UST Oversea Training Program 2016 Report

Amol Jaikar

This report gives summary of the work at Fermilab from Aug 1st to Sep 29th of 2016. The work is divided into two parts; first one is to design and create the OpenStack cloud infrastructure service and another is to study of federated identity management service.

1. OpenStack Design and Installation at FNAL

In this part, we have design the OpenStack framework as per FNAL requirement. OpenStack framework is distributed in many modules to enable flexibility for user. These modules are installed on controller, compute and storage nodes. For network, we have two options to deploy. First one is provider network, in which, virtual machine gets IP address from the administrator's assigned CIDR. Other option is self-service network, where user can create user's own CIDR. In this case, we have selected self-service provided network because of flexibility. In case of storage, OpenStack framework provides object-based and block-based storage. We have installed object and block based storage system. Figure 1 shows the architecture of the OpenStack framework, which consists of one controller node, five compute nodes and two storage nodes.

Controller node is centralized system to manage services like database, identity image computer management, networking management, storage, telemetry and many more. These services help to create infrastructure as a service. Image service provides image to the newly created virtual machine. Identity service provides identity to authenticate users as well as services to access. Telemetry service provides monitoring of virtual machines, billing and benchmarking. Swift and Cinder provides object and block based storage system respectively. You can attach external storage to virtual machine by using Cinder. Management network (private network) is used to communicate between different components as well as different services of the OpenStack. Provider network provides internet access to the instances. With the help of document provided by OpenStack community, we have successfully installed infrastructure as a service.

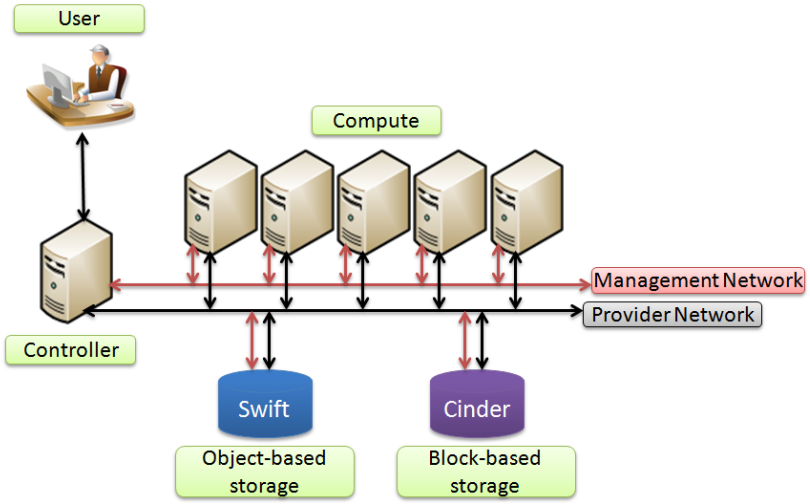

Figure 1. OpenStack Architecture at FNAL

While installing OpenStack framework, we encountered some problem. Problem started with puppet automatic configuration management tool. We have to shut-down the puppet daemon to solve that issue temporarily. Next problem is about FNAL security daemon, it runs periodically to scan DNS server. As we have installed network management module on compute node, it creates and starts *dnsmasq* daemon to work as a DHCP server to provide the IP address to newly created virtual machine.

2. Federated Identity Management Service

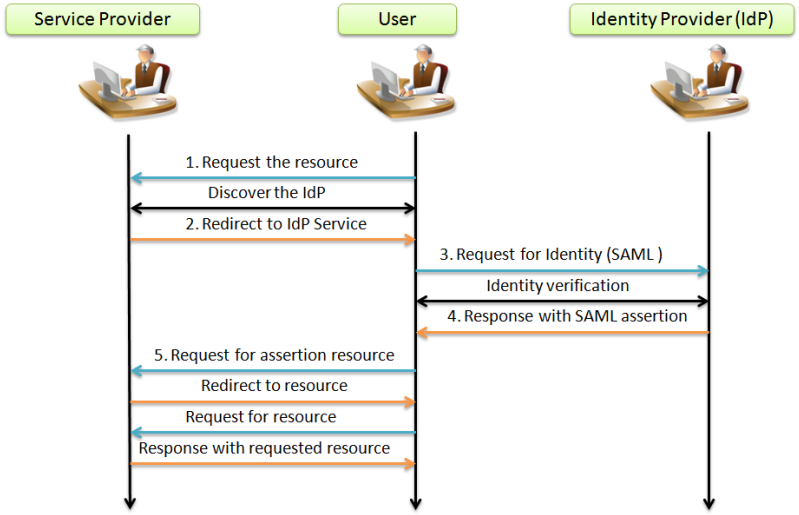

Figure 2. Federated Identity Management service

FNAL is already installed OpenNebula cloud named as Fermicloud. In order to provide the access to Fermicloud users, they have to add their user's identity to the newly created OpenStack cloud, which involves considerable work. To avoid this tedious work, OpenStack has facility to provide temporary access to these users for certain resources. Figure 2 shows the communication mechanism of federated identity service.

User requests for the recourse to the service provider. This service provider can be public cloud or private cloud like another OpenStack. This service provider redirect user's request to identity provider like Active Directory Federation Service (ADFS) to get Single Sign-On (SSO) credentials. These credentials will be active for certain amount of time. Later, user can use the same credentials to access or create the resources. Using these credentials (SAML assertion), users can request the resources. The service provider gets the SAML assertion credentials from the user. Now, service provider can provide the resources by using this credential.