Cloud Application Development

Week 4

Name: - Nilesh Verma
SAP Id.: - 500087239
Batch: - B4 Non-Hons CC&VT
Roll No.: - R2142201812

Keystone:

Keystone is an Openstack service which provides a unified interface for managing the authentication and authorization services. It basically acts as the bridge between the cloud services and user identity. This service provides API client authentication, service discovery, etc. using the OpenStack's Identity API. The Keystone providers various authentication methods like token authentication, password authentication and multi-factor authentication which allows administrator to authorize the user to use the resources given according to roles. All this work is done by the Identity API

Identity API Operations:

- Authentication
- Token Management
- Credentials
- Domains
- Domain Configuration
- Groups
- Policies
- Project
- Project Tags
- Regions
- Roles
- System role assignment
- Service catalog and endpoints
- Unified limits
- Users
- Os-Inherit
- Os-pki (Deprecated)

CLI Programming:

Keystone provides a command line interface (CLI) that allows users to perform administrative tasks and manage user identities and access policies from the command line. Keystone CLI is based on the OpenStack command line client and provides a consistent interface across OpenStack services.

To use the Keystone CLI, a user must first provide credentials to authenticate with her Keystone. Once authenticated, users can perform various administrative tasks such as: For example, creating users and groups, managing access policies, configuring authentication methods, and more.

Some of the Openstack CLI commands are:

- To create a new user: “openstack user create <username> - -password <password>”
- To create a project: “openstack project create <project_name>”
- cat keystonerc_admin
- source keystonerc_admin
- openstack endpoint list
- openstack endpoint show <Endpoint_lD>
- openstack catalog list
- openstack endpoint list
- openstack endpoint show <Endpoint_lD>
- openstack project create <project_name>
- openstack project show <project_name>
- openstack project set --description "description_text" <project_name>
- openstack user create --project <project_name> --password-prompt <user_name>
- openstack role list
- openstack role assignment list --project newproject --user developer01
- openstack role add --project <project_name> --user <user_name> _member
- openstack role add --project <project_name> --user <user_name> admin
- openstack command list I grep openstack-identity -A 130

Instance Creation:

In Openstack Instance can be create in two ways:

1) Using Horizon Dashboard
   - Log in to the Horizon dashboard and navigate to the Project tab.
   - Click on the Compute tab and select the Instances option from the dropdown menu.
   - Click on the Launch Instance button to start the instance creation process.
   - Choose the desired image for the instance. An image is a pre-configured template for a virtual machine that includes an operating system and other software.
   - Choose the desired flavor for the instance. A flavor is a set of specifications for the virtual hardware resources of the instance, such as CPU, memory, and disk space.
   - Set the instance name, and choose the availability zone and other options as needed.
   - Set the network configuration for the instance, such as the network name, subnet, and IP address assignment method.
   - Set the security group configuration for the instance, such as the inbound and outbound traffic rules.
   - Choose the key pair for the instance, which will be used to securely access the instance later on.
   - Click on the Launch Instance button to create the instance.
   - Wait for the instance to be created and become active. You can monitor the progress of the instance creation process on the Instances tab.

2) Using Keystone CLI
   - Log in to the OpenStack environment using the CLI and authenticate with Keystone.
   - Create a new key pair for the instance, which will be used to securely access the instance later.Command: “openstack keypair create <key_pair_name> > <key_pair_file> “
   - Create a new security group for the instance, which will be used to control inbound and outbound traffic to the instance. Command:” openstack security group create <security_group_name>”
   - Add rules to the security group to allow inbound and outbound traffic to the instance. Command: “openstack security group rule create --protocol tcp --dst-port 22:22 --remote-ip 0.0.0.0/0 <security_group_name>”. This command allows SSH traffic (TCP protocol, port 22) from any IP address to the instance.
   - Create a new compute instance by specifying the desired flavor, image, key pair, security group, and other options. Command: “openstack server create --flavor <flavor_name> --image <image_name> --key-name <key_pair_name> --security-group <security_group_name> <instance_name> ”
   - Wait for the instance to be created and become active. To check the status of Instance you can use this command: “openstack server show <instance_name>”