Red Hat OpenStack Platform 12

Firewall Rules for Red Hat OpenStack Platform

List of required ports and protocols.

Last Updated: 2019-06-04

Red Hat OpenStack Platform 12 Firewall Rules for Red Hat OpenStack Platform

List of required ports and protocols.

OpenStack Team
rhos-docs@redhat.com

Legal Notice

Abstract

This article describes the firewall rules created by the Red Hat OpenStack Platform director.

Table of Contents

1. FIREWALL RULES FOR RED HAT OPENSTACK PLATFORM

This article describes the firewall configuration created by the director for Red Hat OpenStack Platform. These ports are required for services running on the overcloud.

IMPORTANT

It is recommended that you test service connectivity before moving your deployment into production. As part of this process, consider checking for any dropped traffic on all intermediary firewalls.

NOTE

In the tables below, certain port numbers are formatted as variables, such as **IronicIPXEPort**. These port numbers will be specific to your deployment and will have been defined in your environment files.

1.1. Reviewing firewall rules for Composable Roles

Red Hat OpenStack Platform director allows you to customize where certain OpenStack services are deployed. For example, you could deploy a standalone node that runs only the Identity Service (keystone). For more information, see the Composable Roles documentation:
https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/12/html/advanced_overcloud_customization/roles

2. REVIEW THE FIREWALL RULES FOR EACH ROLE

Consider segmenting the network traffic that passes between standalone roles. For example, some deployments might want to use granular firewall rules to restrict traffic between standalone keystone nodes, or from one keystone node to a standalone Compute node. This approach would also be useful for spine-leaf networks, where the router can also be used to apply granular firewall rules.

To begin segmenting traffic for standalone roles, you will need to identify the firewall rules apply to each role. You can determine this by reviewing the services assigned to the role. Each service file in **tripleo-heat-templates/puppet/services/*** has an entry named **tripleo.<service>.firewall_rules** which describes the ports required for that service. You can extract this information from the templates using the following command:

```
find -L /usr/share/openstack-tripleo-heat-templates/ -type f | while read f;do if `grep -q firewall_rules $f`;then echo -e "\n $f " ; grep firewall_rules "$f" -A10;fi; done
```

NOTE

The following tables are formatted output from the above command, from a particular point in time. It would be good practice to confirm the settings in the YAML scripts, as they are subject to change.

2.1. TripleO Core

Service	Protocol	Ports	Notes
core	UDP	4789	

2.2. Ceph MDS

Service	Protocol	Ports	Notes
ceph	TCP	6800-7300	

2.3. Ceph Monitor service

Service	Protocol	Ports	Notes
ceph	TCP	6789	

2.4. Ceph OSD

Service	Protocol	Ports	Notes
ceph	TCP	6800-7300	

2.5. Ceph RadosGW service

Service	Protocol	Ports	Notes
ceph_rgw	TCP	**CephRgwInternal**	Ceph RGW

2.6. MySQL Galera

Service	Protocol	Ports	Notes
mysql_galera	TCP	873	MySQL
mysql_galera	TCP	3123	
mysql_galera	TCP	3306	
mysql_galera	TCP	4444	
mysql_galera	TCP	4567	

Service	Protocol	Ports	Notes
mysql_galera	TCP	4568	
mysql_galera	TCP	9200	Galera-monitor

2.7. Redis

Service	Protocol	Ports	Notes
redis	TCP	3124	
redis	TCP	6379	Internal service coordination
redis	TCP	26379	

2.8. RabbitMQ

Service	Protocol	Ports	Notes
rabbitmq	TCP	3122	Rabbitmq
rabbitmq	TCP	4369	Rabbitmq
rabbitmq	TCP	5672	Rabbitmq
rabbitmq	TCP	25672	Rabbitmq

2.9. Mistral API

Service	Protocol	Ports	Notes
mistral_api	TCP	8989	
mistral_api	TCP	13989	

2.10. Neutron L3 VRRP

Service	Protocol	Ports	Notes
VRRP	VRRP		VRRP

2.11. Manila API

Service	Protocol	Ports	Notes
manila	TCP	8786	Manila API
manila	TCP	13786	Manila API

2.12. AODH API

Service	Protocol	Ports	Notes
aodh_api	TCP	8042	
aodh_api	TCP	13042	

2.13. Barbican API

Service	Protocol	Ports	Notes
barbican_api	TCP	9311	
barbican_api	TCP	13311	

2.14. Glance API

Service	Protocol	Ports	Notes
glance	TCP	9292	Glance API
glance	TCP	13292	Glance API (SSL)

2.15. OVN DB Server

Service	Protocol	Ports	Notes
ovn_dbs	TCP	**OVNNorthboundServerPort**	
ovn_dbs	TCP	**OVNSouthboundServerPort**	

2.16. Gnocchi API

Service	Protocol	Ports	Notes
gnocchi	TCP	8041	Gnocchi API
gnocchi	TCP	13041	Gnocchi API (SSL)

2.17. Ceph RBD Mirror

Service	Protocol	Ports	Notes
ceph	TCP	6800-7300	

2.18. RabbitMQ QDR

Service	Protocol	Ports	Notes
rabbitmq	TCP	**RabbitClientPort**	

2.19. Ceilometer API

Service	Protocol	Ports	Notes
ceilometer	TCP	8777	Ceilometer API
ceilometer	TCP	13777	Ceilometer API (SSL)

2.20. Horizon

Service	Protocol	Ports	Notes
horizon	TCP	80	Dashboard
horizon	TCP	443	Dashboard (SSL)

2.21. Ironic API

Service	Protocol	Ports	Notes
ironic	TCP	6385	Ironic API
ironic	TCP	13385	Ironic API (SSL)

2.22. Memcached service

Service	Protocol	Ports	Notes
memcached	TCP	11211	

2.23. Ceph MDS

Service	Protocol	Ports	Notes
ceph	TCP	6800-7300	

2.24. Ceph Monitor service

Service	Protocol	Ports	Notes
ceph	TCP	6789	

2.25. Mistral API

Service	Protocol	Ports	Notes
mistral_api	TCP	8989	
mistral_api	TCP	13989	

2.26. Ceph OSD

Service	Protocol	Ports	Notes
ceph	TCP	6800-7300	

2.27. Ceph RadosGW service

Service	Protocol	Ports	Notes
ceph_rgw	TCP	**CephRgwInternal**	Ceph RGW

2.28. Cinder API

Service	Protocol	Ports	Notes
cinder	TCP	8776	Cinder API
cinder	TCP	13776	Cinder API (SSL)

2.29. Ceilometer SNMP

Service	Protocol	Ports	Notes
SNMP	UDP	161	Ceilometer

2.30. Ironic Conductor

Service	Protocol	Ports	Notes
TFTP	UDP	69	
HTTP	TCP	**IronicIPXEPort**	

2.31. Ironic Inspector

Service	Protocol	Ports	Notes
ironic_inspector	TCP	5050	

2.32. keepalived VRRP

Service	Protocol	Ports	Notes
VRRP	VRRP		VRRP

2.33. NTP

Service	Protocol	Ports	Notes
ntp	UDP	123	NTP

2.34. Opencontrail DPDK

Service	Protocol	Ports	Notes
opencontrail	TCP	8097	
opencontrail	TCP	8085	

2.35. Opencontrail TSN

Service	Protocol	Ports	Notes
opencontrail	TCP	8097	

2.36. Opencontrail vRouter

Service	Protocol	Ports	Notes
opencontrail	TCP	8097	
opencontrail	TCP	8085	

2.37. Gnocchi Statsd

Service	Protocol	Ports	Notes
gnocchi_statsd	UDP	8125	Network daemon for statistics

2.38. Keystone

Service	Protocol	Ports	Notes
keystone	TCP	5000	Keystone Public API
keystone	TCP	13000	Keystone Public API (SSL)
keystone	TCP	35357	Keystone Admin API
keystone	TCP	13357	Keystone Admin API (SSL)

2.39. Neutron API

Service	Protocol	Ports	Notes
neutron	TCP	9696	Neutron API
neutron	TCP	13696	Neutron API (SSL)

2.40. Cinder Volume iSCSI Initiator

Service	Protocol	Ports	Notes
iSCSI	TCP	3260	

2.41. MongoDB

Service	Protocol	Ports	Notes
mongodb_config	TCP	27019	mongodb_config
mongodb_sharding	TCP	27018	mongodb_sharding
mongodb	TCP	27017	MongoDB

2.42. MySQL Galera

Service	Protocol	Ports	Notes
mysql_galera	TCP	873	MySQL
mysql_galera	TCP	3306	
mysql_galera	TCP	4444	
mysql_galera	TCP	4567	
mysql_galera	TCP	4568	
mysql_galera	TCP	9200	Galera-monitor

2.43. Redis

Service	Protocol	Ports	Notes

Service	Protocol	Ports	Notes
redis	TCP	6379	Internal service coordination
redis	TCP	26379	

2.44. Nova API

Service	Protocol	Ports	Notes
nova	TCP	8773	Nova EC2 API
nova	TCP	3773	Nova EC2 API (SSL)
nova	TCP	8774	Nova API
nova	TCP	13774	Nova API (SSL)
nova	TCP	8775	Nova Metadata

2.45. EC2 API

Service	Protocol	Ports	Notes
ec2_api	TCP	8788	
ec2_api	TCP	13788	

2.46. etcd

Service	Protocol	Ports	Notes
etcd	TCP	2379	
etcd	TCP	2380	

2.47. HAProxy

Service	Protocol	Ports	Notes
haproxy_stats	TCP	1993	

2.48. Neutron DHCP

Service	Protocol	Ports	Notes
neutron_DHCP	UDP	67	Provisioning the Overcloud
neutron_DHCP	UDP	68	

2.49. Heat CloudFormation API service

Service	Protocol	Ports	Notes
heat	TCP	8000	Heat AWS CloudFormation-compatible API
heat	TCP	13800	Heat AWS CloudFormation-compatible API (SSL)

2.50. Heat AWS CloudWatch-compatible API

Service	Protocol	Ports	Notes
heat	TCP	8003	Heat AWS CloudWatch-compatible API
heat	TCP	13003	Heat AWS CloudWatch-compatible API (SSL)

2.51. L2GW Agent Input

Service	Protocol	Ports	Notes
neutron_l2gw_agent	TCP	**L2gwAgentManagerTableListeningPort**	

2.52. Heat API

Service	Protocol	Ports	Notes
heat	TCP	8004	Heat API Endpoint
heat	TCP	13004	Heat API Endpoint (SSL)

Service	Protocol	Ports	Notes

2.53. Neutron Nuage OVS Agent

Service	Protocol	Ports	Notes
neutron_vxlan	UDP	4789	VXLAN
neutron_vxlan	TCP	**NuageMetadataPort**	VXLAN

2.54. Swift Proxy

Service	Protocol	Ports	Notes
swift	TCP	8080	Swift Proxy
swift	TCP	13808	Swift Proxy (SSL)

2.55. Neutron OVS Agent

Service	Protocol	Ports	Notes
neutron_vxlan	UDP	4789	VXLAN
neutron_vxlan	GRE	GRE	

2.56. Swift Storage

Service	Protocol	Ports	Notes
swift	TCP	873	Rsync
swift	TCP	6000	Object Server
swift	TCP	6001	Container Server
swift	TCP	6002	Account Server

2.57. Nova Libvirt

Service	Protocol	Ports	Notes
nova_libvirt	TCP	16514	
nova_libvirt	TCP	49152-49215	
nova_libvirt	TCP	5900-6923	

2.58. Nova Migration Target

Service	Protocol	Ports	Notes
nova_migration_target	TCP	**MigrationSshPort**	**MigrationSshPort** is **2022** by default.

2.59. Nova Placement

Service	Protocol	Ports	Notes
nova_placement	TCP	8778	
nova_placement	TCP	13778	

2.60. Nova VNC Proxy

Service	Protocol	Ports	Notes
nova_vnc_proxy	TCP	6080	
nova_vnc_proxy	TCP	13080	

2.61. Octavia API

Service	Protocol	Ports	Notes
octavia_api	TCP	9876	
octavia_api	TCP	13876	

2.62. OpenDaylight API

Service	Protocol	Ports	Notes
opendaylight_api	TCP	6640	
opendaylight_api	TCP	6653	
opendaylight_api	TCP	2550	
opendaylight_api	TCP	8185	

2.63. OpenDaylight OVS Agent

Service	Protocol	Ports	Notes
opendaylight_ovs	UDP	4789	VXLAN
opendaylight_ovs	GRE	GRE	

2.64. OVN Controller

Service	Protocol	Ports	Notes
ovn_controller	UDP	4789	neutron vxlan networks
ovn_controller	UDP	6081	neutron geneve networks

2.65. pacemaker

Service	Protocol	Ports	Notes
pacemaker	TCP	2224	
pacemaker	TCP	3121	
pacemaker	TCP	21064	
pacemaker	UDP	5405	

2.66. pacemaker remote

Service	Protocol	Ports	Notes
pacemaker	TCP	3121	

2.67. Panko API

Service	Protocol	Ports	Notes
panko_api	TCP	8977	
panko_api	TCP	13977	

2.68. RabbitMQ

Service	Protocol	Ports	Notes
rabbitmq	TCP	4369	Rabbitmq
rabbitmq	TCP	5672	Rabbitmq
rabbitmq	TCP	25672	Rabbitmq

2.69. Sahara API

Service	Protocol	Ports	Notes
sahara	TCP	8386	Sahara API
sahara	TCP	13386	Sahara API (SSL)