**Configuring OpenSSL in OpenStack Queens**

**Enable SSL and Configure SSL**

* Enable SSL as follows:

# a2enmod ssl

# service apache2 restart

# sudo a2ensite default-ssl.conf

* Create SSL using OpenSSL as follows:

# mkdir /etc/apache2/ssl/

# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/openstack.key -out /etc/apache2/ssl/openstack.crt

* Configure SSL as follows:

# sed -i "s/^\(\s\*SSLCertificateFile\).\*/\1 \/etc\/apache2\/ssl\/openstack.crt/" /etc/apache2/sites-available/default-ssl.conf

# sed -i "s/^\(\s\*SSLCertificateKeyFile\).\*/\1 \/etc\/apache2\/ssl\/openstack.key/" /etc/apache2/sites-available/default-ssl.conf

* For redirect http traffic to https, update /etc/apache2/sites-available/000-default.conf as follows:

# sed -i '/^\(\s\*DocumentRoot\)/a\ redirect / https://controller' /etc/apache2/sites-available/000-default.conf

# service apache2 restart

**Change OpenStack Service endpoint URL**

Change the endpoint URLs from https to https in endpoints table in the keystone Database.

**Figure 1:** OpenStack endpoints

If URL changing is done, Populate the Identity service database using the command given below:

# su -s /bin/sh -c "keystone-manage db\_sync" keystone

**SSL for keystone endpoints**

* Update the /etc/apache2/sites-available/keystone.conf file as follows:

# sed -i "s/^\(\s\*SSLCertificateFile\).\*/\1 \/etc\/apache2\/ssl\/openstack.crt/" /etc/apache2/sites-available/keystone.conf

# sed -i "s/^\(\s\*SSLCertificateKeyFile\).\*/\1 \/etc\/apache2\/ssl\/openstack.key/" /etc/apache2/sites-available/ keystone.conf

# service apache2 restart

* Update the admin-openrc file as follows:

# sed -i -e 's/export OS\_AUTH\_URL=http:\/\/controller:5000\/v3/export OS\_AUTH\_URL=https:\/\/controller:5000\/v3/g' admin-openrc

* Check the service as follows:

# . admin-openrc

# openstack token issue --insecure

**Figure 2:** OpenStack token issue

**SSL for glance endpoints**

* Update the /etc/glance/glance-api.conf file as follows:

# crudini --set /etc/glance/glance-api.conf DEFAULT cert\_file /etc/apache2/ssl/openstack.crt

# crudini --set /etc/glance/glance-api.conf DEFAULT key\_file /etc/apache2/ssl/openstack.key

# crudini --set /etc/glance/glance-api.conf keystone\_authtoken auth\_uri <https://controller:5000>

# crudini --set /etc/glance/glance-api.conf keystone\_authtoken auth\_url <https://controller:5000>

# crudini --set /etc/glance/glance-api.conf keystone\_authtoken certfile /etc/apache2/ssl/openstack.crt

# crudini --set /etc/glance/glance-api.conf keystone\_authtoken keyfile /etc/apache2/ssl/openstack.key

# crudini --set /etc/glance/glance-api.conf keystone\_authtoken insecure = true

* Update the /etc/glance/glance-registry.conf file as follows:

# crudini --set /etc/glance/glance-registry.conf DEFAULT cert\_file /etc/apache2/ssl/openstack.crt

# crudini --set /etc/glance/glance-registry.conf DEFAULT key\_file /etc/apache2/ssl/openstack.key

# crudini --set /etc/glance/glance-registry.conf conf keystone\_authtoken auth\_uri <https://controller:5000>

# crudini --set /etc/glance/glance-registry.conf keystone\_authtoken auth\_url <https://controller:5000>

# crudini --set /etc/glance/glance-registry.conf keystone\_authtoken certfile /etc/apache2/ssl/openstack.crt

# crudini --set /etc/glance/glance-registry.conf keyfile /etc/apache2/ssl/openstack.key

# crudini --set /etc/glance/glance-registry.conf insecure = true

* Restart the Image services as follows:

# service glance-registry restart

# service glance-api restart

* Check the service as follows:

# openstack image list –insecure

**Figure 3:** OpenStack image list

**SSL for nova endpoints**

* Update the /etc/nova/nova.conf file as follows:

# crudini –set /etc/nova/nova.conf DEFAULT ssl\_only = true

# crudini –set /etc/nova/nova.conf DEFAULT cert /etc/apache2/ssl/openstack.crt

# crudini –set /etc/nova/nova.conf DEFAULT key /etc/apache2/ssl/openstack.key

# crudini –set /etc/nova/nova.conf DEFAULT enabled\_ssl\_apis osapi\_compute,metadata

# crudini –set /etc/nova/nova.conf glance api\_servers https://controller:9292

# crudini –set /etc/nova/nova.conf glance certfile /etc/apache2/ssl/openstack.crt

# crudini –set /etc/nova/nova.conf glance keyfile /etc/apache2/ssl/openstack.key

# crudini –set /etc/nova/nova.conf glance insecure true

# crudini –set /etc/nova/nova.conf keystone\_authtoken auth\_uri https://controller:5000

# crudini –set /etc/nova/nova.conf keystone\_authtoken auth\_url https://controller:5000

# crudini –set /etc/nova/nova.conf keystone\_authtoken certfile /etc/apache2/ssl/openstack.crt

# crudini –set /etc/nova/nova.conf keystone\_authtoken keyfile /etc/apache2/ssl/openstack.key

# crudini –set /etc/nova/nova.conf keystone\_authtoken insecure true

# crudini –set /etc/nova/nova.conf placement auth\_url https://controller:5000/v3

# crudini –set /etc/nova/nova.conf placement certfile /etc/apache2/ssl/openstack.crt

# crudini –set /etc/nova/nova.conf placement keyfile /etc/apache2/ssl/openstack.key

# crudini –set /etc/nova/nova.conf placement insecure true

# crudini –set /etc/nova/nova.conf vnc novncproxy\_base\_url <https://controller:6080/vnc_auto.html>

# crudini –set /etc/nova/nova.conf wsgi ssl\_cert\_file /etc/apache2/ssl/openstack.crt

# crudini –set /etc/nova/nova.conf wsgi ssl\_key\_file /etc/apache2/ssl/openstack.key

* SSL for nova-placement endpoints

Update the /etc/apache2/sites-available/nova-placement.conf file as follows:

# sed -i "s/^\(\s\*SSLCertificateFile\).\*/\1 \/etc\/apache2\/ssl\/openstack.crt/" /etc/apache2/sites-available/nova-placement.conf

# sed -i "s/^\(\s\*SSLCertificateKeyFile\).\*/\1 \/etc\/apache2\/ssl\/openstack.key/" /etc/apache2/sites-available/nova-placement.conf

# service apache2 restart

* Restart the Compute services as follows:

# service nova-api restart

# service nova-consoleauth restart

# service nova-scheduler restart

# service nova-conductor restart

# service nova-novncproxy restart

# service nova-compute restart

* Check the service as follows:

# openstack compute service list –insecure

**Figure 4**: OpenStack Compute service list

**SSL for neutron endpoints**

* Update the /etc/neutron/neutron.conf file as follows:

# crudini –set /etc/neutron/neutron.conf DEFAULT use\_ssl true

# crudini –set /etc/neutron/neutron.conf keystone\_authtoken auth\_uri https://controller:5000

# crudini –set /etc/neutron/neutron.conf keystone\_authtoken auth\_url https://controller:5000

# crudini –set /etc/neutron/neutron.conf keystone\_authtoken certfile /etc/apache2/ssl/openstack.crt

# crudini –set /etc/neutron/neutron.conf keystone\_authtoken keyfile /etc/apache2/ssl/openstack.key

# crudini –set /etc/neutron/neutron.conf keystone\_authtoken insecure true

# crudini –set /etc/neutron/neutron.conf nova auth\_url https://controller:5000

# crudini –set /etc/neutron/neutron.conf nova certfile /etc/apache2/ssl/openstack.crt

# crudini –set /etc/neutron/neutron.conf nova insecure true

# crudini –set /etc/neutron/neutron.conf nova keyfile /etc/apache2/ssl/openstack.key

# crudini –set /etc/neutron/neutron.conf ssl cert\_file /etc/apache2/ssl/openstack.crt

# crudini –set /etc/neutron/neutron.conf ssl key\_file /etc/apache2/ssl/openstack.key

* Update the /etc/nova/nova.conf file as follows:

# crudini –set /etc/nova/nova.conf neutron url https://controller:9696

# crudini –set /etc/nova/nova.conf neutron auth\_url https://controller:5000

# crudini –set /etc/nova/nova.conf neutron certfile /etc/apache2/ssl/openstack.crt

# crudini –set /etc/nova/nova.conf neutron keyfile /etc/apache2/ssl/openstack.key

# crudini –set /etc/nova/nova.conf neutron insecure true

* Restart the Restart the Compute API service and the Networking services as follows:

# service neutron-server restart

# service neutron-linuxbridge-agent restart

# service neutron-dhcp-agent restart

# service neutron-metadata-agent restart

# service neutron-l3-agent restart

# service nova-compute restart

# service neutron-linuxbridge-agent restart

* Check the service as follows:

# openstack network agent list –insecure

**Figure 5:** OpenStack network agent list

**SSL for Heat endpoints**

* Update the /etc/heat/heat.conf file as follows:

# crudini –set /etc/heat/heat.conf DEFAULT heat\_metadata\_server\_url https://controller:8000

#crudini –set /etc/heat/heat.conf DEFAULT heat\_waitcondition\_server\_url https://controller:8000/v1/waitcondition

#crudini –set /etc/heat/heat.conf clients\_keystone auth\_uri https://controller:5000

#crudini –set /etc/heat/heat.conf clients\_keystone cert\_file /etc/apache2/ssl/openstack.crt

#crudini –set /etc/heat/heat.conf clients\_keystone key\_file /etc/apache2/ssl/openstack.key

#crudini –set /etc/heat/heat.conf clients\_keystone insecure true

#crudini –set /etc/heat/heat.conf ec2authtoken auth\_uri https://controller:5000/v3

#crudini –set /etc/heat/heat.conf ec2authtoken cert\_file /etc/apache2/ssl/openstack.crt

#crudini –set /etc/heat/heat.conf ec2authtoken key\_file /etc/apache2/ssl/openstack.key

#crudini –set /etc/heat/heat.conf ec2authtoken insecure true

#crudini –set /etc/heat/heat.conf heat\_api cert\_file /etc/apache2/ssl/openstack.crt

#crudini –set /etc/heat/heat.conf heat\_api key\_file /etc/apache2/ssl/openstack.key

#crudini –set /etc/heat/heat.conf keystone\_authtoken auth\_uri https://controller:5000

#crudini –set /etc/heat/heat.conf keystone\_authtoken auth\_url https://controller:5000

#crudini –set /etc/heat/heat.conf keystone\_authtoken certfile /etc/apache2/ssl/openstack.crt

#crudini –set /etc/heat/heat.conf keystone\_authtoken keyfile /etc/apache2/ssl/client-openstack.key

#crudini –set /etc/heat/heat.conf keystone\_authtoken insecure true

#crudini –set /etc/heat/heat.conf trustee auth\_url <https://controller:5000>

* Check the service as follows:

# openstack orchestration service list –insecure

**Figure 6:** OpenStack orchestration service list

**SSL for horizon**

* Update the /etc/openstack-dashboard/local\_settings.py file as follows:

# sed -i -e 's/#OPENSTACK\_SSL\_NO\_VERIFY = False/OPENSTACK\_SSL\_NO\_VERIFY = True/g' /etc/openstack-dashboard/local\_settings.py

Restart apache2 as follows:

# Service apache2 restart

**Figure 7:** OpenStack Dashboard