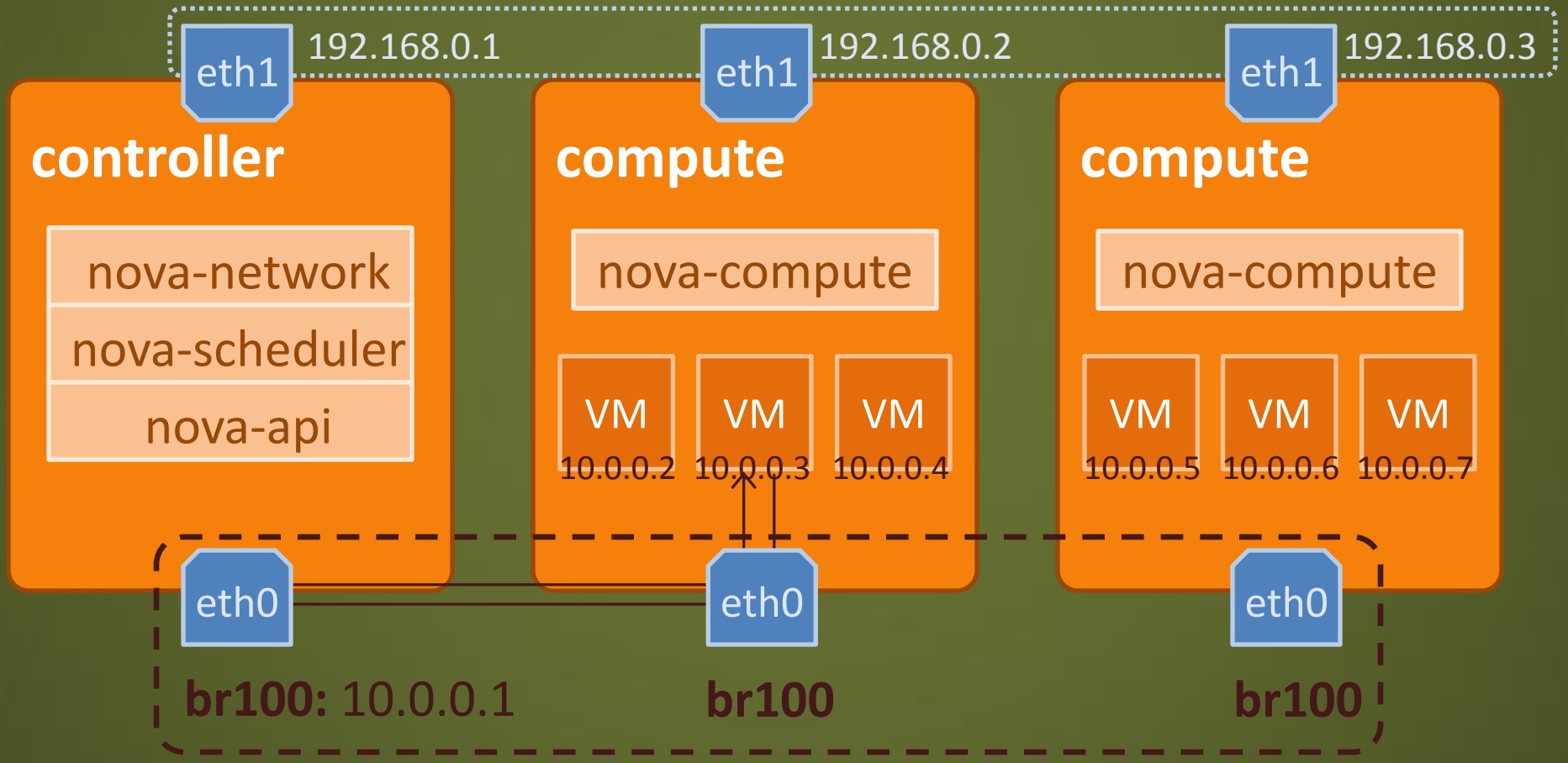


Flat network, multiple compute nodes with a single network adapter for smoke testing or a proof of concept

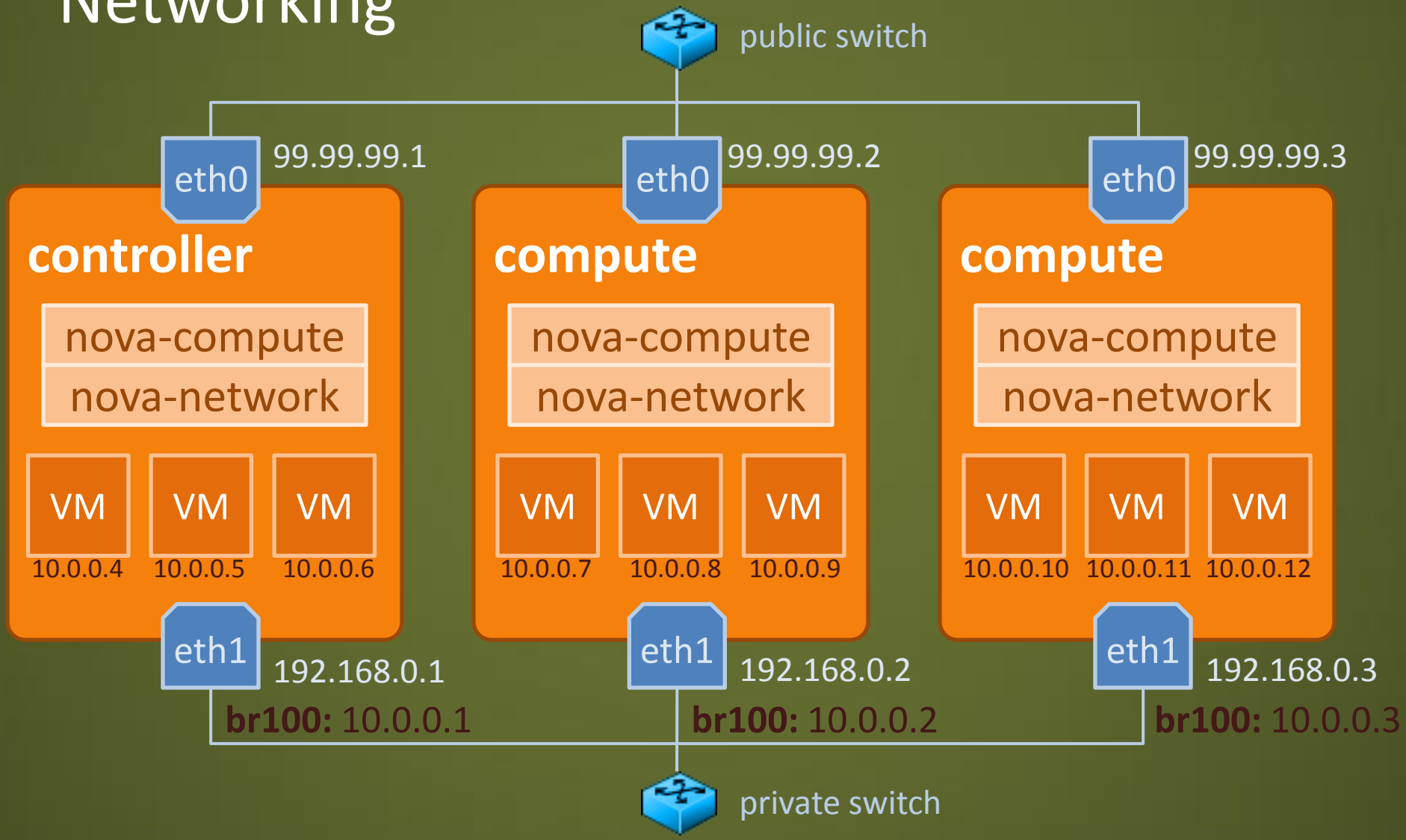


Note: OpenStack uses NAT to assign floating IP to VMs

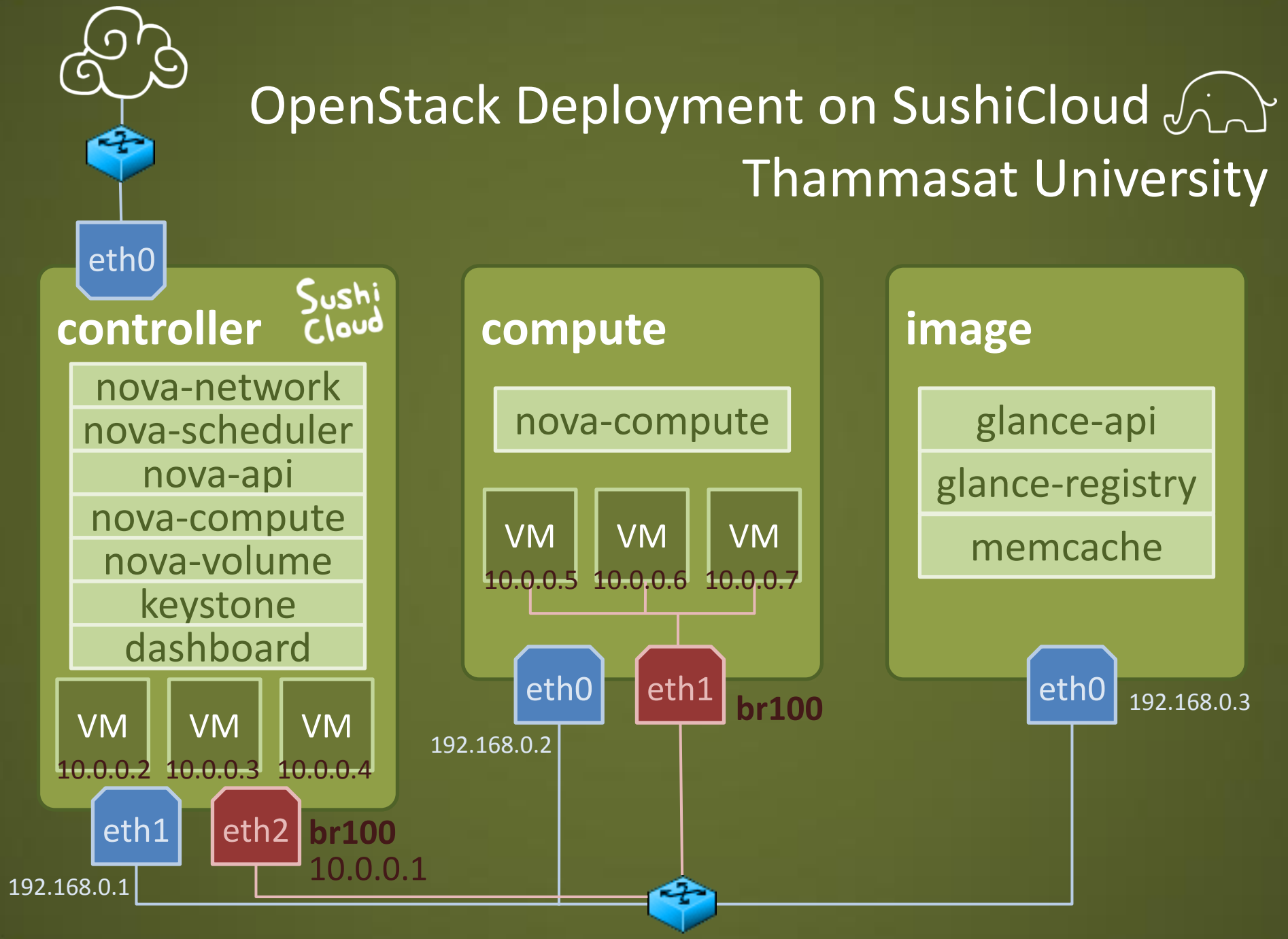
Flat network, multiple compute nodes with multiple network adapters for separate admin and data traffic



Flat DHCP network, multiple interfaces, multiple servers for High Availability Networking



OpenStack Deployment on SushiCloud
Thammasat University



OpenStack Installation Instructions

- Scripted installation for proof-of-concept, learning, or development: DevStack (http://devstack.org/)
- Manual installation on Ubuntu, Debian, CentOS, Fedora or Red Hat Enterprise Linux 6 for deployment / production: OpenStack Manuals (http://docs.openstack.org/)
- Other Installation
  - ISO Distribution Installation: StackOps Distro - Community Edition / Enterprise Edition (http://www.stackops.com/)
  - Puppet Deployment Tool (dodai-deploy): OpenStack Manuals (http://docs.openstack.org/)

Hardware Recommendations

Recommended hardware configurations for a minimum production deployment for the cloud controller nodes

Server	Recommended Hardware	Notes
Cloud Controller node (runs network, volume, API, scheduler and image services)	Processor: 64-bit x86 Memory: 12 GB RAM Disk space: 30 GB (SATA or SAS or SSD) Volume storage: two disks with 2 TB (SATA) for volumes attached to the compute nodes Network: one 1 GB Network Interface Card (NIC)	32-bit processors will work for the cloud controller node. A quad core server with 12 GB RAM would be more than sufficient for a cloud controller node. Two NICS are recommended but not required.

http://docs.openstack.org/

Hardware Recommendations

Recommended hardware configurations for a minimum production deployment for the compute nodes

Server	Recommended Hardware	Notes
Compute nodes (runs virtual instances)	Processor: 64-bit x86 Memory: 32 GB RAM Disk space: 30 GB (SATA) Network: two 1 GB NICs	Note that you cannot run 64-bit VM instances on a 32-bit compute node. A 64-bit compute node can run either 32- or 64-bit VMs, however. With 2 GB RAM you can run one m1.small instance on a node or three m1.tiny instances without memory swapping, so 2 GB RAM would be a minimum for a test-environment compute node.

http://docs.openstack.org/

Compute and Image System Requirements

- Operating System: OpenStack currently has packages for the following distributions: CentOS, Debian, Fedora, RHEL, Debian, and Ubuntu.
- Database: For OpenStack Compute, you need access to either a PostgreSQL or MySQL database, or you can install it as part of the OpenStack Compute installation process. For Object Storage, the container and account servers use SQLite, and you can install it as part of the installation process.
- Network Time Protocol: You must install a time synchronization program such as NTP. For Compute, time synchronization keeps your cloud controller and compute nodes talking to the same time server to avoid problems scheduling VM launches on compute nodes. For Object Storage, time synchronization ensure the object replications are accurately updating objects when needed so that the freshest content is served.

Our Testbed Environment

- Cloud Controller node (runs network, volume, API, scheduler and compute)
- Compute node (runs virtual instances)
- Each node
- Processor: 64-bit 12-cores 2.1 GHz Opteron
- Memory: 48GB RAM
- Disk space: 600GB
- Volume storage: 300GB
- Network: four 1Gbps NICs

Our Testbed Environment

- Glance node (runs image services)
- Processor: 64-bit two Quad core Xeon 5500 2.40Ghz
- Memory: 72GB RAM
- Disk space: 750GB
- Network: two 1Gbps NICs

Usage Scenario

- Once Upon a time, supposed you are a system admin of a small public cloud service provider company
- You want to create Cloud users and projects for a customer company
- Users access OpenStack to create and launch virtual machines by themselves

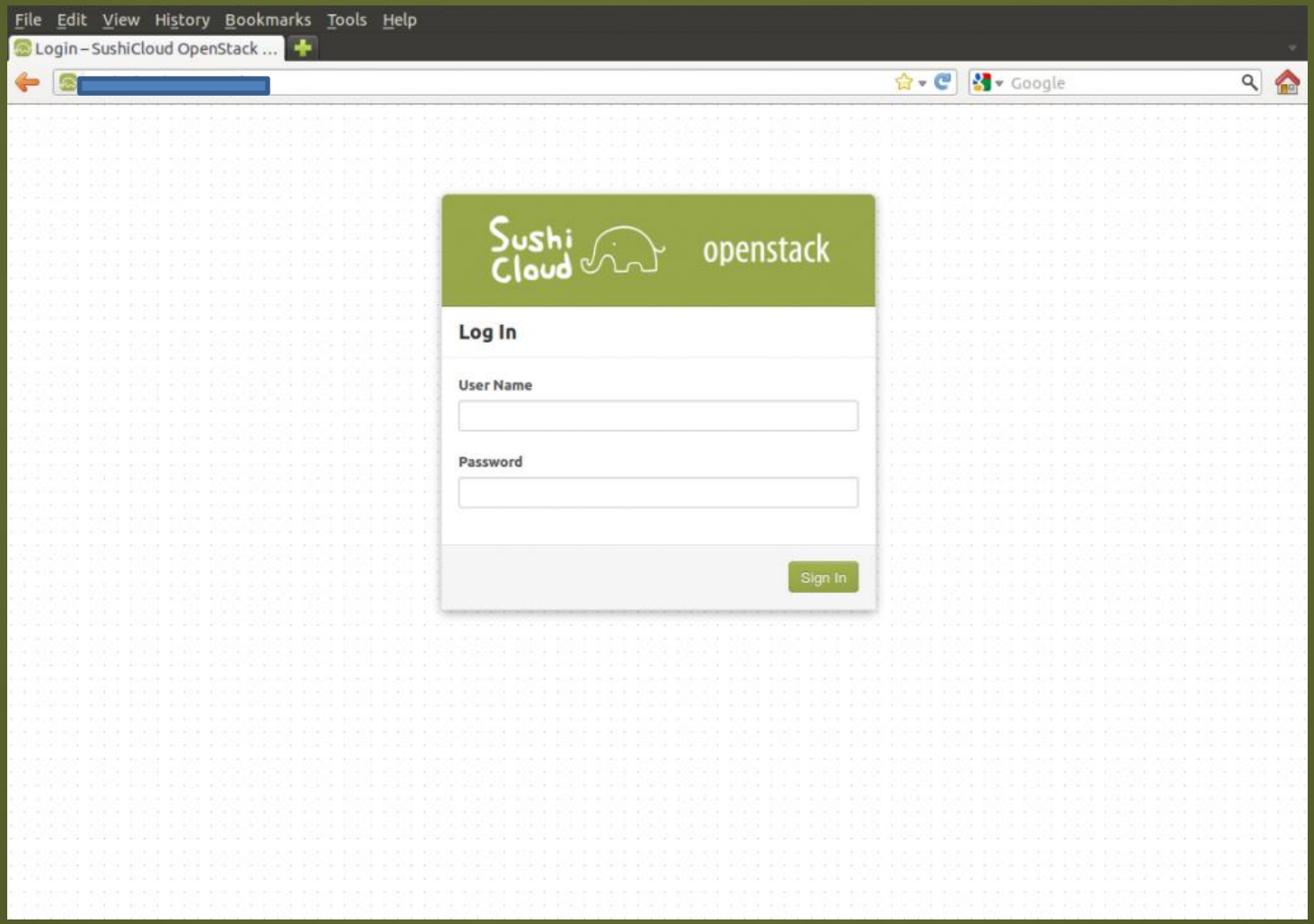
Using OpenStack Dashboard

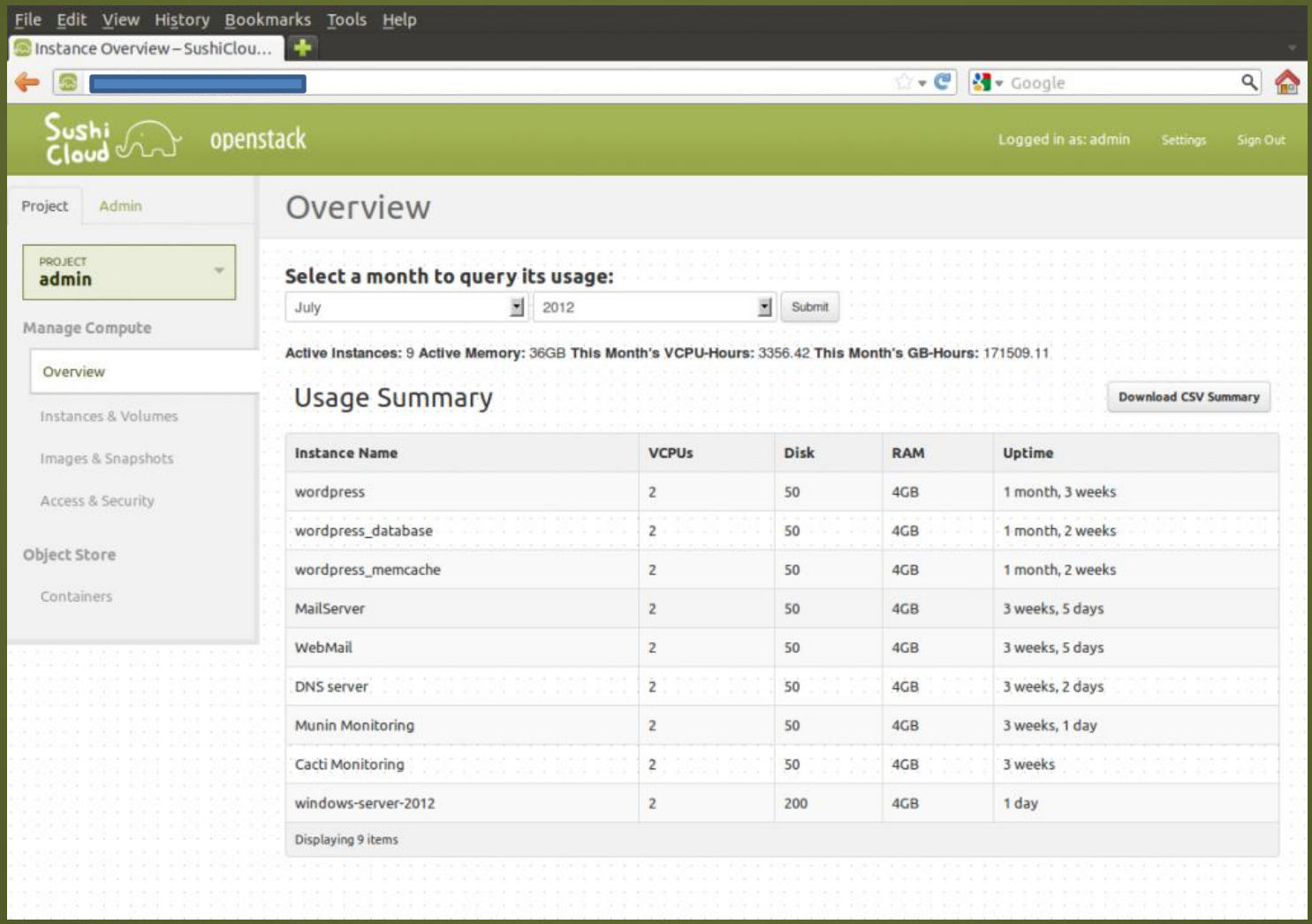
- Add Users and Projects
- Create key-pair
- Launch Instance
- Configure Access
- Access Instance

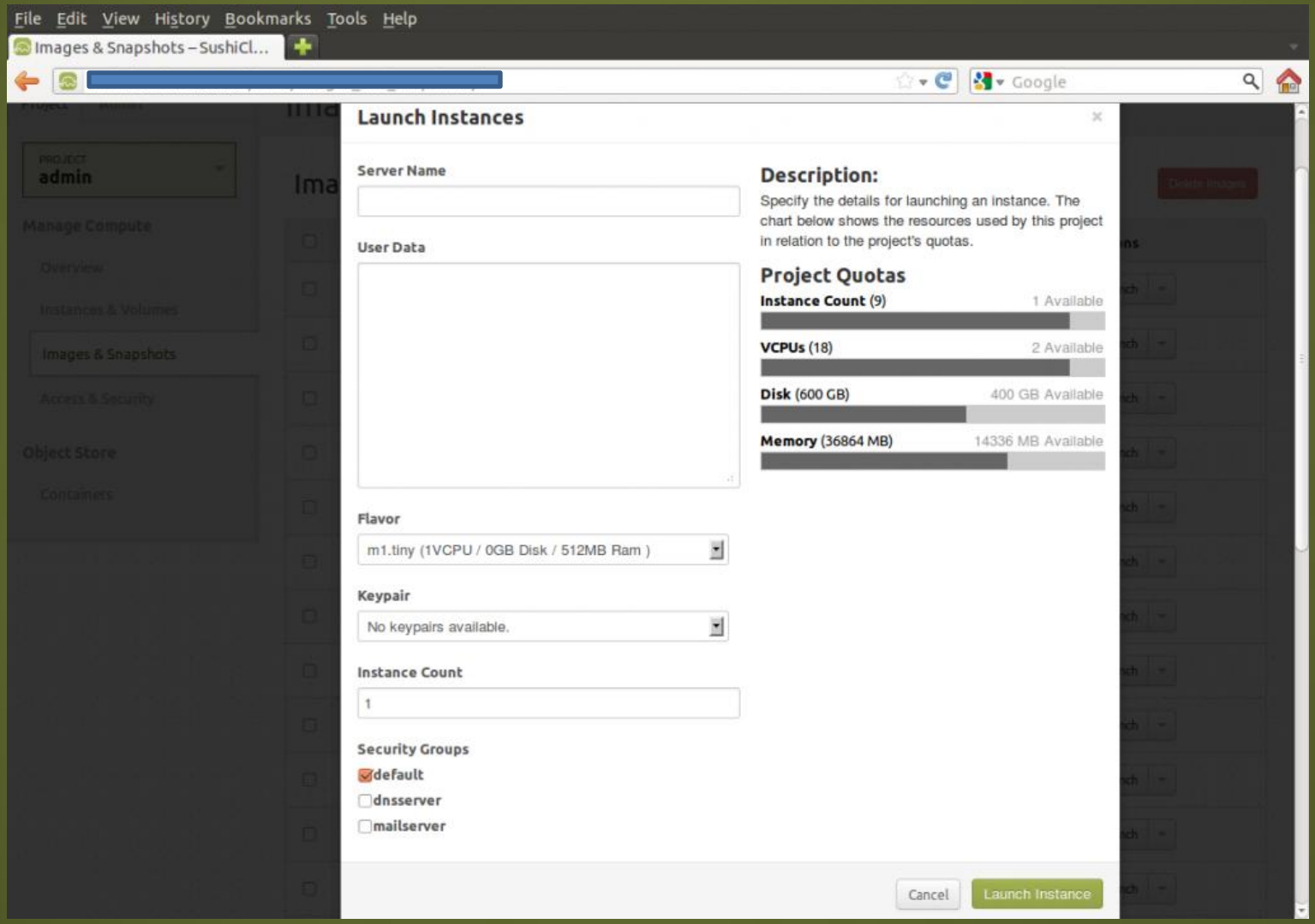
Part II: Demo

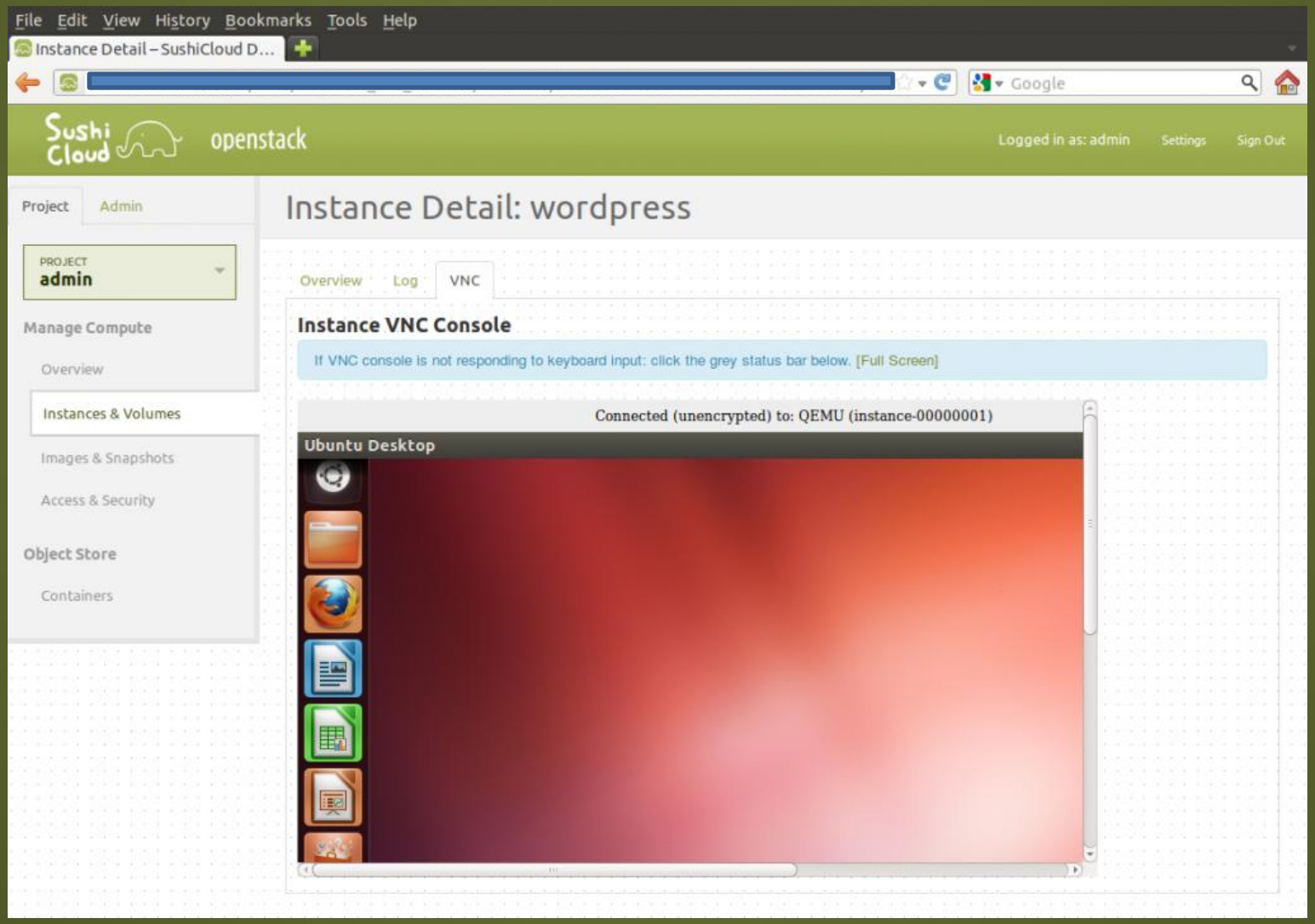
SuhiCloud Testbed

Backup


File Edit View History Bookmarks Tools Help
Login – SushiCloud OpenStack ...
Google
Sushi Cloud
openstack
Log In
User Name
Password
Sign In


File Edit View History Bookmarks Tools Help
Instance Overview – SushiClou...
Google
Sushi Cloud
openstack
Logged in as: admin
Settings
Sign Out
Project
Admin
PROJECT
admin
Manage Compute
Overview
Instances & Volumes
Images & Snapshots
Access & Security
Object Store
Containers
Overview
Select a month to query its usage:
July
2012
Submit
Active Instances: 9 Active Memory: 36GB This Month's VCPU-Hours: 3356.42 This Month's GB-Hours: 171509.11
Usage Summary
Download CSV Summary
Instance Name
VCPUs
Disk
RAM
Uptime
wordpress
2
50
4GB
1 month, 3 weeks
wordpress_database
2
50
4GB
1 month, 2 weeks
wordpress_memcache
2
50
4GB
1 month, 2 weeks
MailServer
2
50
4GB
3 weeks, 5 days
WebMail
2
50
4GB
3 weeks, 5 days
DNS server
2
50
4GB
3 weeks, 2 days
Munin Monitoring
2
50
4GB
3 weeks, 1 day
Cacti Monitoring
2
50
4GB
3 weeks
windows-server-2012
2
200
4GB
1 day
Displaying 9 items


File Edit View History Bookmarks Tools Help
Images & Snapshots – SushiCl...
Google
PROJECT
admin
Manage Compute
Overview
Instances & Volumes
Images & Snapshots
Access & Security
Object Store
Containers
Launch Instances
Server Name
User Data
Flavor
m1.tiny (1VCPU / 0GB Disk / 512MB Ram)
Keypair
No keypairs available.
Instance Count
1
Security Groups
default
dnsserver
mailserver
Description:
Specify the details for launching an instance. The chart below shows the resources used by this project in relation to the project's quotas.
Project Quotas
Instance Count (9) 1 Available
VCPUs (18) 2 Available
Disk (600 GB) 400 GB Available
Memory (36864 MB) 14336 MB Available
Cancel
Launch Instance


File Edit View History Bookmarks Tools Help
Instance Detail – SushiCloud D...
Google
Sushi Cloud
openstack
Logged in as: admin
Settings
Sign Out
Project
Admin
PROJECT
admin
Manage Compute
Overview
Instances & Volumes
Images & Snapshots
Access & Security
Object Store
Containers
Instance Detail: wordpress
Overview
Log
VNC
Instance VNC Console
If VNC console is not responding to keyboard input: click the grey status bar below. [Full Screen]
Connected (unencrypted) to: QEMU (instance-00000001)
Ubuntu Desktop