SambaXP 2014

openstack and SAMBA

CLOUD SOFTWARE

opening windows to a wider world

Simo Sorce
Samba Team Member
Identity Management Team – Red Hat

redhat.

What is OpenStack ?

OpenStack is a cloud “operating system”

But what is a “cloud operating system” ?

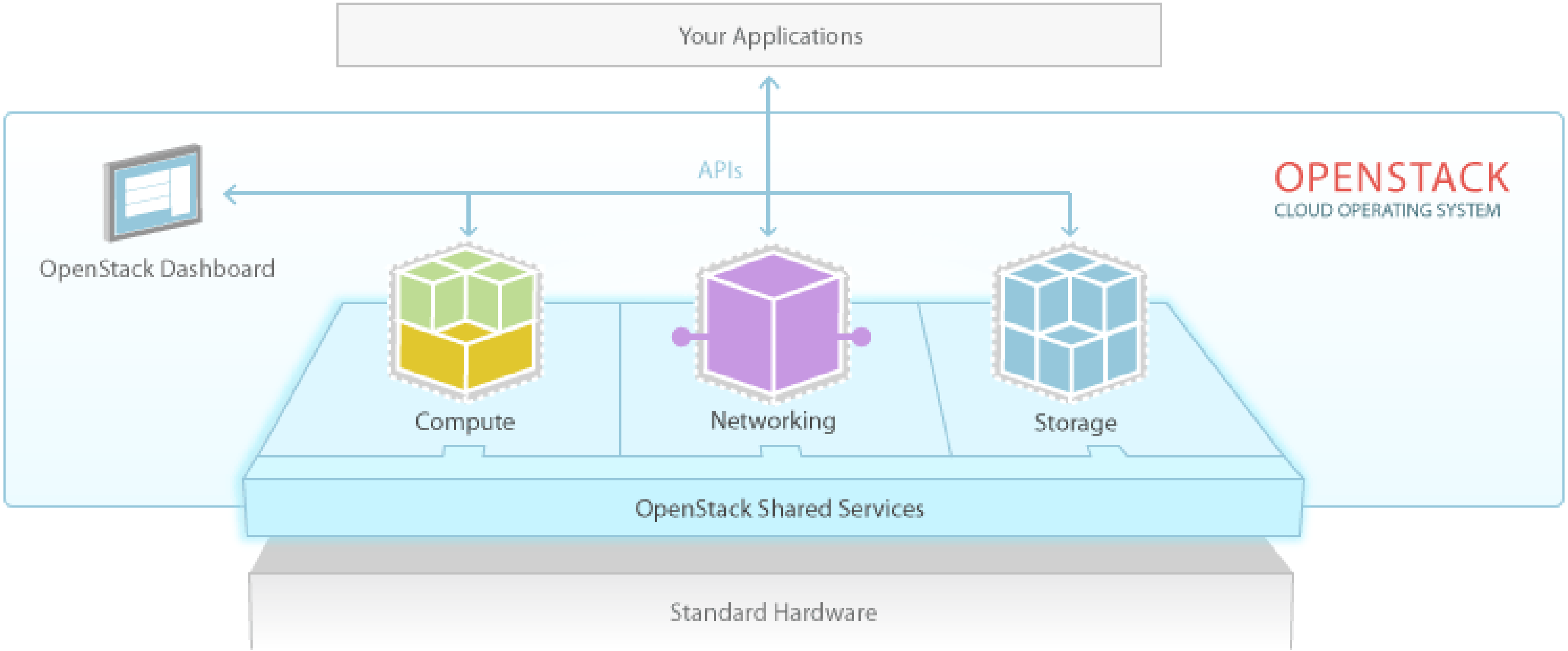
A cloud infrastructure is a collection of services that provide a coherent computing platform that can be accessed on-demand and in a self-service mode.

Elasticity and resource pooling are the key drivers, resources are made available as needed and resources are pooled to use the hardware as efficiently as possible.

Services can be metered and measured to provide and elastically instantiated to provide the requested service level within predetermined policies.

Services are available via Network using well defined APIs

Base components:



Compute – manages large pools of hardware and VMs

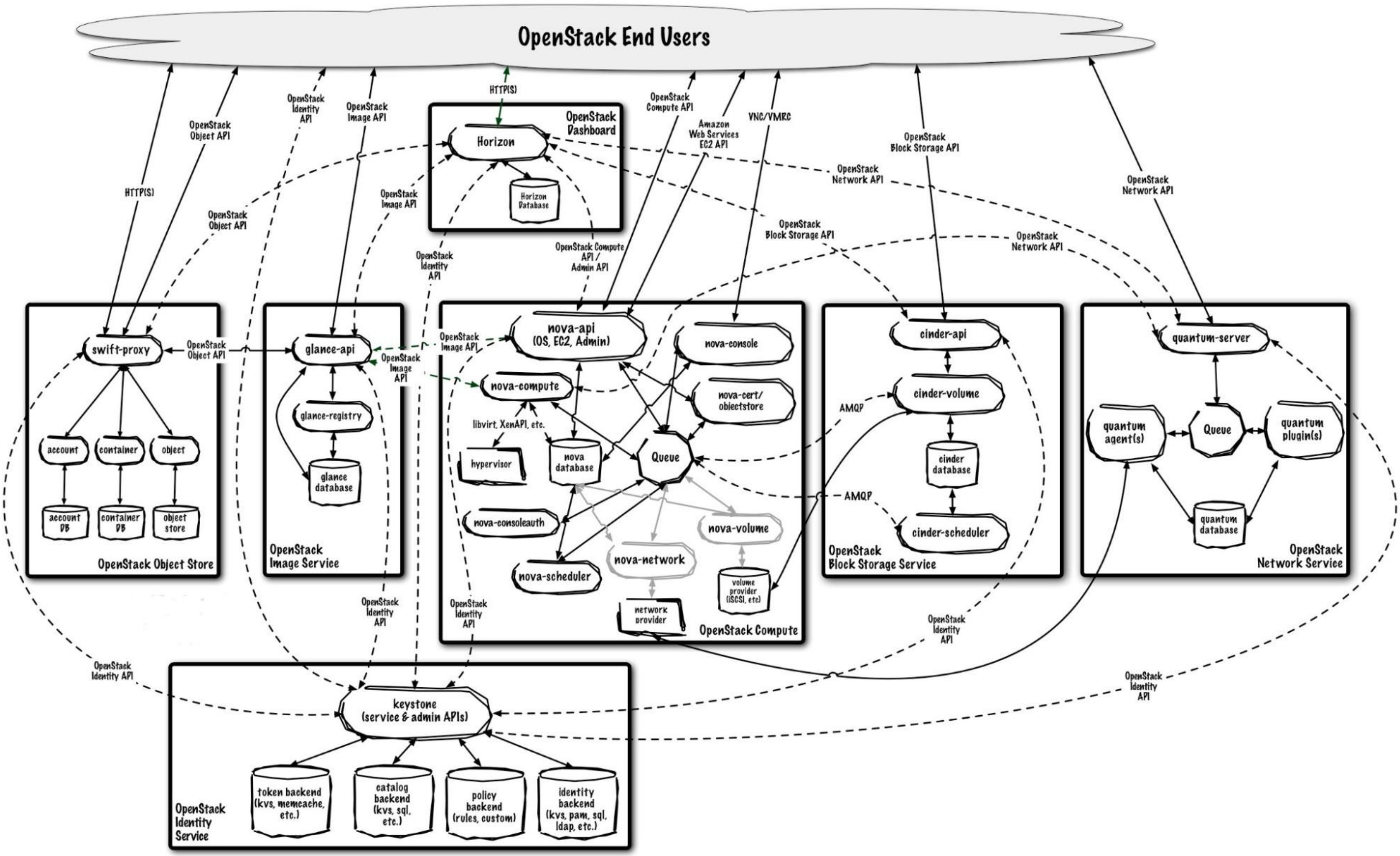
Storage – services that provide block and object storage

Networking – manages software defined networks

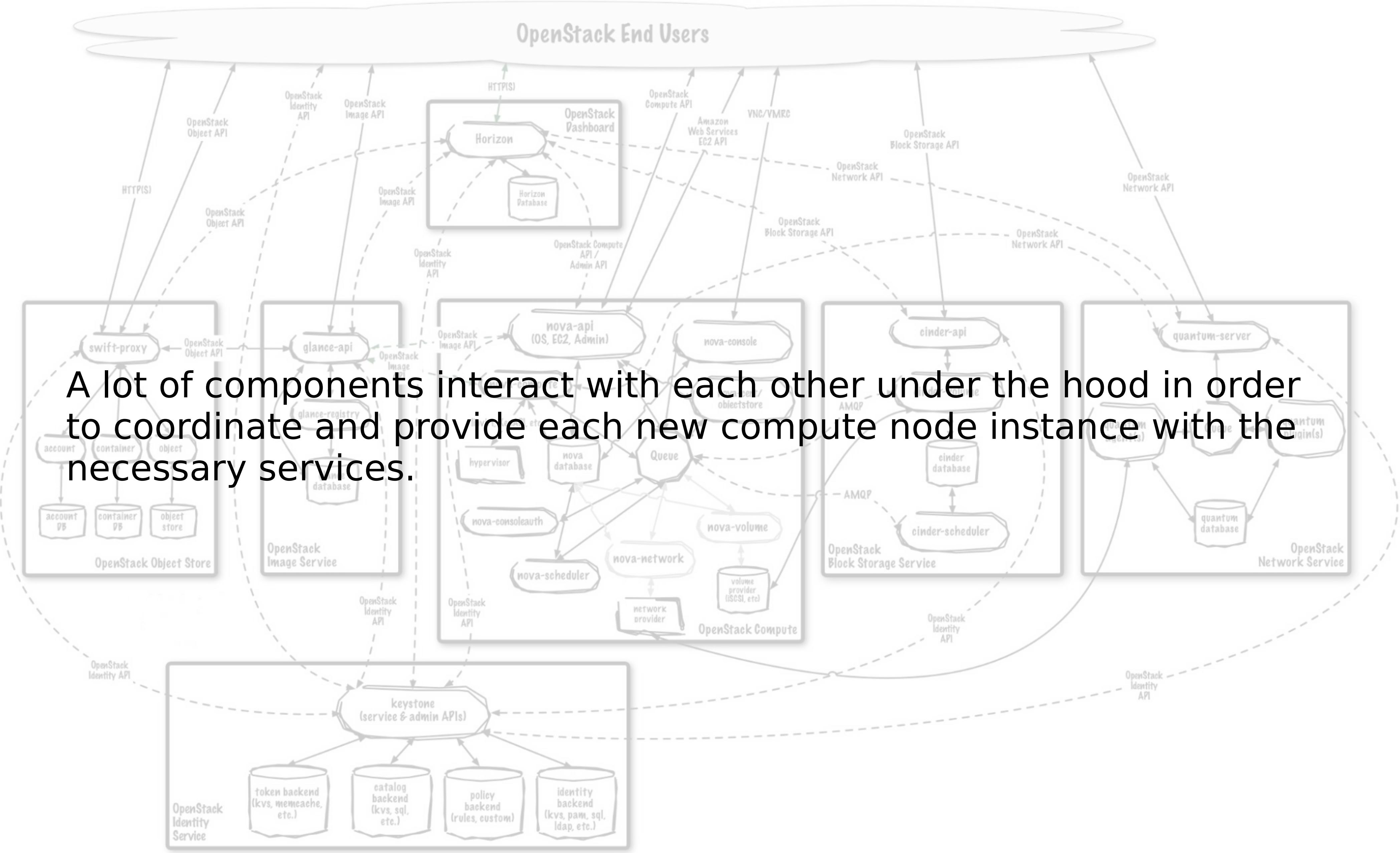
Dashboard – control panel for users and administrators

Shared Services – provisioning, monitoring and AAA services

Complex view:

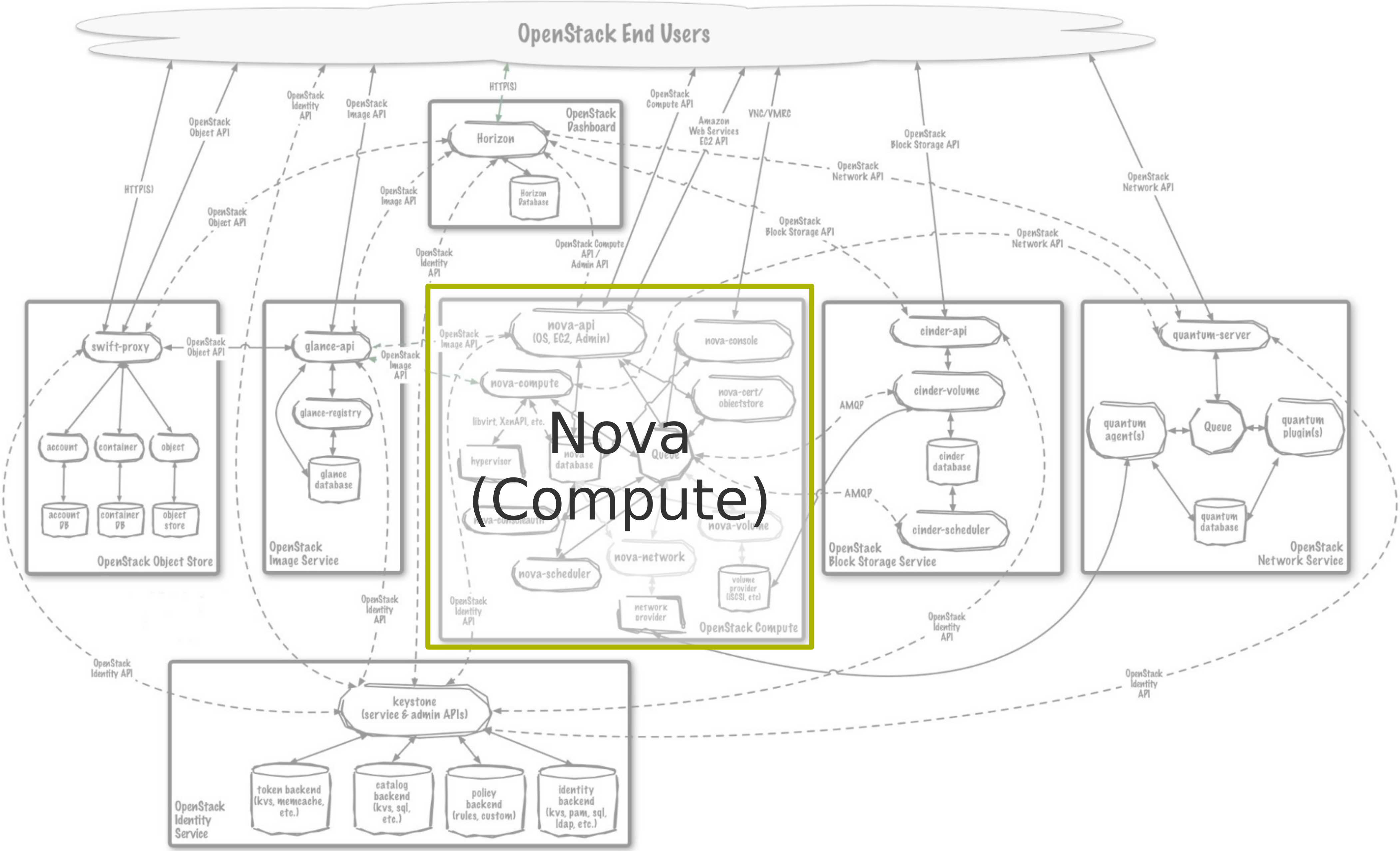


Complex view:



A lot of components interact with each other under the hood in order to coordinate and provide each new compute node instance with the necessary services.

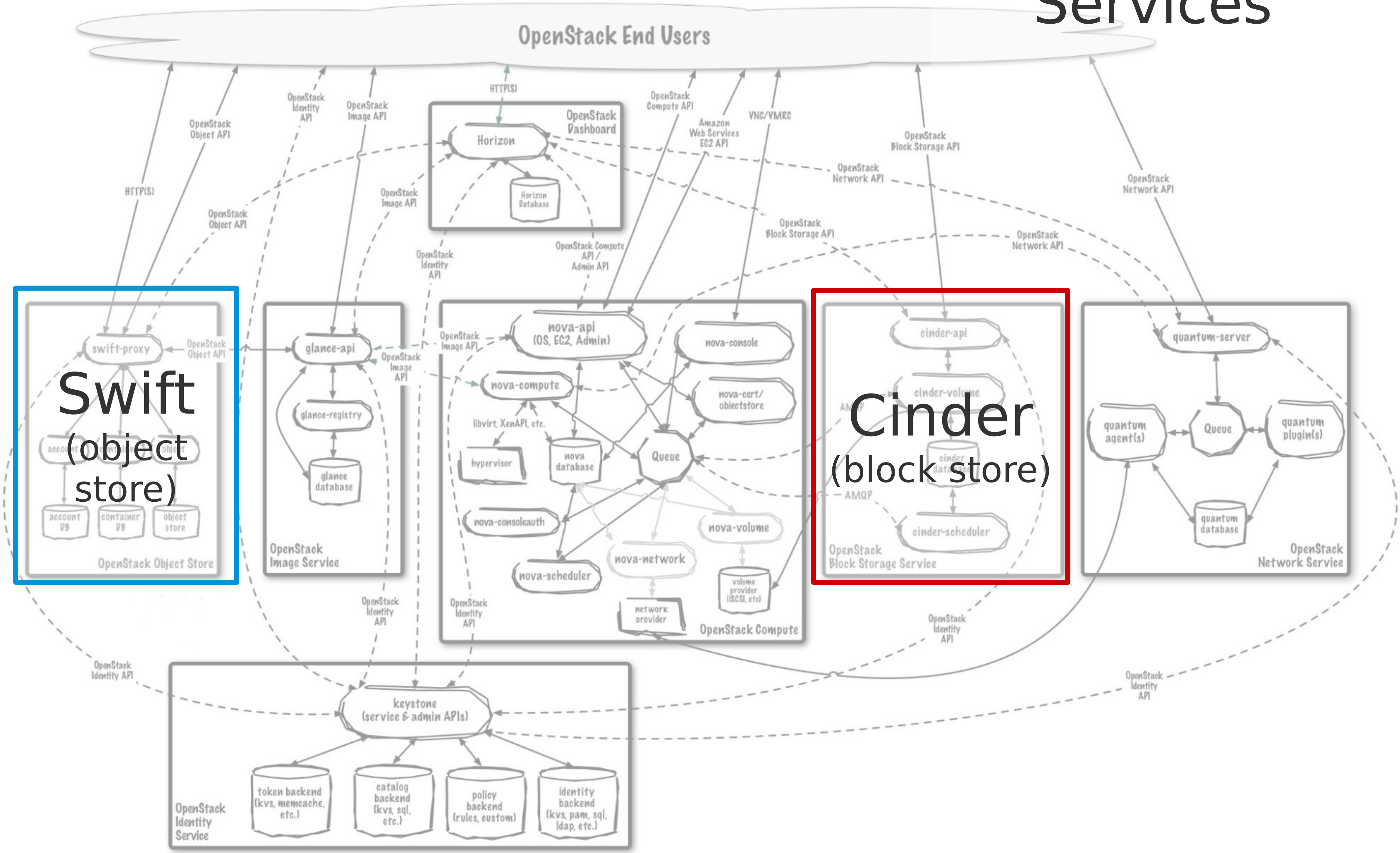
Complex view:



Nova (Compute)

Complex view:

Storage Services



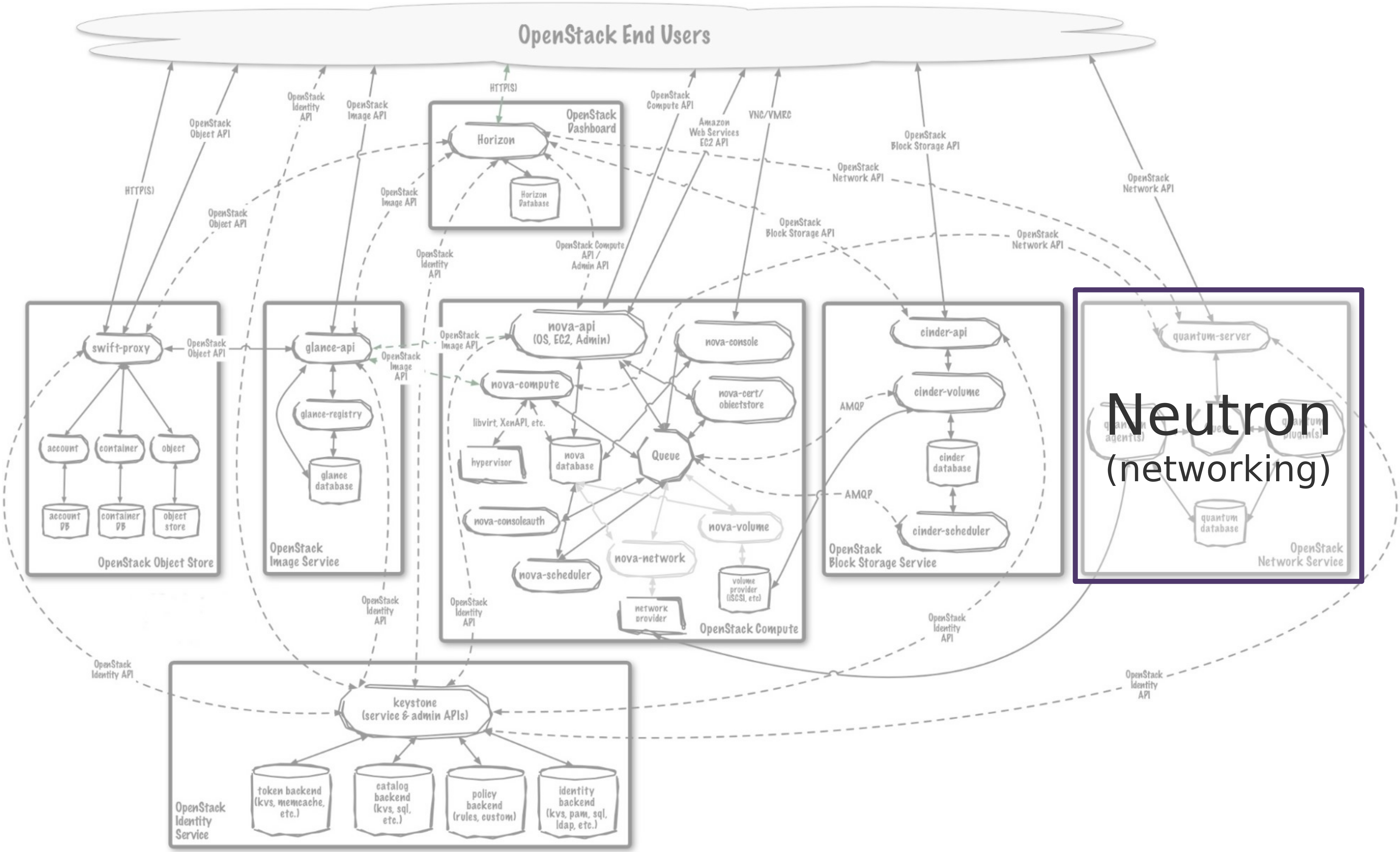
Swift

(object store)

Cinder

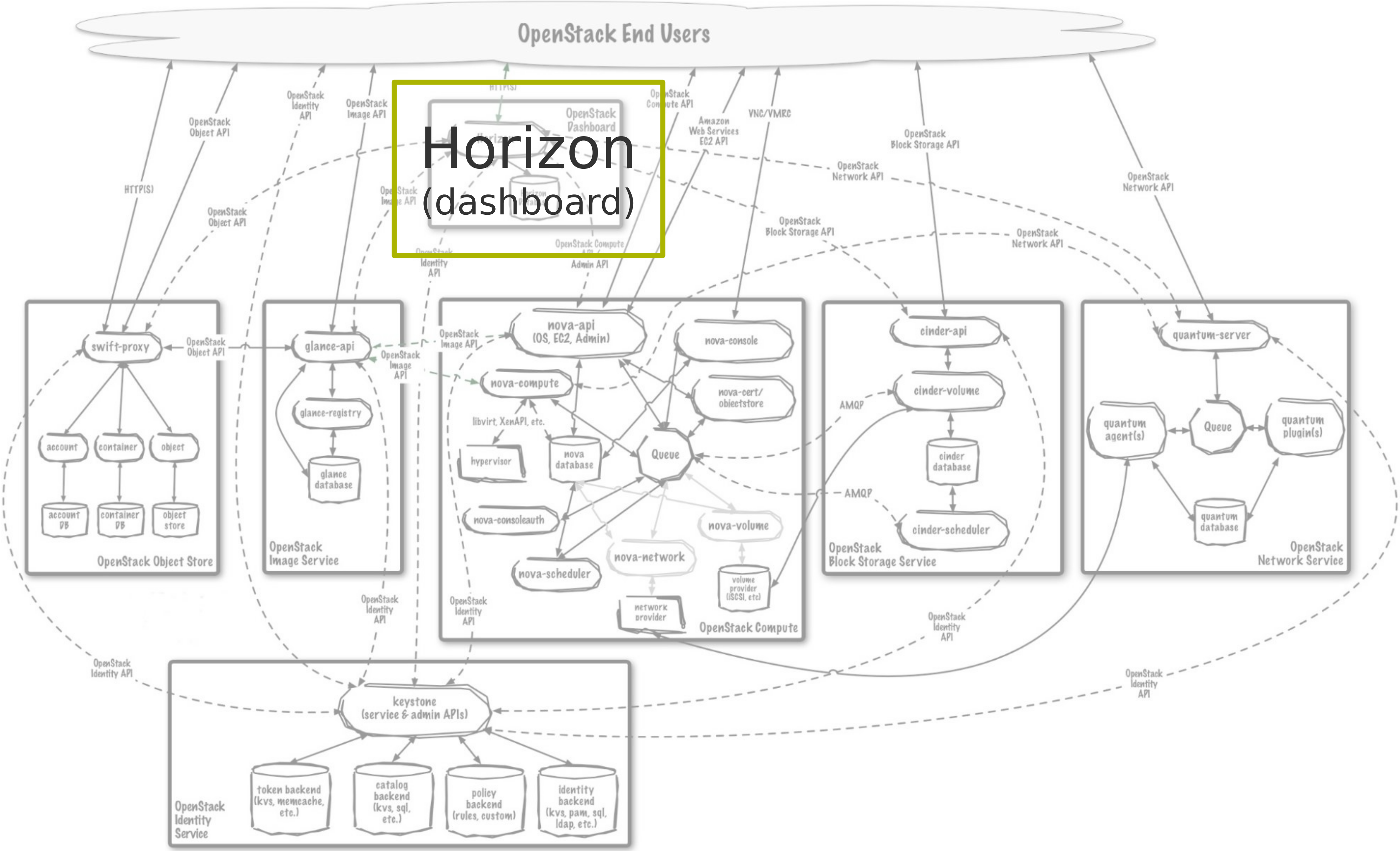
(block store)

Complex view:



Neutron
(networking)

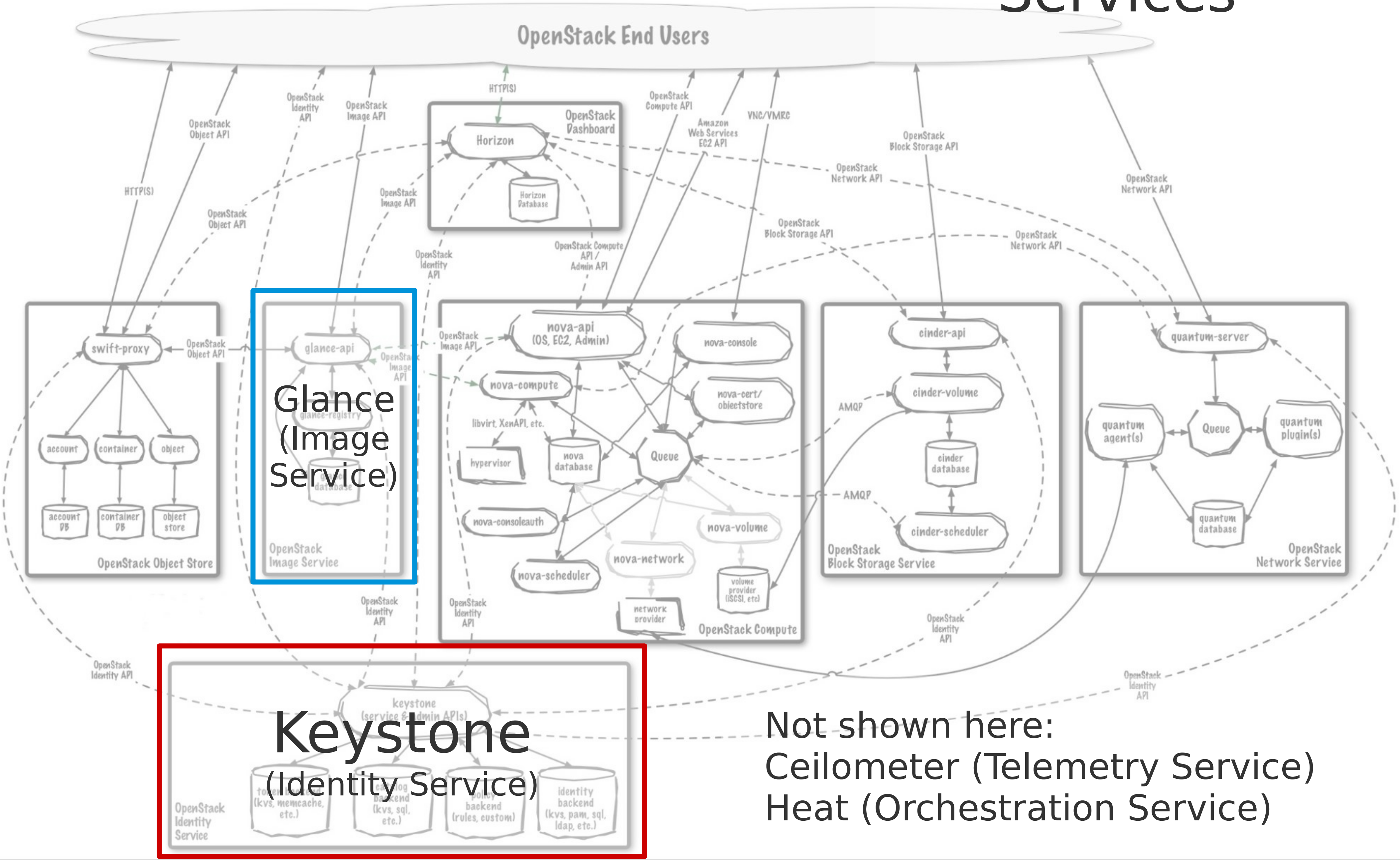
Complex view:



Horizon
(dashboard)

Complex view:

Shared Services



Glance (Image Service)

Keystone (Identity Service)

Not shown here:
Ceilometer (Telemetry Service)
Heat (Orchestration Service)

What can Samba do to complement or enhance the OpenStack experience ?

Samba operates in 2 areas, the classic File Server space and the Identity Management space with the Samba AD Domain Controller

File Services:

- classic SMB/clustered file serving for guests
- Image/block Storage (ex. when Hyper-V is used [uses SMB3])

Identity Management

- Windows Domain Controller for guests of the same tenant
- Infrastructure Identity Management, fronted by Keystone

Samba File Server for guests

Traditionally Samba is used as a reliable file server for windows Guests.

Samba on a cloud might provide exceptional scaling capabilities, using the underlying elasticity of the OpenStack cloud.
On-demand scaling of Samba CTDB clusters ?

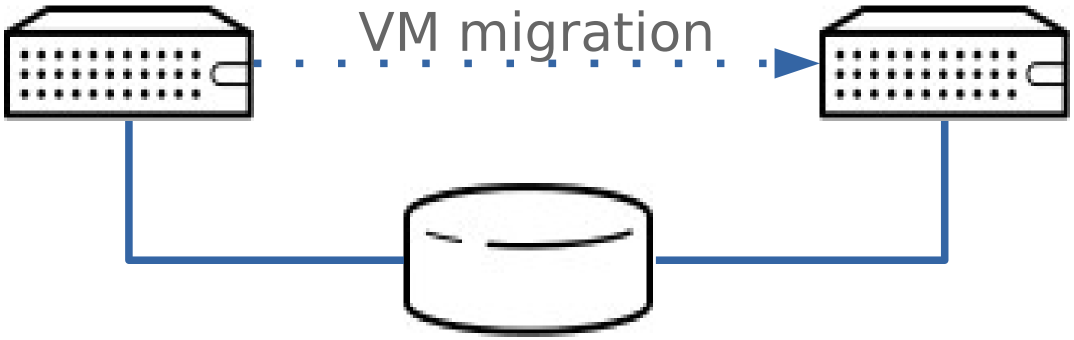
As the number of guests using Samba services increase or decrease the cloud infrastructure can automatically scale the number of nodes available.

Using a distributed filesystem underneath Samba, that can scale for performance, may prove to be a very interesting combination.

Samba File Server for the infrastructure

File-level/Block-level storage is used by compute nodes in order to support **live** migration of guest images from one node to another. Shared storage is necessary to allow multiple nodes to attach to the same image file an have proper concurrent access.

File based storage is used in OpenStack with NFS and GlusterFS, and experimentally with Ceph. This is an area where Samba vendors may want to invest to make SMB a viable option, especially in the case where Hyper-V is used as Hypervisor.



NFS, GlusterFS, Ceph or Samba ?

Samba Domain Controller for guests

Using Samba as a Domain Controller for the cloud is almost straightforward, however there are small twists in this case:

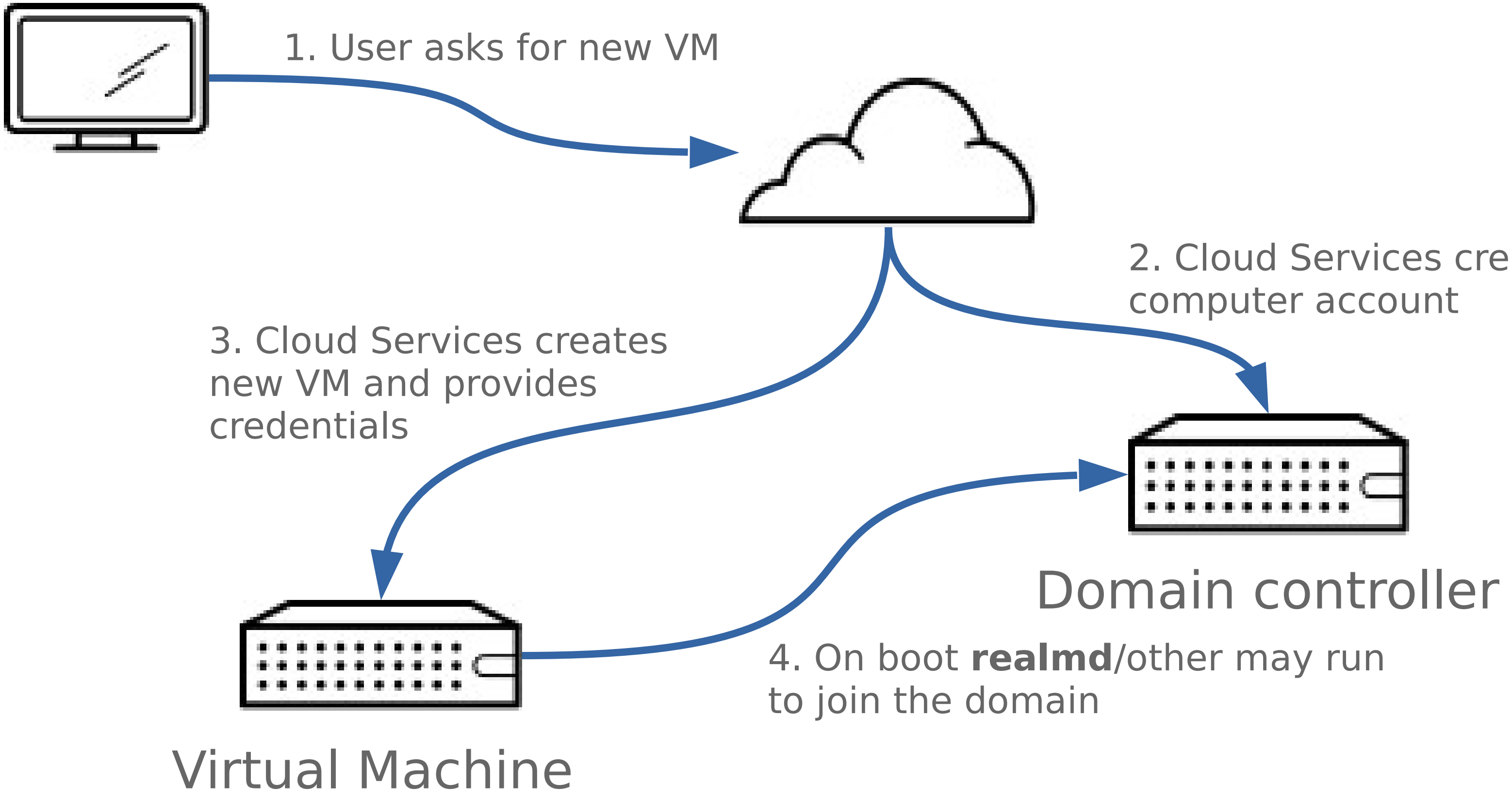
- guests are **very** dynamic, a VM can be created and destroyed in a matter of minutes in a cloud environment.

Open issues:

- how do we join a tenant domain seamlessly but securely when the guest is created ?

- how to reuse machine credentials when a guest is recreated ? (important to avoid service disruption with kerberos)

Cloud driven domain joins



1. User asks for new VM

2. Cloud Services create computer account

3. Cloud Services creates new VM and provides credentials

4. On boot **realmd**/other may run to join the domain

FreeIPA supports pre-creating inactive computer accounts with an OTP password to be changed at join. **realmd** can be used for enrolling machines similarly into a Samba-AD environments.

Samba AD for infrastructure services

In private or hybrid clouds a tenant may want to keep using their identity management infrastructure to extend access to cloud services.

This means re-using enterprise identities for direct access to OpenStack services, in order to create and spin guests on demand.

Windows clients joined to MS Active Directory	Windows clients joined to a Samba AD domain	Heterogeneous clients
Samba AD or FreeIPA in **trusted** domain	Samba AD in same domain or FreeIPA in **trusted** domain	Anything goes: Samba, FreeIPA, LDAP, Krb5, ...

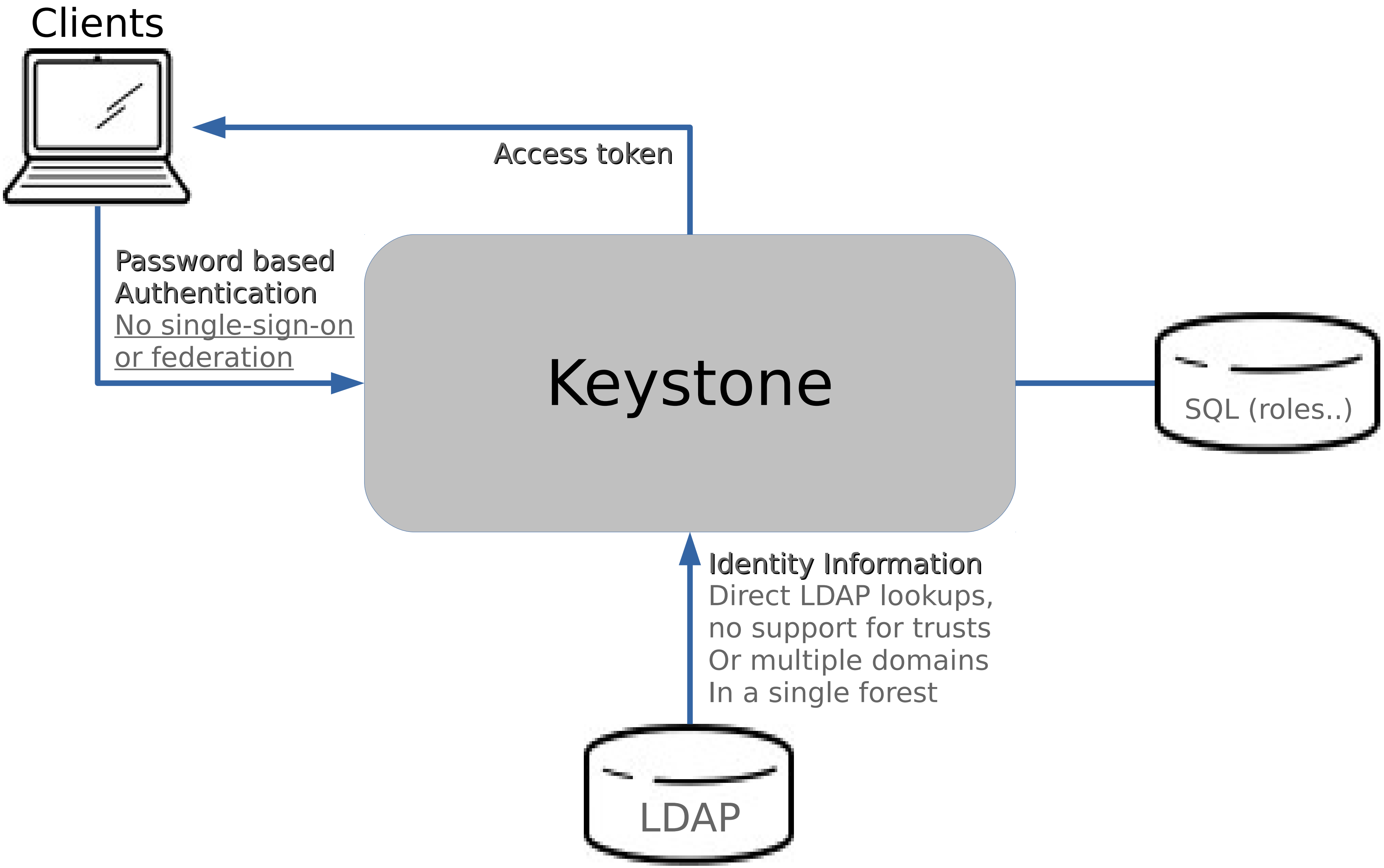
Identity Management in OpenStack

Authentication and authorization for OpenStack services are managed via a service called **Keystone**.

Keystone is often improperly seen as an Identity Manager service because it brokers this function, but we have been working in the past year to properly frame it in its natural authorization service role and leave the real identity management function to more mature services.

Our idea is to leverage existing systems like Samba AD or FreeIPA to provide identity and authentication, since these systems can easily bridge directly or via trust relationships to enterprise identities eliminating the pain of managing another set of users and groups in the OpenStack infrastructure and allowing Single-Sign-On to OpenStack services.

Keystone Role (current status)



Clients

Access token

Password based Authentication

No single-sign-on or federation

Keystone

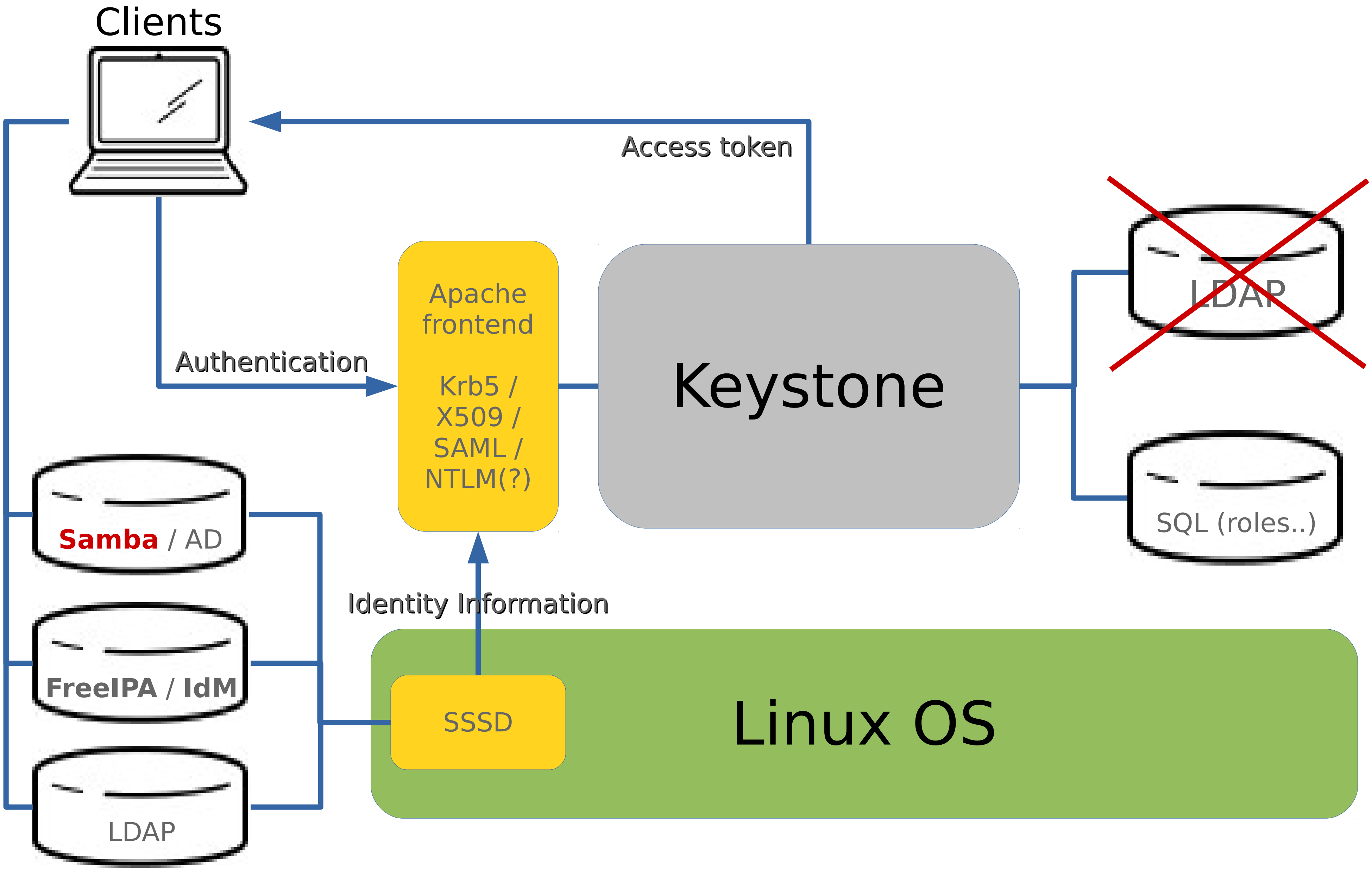
SQL (roles..)

Identity Information

Direct LDAP lookups, no support for trusts Or multiple domains In a single forest

LDAP

Keystone Role (current Red Hat vision)



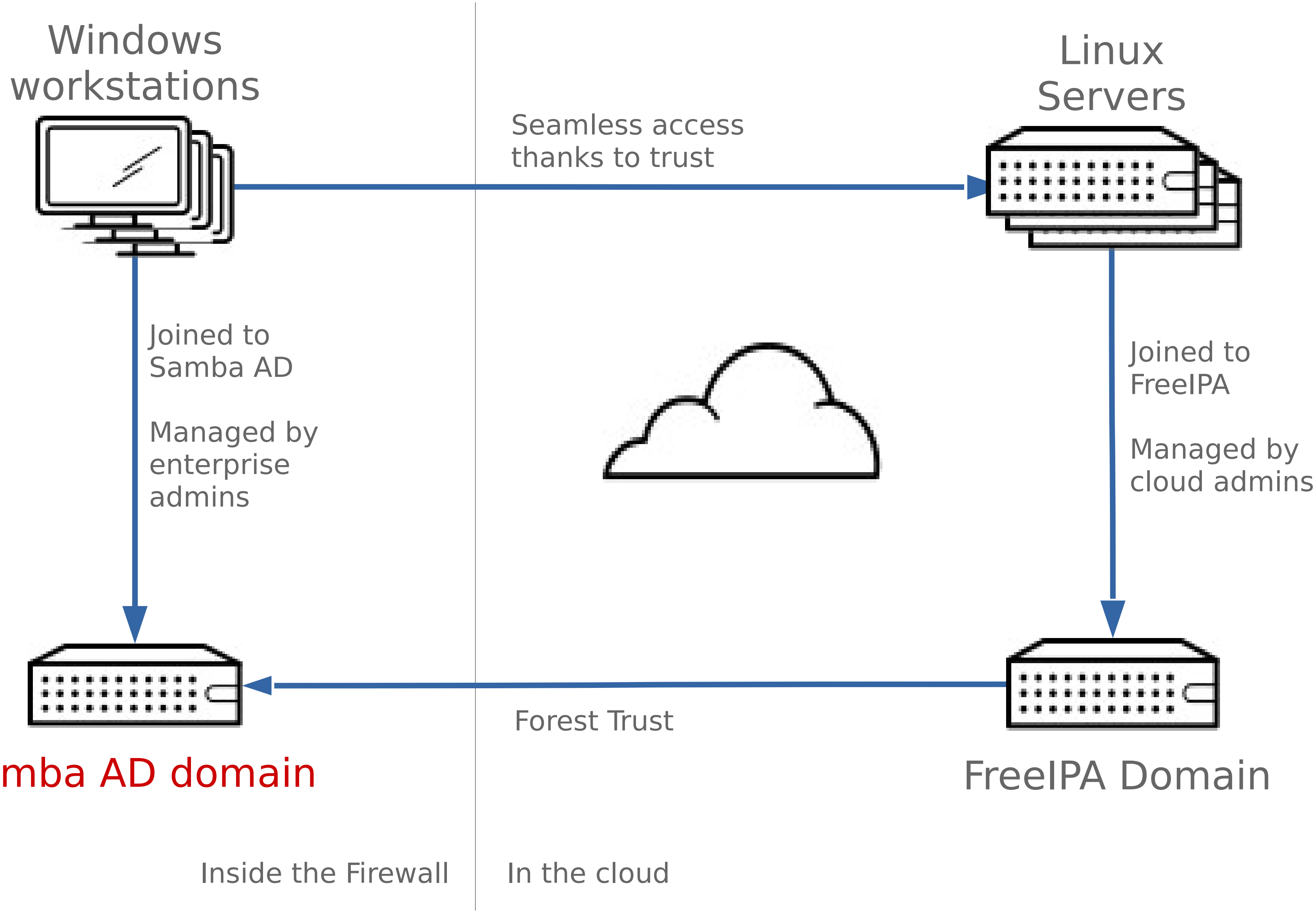
The importance of trust relationships

A cloud infrastructure can be seen as a “resource domain” as know in classic Windows Domain architectures.

It is very useful to have a completely separate administrative environment dedicated to the cloud infrastructure, yet use the enterprise user identities to authenticate and operate in this environment.

Not only Domain trusts, but also Forest trusts play a big role in allowing separation of duties, and confinement. Forest trusts are especially important as they restrict quite clearly what kind of information is allowed to flow. A compromised public cloud infrastructure will still be confined to public resources and not bleed “inside the corporate firewall”

Example deployment with trusts



Windows workstations

Seamless access thanks to trust

Linux Servers

Joined to Samba AD

Managed by enterprise admins

Joined to FreeIPA

Managed by cloud admins

Forest Trust

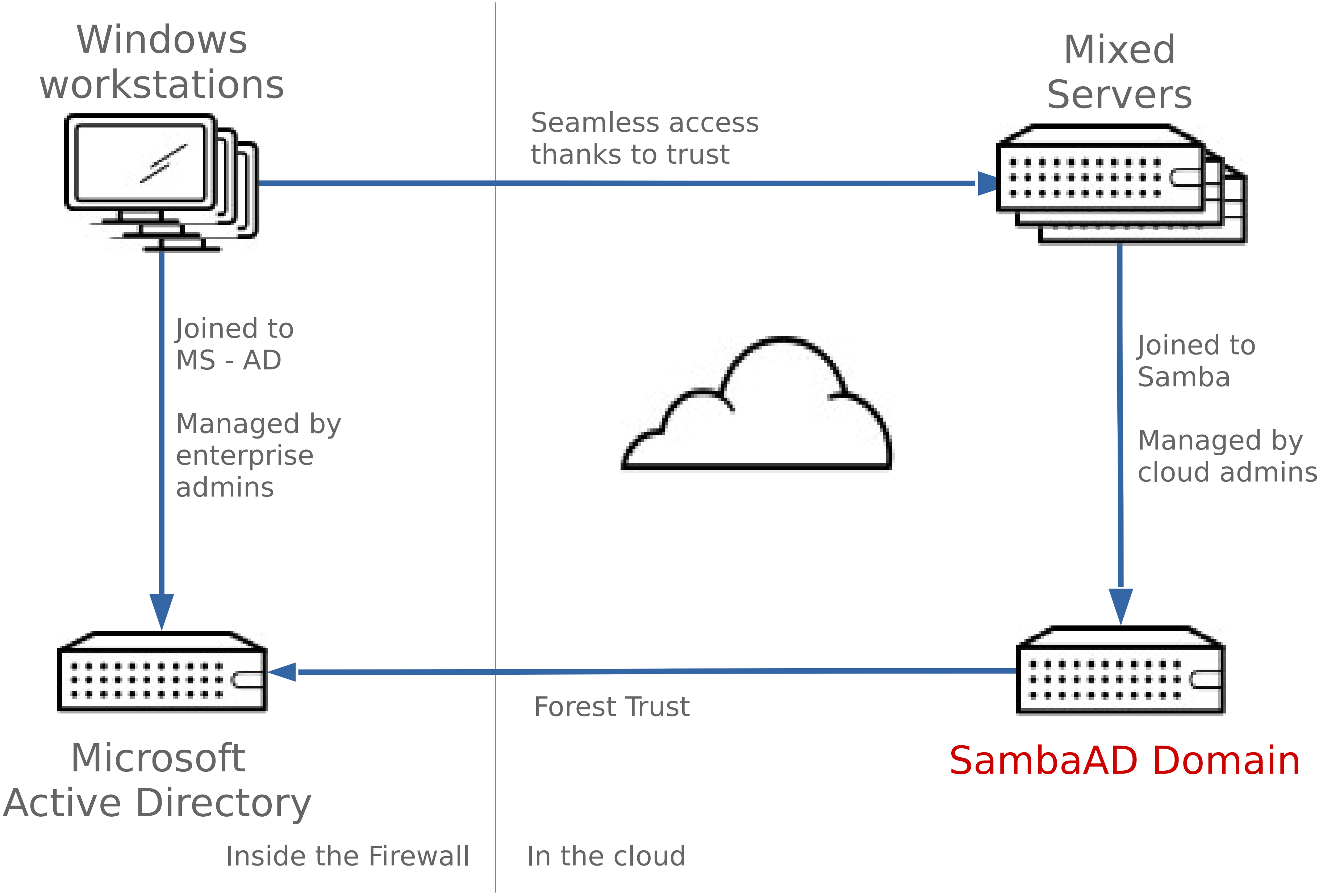
Samba AD domain

FreeIPA Domain

Inside the Firewall

In the cloud

Example deployment with trusts



Windows workstations

Seamless access thanks to trust

Mixed Servers

Joined to MS - AD

Managed by enterprise admins

Joined to Samba

Managed by cloud admins

Forest Trust

Microsoft Active Directory

SambaAD Domain

Inside the Firewall

In the cloud

TODO: File Server

The File Server is the more mature option so there isn't a lot of core work to do, but there is work to do to integrate Samba with OpenStack services to make it useful.

- Make Samba File Server an option for file/block store services in OpenStack (see Manila project ?)

- Build a CTDB driver for a highly scalable Samba file-store or block-store service, with automatic on-demand scaling capabilities.

Domain Controller next steps ?

The Identity Management space needs quite some more work.

* Add Forest Trust capabilities to Samba AD to support cloud deployments “resource domain”-style

- Improve computer-account life-cycle for elastic deployments, necessary for secure auto-enrollment

- Make it possible to use Krb5/NTLM(?) auth. with Horizon and Keystone for SingleSingOn access.

Questions ?

Contacts:
simo@samba.org / simo@redhat.com

OpenStack diagrams courtesy of openstack.org
http://www.openstack.org/software/

Try OpenStack from Red Hat at
http://openstack.redhat.com