1. **准备**
2. CentOs 7 操作系统
3. 已正确运行的Kilo版本OpenStack系统
4. 对OpenStack有初步了解
5. **OpenStack通信概述**

Openstack由keystone、nova、neutron等各自独立的组件组成，各个组件之间的通信分为两种：一种是基于AMQP（Advanced Message Queuing Protocol ）的消息队列机制；一种是基于REST风格的Http通信：

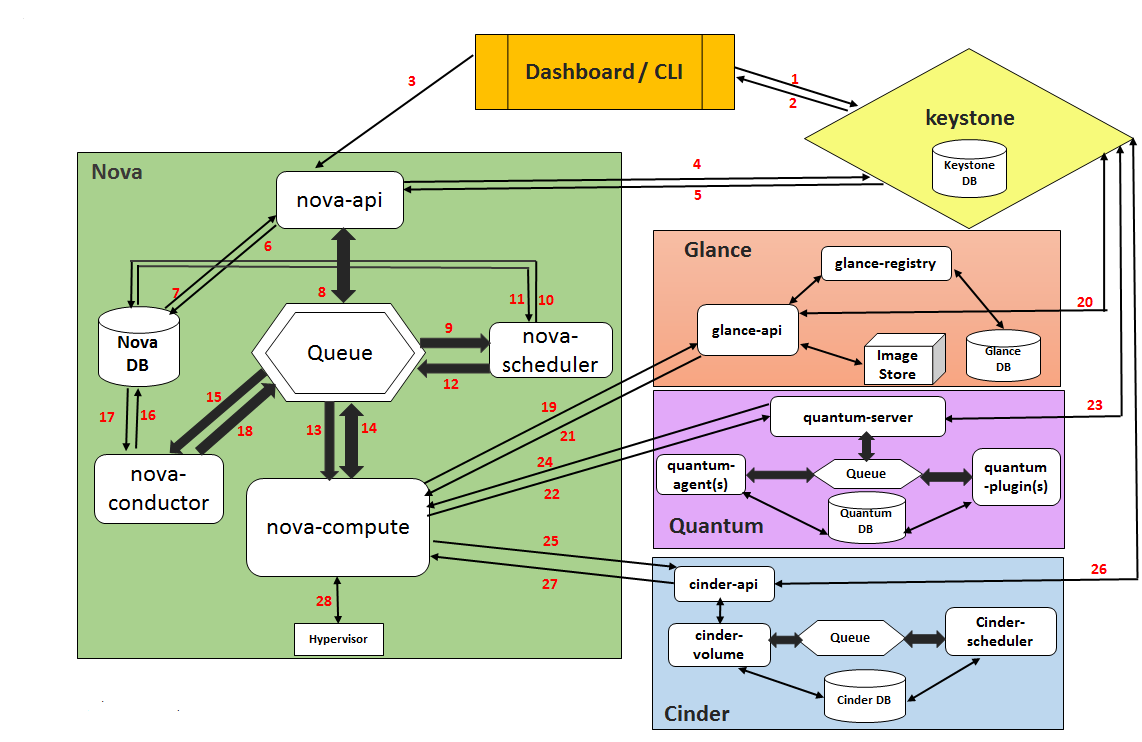


图1 openstack组件通信

组件内部通信基于AMQP或者Http，组件之间的通信基于Http。为了加强openstack平台安全，本文讲解如何使用ssl加密组件之间的Http通信。

1. **keystone配置SSL**

keystone作为openstack的Identity Service，为User访问资源时提供认证服务。

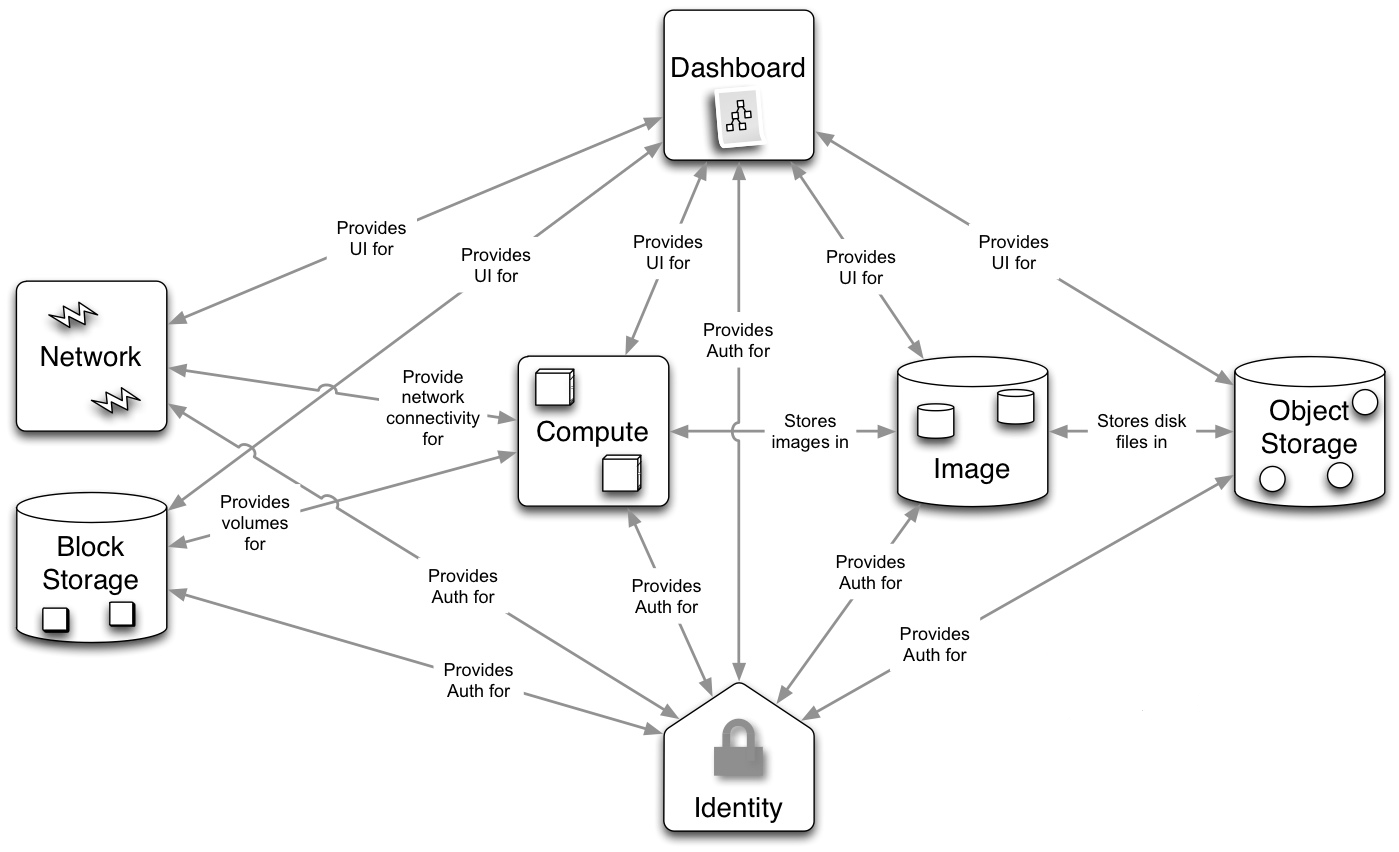


图2 keystone认证

因为keystone会与其他所有组件通信，因此先配置好keystone的ssl加密，然后再配置其他组件http的ssl加密。Keystone有两种运行方式：一种是使用自带的Eventlet服务器运行（默认运行方式）keystone；另一种是使用Apache Httpd运行keystone。根据实际情况选择下面其一。

**1、Eventlet运行Keystone**

**（1）生成自签名证书：**

keystone-manage pki\_setup --keystone-user keystone --keystone-group keystone

默认保存在/etc/keystone/ssl/cert和private中。

/etc/keystone/ssl/certs/

/etc/keystone/ssl/certs/

/etc/keystone/ssl/private/

1. **修改权限：**

chown -R keystone:keystone/etc/keystone/ssl

1. **修改keystone配置文件：/etc/keystone/keystone.conf**

[eventlet\_server\_ssl]

enable = true

certfile = /etc/keystone/ssl/certs/signing\_cert.pem

keyfile = /etc/keystone/ssl/private/signing\_key.pem

ca\_certs = /etc/keystone/ssl/certs/ca.pem

1. **创建SSL endpoint**

需要先创建SSL 加密的endpoint然后再删旧的（非加密）endpoint，否则会因为找不到认证端口，导致后续操作无法进行。推荐先创建完所有组件SSL加密的endpoint，测试openstack在加密情况下能正常运行再删除旧的endpoint。

openstack endpoint create --publicurl https://lingyuecloud:5000/v2.0 --internalurl https://lingyuecloud:5000/v2.0 --adminurl https://lingyuecloud:35357/v2.0 --region RegionOne identity

1. **删除http endpoint**

openstack endpoint delete endpointID

1. **添加、修改环境变量**

export OS\_AUTH\_URL=https://lingyuecloud:35357/v3

export OS\_CACERT=/etc/keystone/ssl/certs/ca.pem

1. **重启keystone服务**

sytemctl restart openstack-keystone

1. **验证**

keystone endpoint list

**2、keystone在httpd上运行**

**（1）安装mod\_ssl包**

yum install mod\_ssl -y

1. **修改cert\_subject默认值**

/etc/keystone/keystone.conf

cert\_subject = /C=CN/ST=ShiChuan/L=Chengdu/O=lingyuecloud/CN=lingyue

注：CN为验证ca证书时访问的服务器（name或者ip）

**（3）生成证书等**

keystone-manage pki\_setup --keystone-user keystone --keystone-group keystone

默认保存在/etc/keystone/ssl/cert和private中。

/etc/keystone/ssl/certs/ca.pem

/etc/keystone/ssl/certs/signing\_cert.pem

/etc/keystone/ssl/private/signing\_key.pem

**（4）修改权限：**

chown -R keystone:keystone/etc/keystone/ssl

**（5）修改****/etc/httpd/conf.d/wsgi-keystone.conf添加如下内容：**

Listen 5000

Listen 35357

<VirtualHost lingyuecloud:5000>

WSGIDaemonProcess keystone-public processes=5 threads=1 user=keystone group=keystone display-name=%{GROUP}

WSGIProcessGroup keystone-public

SSLEngine on

SSLVerifyDepth 1

SSLProtocol +TLSv1 +TLSv1.1 +TLSv1.2

SSLCipherSuite HIGH:!RC4:!MD5:!aNULL:!eNULL:!EXP:!LOW:!MEDIUM

SSLCertificateFile /etc/keystone/ssl/certs/signing\_cert.pem

SSLCertificateKeyFile /etc/keystone/ssl/private/signing\_key.pem

SSLCACertificateFile /etc/keystone/ssl/certs/ca.pem

#SSLVerifyClient require

WSGIScriptAlias / /var/www/cgi-bin/keystone/main

WSGIApplicationGroup %{GLOBAL}

WSGIPassAuthorization On

LogLevel info

ErrorLogFormat "%{cu}t %M"

ErrorLog /var/log/httpd/keystone-error.log

CustomLog /var/log/httpd/keystone-access.log combined

</VirtualHost>

<VirtualHost lingyuecloud:35357>

WSGIDaemonProcess keystone-admin processes=5 threads=1 user=keystone group=keystone display-name=%{GROUP}

WSGIProcessGroup keystone-admin

SSLEngine on

SSLVerifyDepth 1

SSLProtocol +TLSv1 +TLSv1.1 +TLSv1.2

SSLCipherSuite HIGH:!RC4:!MD5:!aNULL:!eNULL:!EXP:!LOW:!MEDIUM

SSLCertificateFile /etc/keystone/ssl/certs/signing\_cert.pem

SSLCertificateKeyFile /etc/keystone/ssl/private/signing\_key.pem

SSLCACertificateFile /etc/keystone/ssl/certs/ca.pem

#SSLVerifyClient require

WSGIScriptAlias / /var/www/cgi-bin/keystone/admin

WSGIApplicationGroup %{GLOBAL}

WSGIPassAuthorization On

LogLevel info

ErrorLogFormat "%{cu}t %M"

ErrorLog /var/log/httpd/keystone-error.log

CustomLog /var/log/httpd/keystone-access.log combined

</VirtualHost>

注：lingyuecloud为服务器名

1. **重启httpd服务**

systemctl restart httpd

1. **验证**

openstack endpoint list

**四、Nova配置SSL**

**（1）复制证书**

mkdir /etc/nova/ssl

\cp /etc/keystone/ssl/certs/signing\_cert.pem /etc/nova/ssl/

\cp /etc/keystone/ssl/certs/ca.pem /etc/nova/ssl/

\cp /etc/keystone/ssl/private/signing\_key.pem /etc/nova/ssl/

**（2）修改权限**

chown -R nova:nova/etc/nova/ssl

**（3）修改NOVA配置文件**

**/etc/nova/nova.conf**

[keystone\_authtoken]

auth\_uri=https://lingyuecloud:5000/v2.0

cafile=/etc/nova/ssl/ca.pem

insecure=true

auth\_host=lingyuecloud

auth\_protocol=https

identity\_uri=https://lingyuecloud:35357

**（4）重启NOVA服务**

service openstack-nova-api restart

service openstack-nova-compute restart

service openstack-nova-scheduler restart

service openstack-nova-cert restart

service openstack-nova-conductor restart

**（5）指定NOVA使用的证书**

/etc/nova/nova.conf

[DEFAULT]

enabled\_ssl\_apis = osapi\_compute

ssl\_cert\_file=/etc/nova/ssl/signing\_cert.pem

ssl\_key\_file=/etc/nova/ssl/signing\_key.pem

**（6）创建SSL endpoint**

openstack endpoint create --publicurl https://lingyuecloud:8774/v2/%\(tenant\_id\)s --internalurl https://lingyuecloud:8774/v2/%\(tenant\_id\)s --adminurl https://lingyuecloud:8774/v2/%\(tenant\_id\)s --region RegionOne compute

**（7）删除http endpoint**

openstack endpoint delete endpointID

**（8）重启NOVA服务**

**（9）配置NOVA以SSL方式访问其它组件**

/etc/nova/nova.conf

[cinder]

endpoint\_template=https://lingyuecloud:8776/v2/%(project\_id)s

cafile=/etc/nova/ssl/ca.pem

[glance]

protocol=https

api\_servers=https://lingyuecloud:9292

api\_insecure=true

[neutron]

url=https://lingyuecloud:9696

admin\_auth\_url=https://lingyuecloud:5000/v2.0

cafile=/etc/nova/ssl/ca.pem

insecure=true

**（10）验证**

nova service-list

**五、Glance 配置SSL**

**（1）复制证书**

mkdir /etc/glance/ssl

\cp /etc/keystone/ssl/certs/signing\_cert.pem /etc/glance/ssl/

\cp /etc/keystone/ssl/certs/ca.pem /etc/glance/ssl/

\cp /etc/keystone/ssl/private/signing\_key.pem /etc/glance/ssl/

**（2）修改权限**

chown -R glance:glance /etc/glance/ssl

**（3）修改Glance认证方式**

**vi /etc/glance/glance-api.conf**

[keystone\_authtoken]

auth\_uri=https://lingyuecloud:5000/v2.0

cafile=/etc/glance/ssl/ca.pem

insecure=true

auth\_host= lingyuecloud

auth\_protocol=https

identity\_uri=https://lingyuecloud35357

**vi /etc/glance/glance-registry.conf**

[keystone\_authtoken]

auth\_uri=https://lingyuecloud5000/v2.0

cafile=/etc/glance/ssl/ca.pem

insecure=true

auth\_host= lingyuecloud

auth\_protocol=https

identity\_uri=https://lingyuecloud:35357

**vi /etc/glance/glance-cache.conf**

[DEFAULT]

auth\_url=https://lingyuecloud:5000/v2.0

**（4）重启Glance服务**

service openstack-glance-api restart

service openstack-glance-registry restart

**（5）指定Glance使用的证书**

**vi /etc/glance/glance-api.conf**

[DEFAULT]

cert\_file=/etc/glance/ssl/signing\_cert.pem

key\_file=/etc/glance/ssl/signing\_key.pem

registry\_client\_protocol=https

registry\_client\_ca\_file=/etc/glance/ssl/ca.pem

**vi /etc/glance/glance-registry.conf**

[DEFAULT]

cert\_file=/etc/glance/ssl/signing\_cert.pem

key\_file=/etc/glance/ssl/signing\_key.pem

**（6）创建SSL endpoint**

openstack endpoint create --publicurl https://lingyuecloud:9292 --internalurl https://lingyuecloud:9292 --adminurl https://lingyuecloud:9292 --region RegionOne image

**（7）删除http endpoint**

opentack endpoint delete endpointID

**（8）重启Glance服务**

**（9）配置Glance以SSL方式访问其它组件**

**vi /etc/glance/glance-api.conf**

[glance\_store]

cinder\_endpoint\_template=https://lingyuecloud:8776/v2/%(project\_id)s

**vi /etc/glance/glance-registry.conf**

[glance\_store]

cinder\_endpoint\_template=https://lingyuecloud:8776/v2/%(project\_id)s

**（10）验证**

glance image-list

nova image-list

**注：系统镜像推荐使用raw**

**六、Cinder配置SSL**

**（1）复制证书**

mkdir /etc/cinder/ssl

cp /etc/keystone/ssl/certs/signing\_cert.pem /etc/cinder/ssl/

cp /etc/keystone/ssl/certs/cp.pem /etc/cinder/ssl/

cp /etc/keystone/ssl/private/signing\_key.pem /etc/cinder/ssl/

**（2）修改权限：**

chown -R cinder:cinder/etc/cinder/ssl

**（3）修改Cinder认证方式**

vi /etc/cinder/ cinder.conf

[keystone\_authtoken]

auth\_uri = https://lingyuecloud:5000

auth\_url = https://lingyuecloud:35357

cafile=/etc/cinder/ssl/ca.pem

insecure = true

auth\_host = lingyuecloud

auth\_protocol = https

identity\_uri=https://lingyuecloud:35357

**（4）重启Cinder服务**

service openstack-cinder-api restart

service openstack-cinder-scheduler restart

service openstack-cinder-volume restart

**（5）指定Cinder使用的证书**

vi /etc/cinder/cinder.conf

[DEFAULT]

ssl\_cert\_file=/etc/cinder/ssl/signing\_cert.pem

ssl\_key\_file=/etc/cinder/ssl/signing\_key.pem

**（6）创建SSL endpoint**

openstack endpoint create --publicurl https://*lingyuecloud*:8776/v2/%\(tenant\_id\)s --internalurl https://*lingyuecloud*:8776/v2/%\(tenant\_id\)s --adminurl https://*lingyuecloud*:8776/v2/%\(tenant\_id\)s --region RegionOne volume

openstack endpoint create --publicurl https://*lingyuecloud*:8776/v2/%\(tenant\_id\)s --internalurl https://*lingyuecloud*:8776/v2/%\(tenant\_id\)s --adminurl https://*lingyuecloud*:8776/v2/%\(tenant\_id\)s --region RegionOne volumev2

**（7）删除http endpoint**

openstack endpoint delete endpointID

**（8）重启Cinder服务**

**（9）配置Cinder以SSL方式访问其它组件**

/etc/cinder/cinder.conf

[DEFAULT]

glance\_host = lingyuecloud

glance\_api\_servers = https://lingyuecloud:9292

glance\_api\_insecure = true

glance\_ca\_certificates\_file = /etc/cinder/ssl/ca.pem

nova\_endpoint\_template = https://lingyuecloud8774/v2/%(project\_id)s

nova\_ca\_certificates\_file = /etc/cinder/ssl/ca.pem

nova\_api\_insecure = true

**（10）验证**

cinder service-list

nova list

**七、Neutron配置SSL**

**（1）复制证书**

mkdir /etc/neutron/ssl

cp /etc/keystone/ssl/certs/signing\_cert.pem /etc/neutron/ssl/

cp /etc/keystone/ssl/certs/cp.pem /etc/neutron/ssl/

cp /etc/keystone/ssl/private/signing\_key.pem /etc/neutron/ssl/

**（2）修改权限：**

chown -R neutron:neutron /etc/neutron/ssl

**（3）修改Neutron认证方式**

**vi /etc/neutron/metadata\_agent.ini**

auth\_url = https://lingyuecloud:5000/v2.0

**vi /etc/neutron/neutron.conf**

[keystone\_authtoken]

auth\_uri = https://lingyuecloud:5000/v2.0

identity\_uri = https://lingyuecloud:35357

cafile=/etc/neutron/ssl/ca.pem

insecure=true

auth\_host=lingyuecloud

auth\_protocol=https

**（4）重启cinder服务**

service neutron-server restart

service neutron-dhcp-agent restart （控制节点不需要重启该服务）

service neutron-l3-agent restart

service neutron-metadata-agent restart

service neutron-lbaas-agent restart

service neutron-openvswitch-agent restart

**（5）指定Neutron使用的证书**

/etc/neutron/neutron.conf

[DEFAULT]

use\_ssl = True

ssl\_cert\_file = /etc/neutron/ssl/signing\_cert.pem

ssl\_key\_file = /etc/neutron/ssl/signing\_key.pem

**（6）创建SSL endpoint**

openstack endpoint create --publicurl https://lingyuecloud:9696 --adminurl https://lingyuecloud:9696 --internalurl https://lingyuecloud:9696 --region RegionOne network

**（7）删除http endpoint**

openstack endpoint delete endpointID

**（8）重启Neutron服务**

**（9）配置Neutron以SSL方式访问其它组件**

vi /etc/neutron/neutron.conf

[DEFAULT]

nova\_url = https://lingyuecloud:8774/v2

nova\_admin\_auth\_url =https://lingyuecloud:5000/v2.0

[nova]

cafile = /etc/neutron/ssl/ca.pem

**（10）验证**

neutron agent-list

nova net-list

**八、Horizon配置SSL**

**vi /etc/openstack-dashboard/local\_settings**

OPENSTACK\_KEYSTONE\_URL = "https://lingyuecloud:5000/v2.0"

OPENSTACK\_SSL\_NO\_VERIFY = True

OPENSTACK\_SSL\_CACERT = '/etc/keystone/ssl/certs/ca.pem'

重启httpd服务