Применение Floating IP port forwarding

В версии РУСТЭК Stein используется механизм Floating IP port forwarding. В более ранних версиях нельзя было разным виртуальным машинам одновременно использовать плавающий IP-адрес. Теперь можно - в режиме использования разных портов.

Цели использования механизма.

Переадресация портов является распространенной функцией в сетях и, в частности, в облачных системах PaaS и SaaS, которые нацелены на повторное использование одного и того же Floating IP-адреса для разных клиентов, которые используют разные виртуальные машины(далее ВМ) для своих нужд.

Это особенно актуально для инсталляций, в которых отсутствует большое количество Floating IP-адресов, которые могут использоваться конечными клиентами.

Распространенным вариантом использования этой функции является клиент, запрашивающий конкретную услугу, где обслуживающая платформа (PaaS, SaaS) выделяет ВМ для запуска службы, а затем выделяет клиентский порт для доступа к этой услуге. Это означает, что различные клиенты будут использовать один и тот же Floating IP-адрес, но разные порты назначения TCP / UDP для различных ВМ в конечных точках.

Пример, использования механизма для 3х серверов с 2х Floating IP:

client1 -> 1.1.1.1:22 TCP => пересылается на 192.168.0.100 порт 22 TCP (VM1)

client2 -> 1.1.1.1:2022 TCP => пересылается на 192.168.0.101 порт 22 TCP (VM2)

client3 -> 1.1.1.2:2022 TCP => пересылается на 192.168.0.102 порт 22 TCP (VM3)

Механизм переадресации возможно использовать только на Floating IP-адресах, которые не назначены ВМ или Роутерам.

Если порт ВМ удален, записи переадресации портов на Floating IP-адресах, соответствующие этому порту, также удаляются. То же самое применимо в случае удаления Floating IP.

При использовании переадресации порта на Floating IP необходимо разрешить в группе безопасности ВМ прохождение пакетов на соответствующий порт назначения, например при трансляции:

client -> 1.1.1.2:2022 TCP => пересылается на 192.168.0.101 порт 22 TCP VM

необходимо открыть 22 порт TCP на ВМ правилами безопасности.

Альтернативным вариантом является использование клиентом ВМ с Floating IP, которая реализует DNAT port forwarding на другие ВМ без использования выделенных Floating IP адресов для данных ВМ.

Управление Floating IP port forwarding через CLI.

Реализуемая в примерах схема:

client -> 10.11.7.4:2222 TCP => пересылается на 192.168.2.79 порт 22 TCP VM

Выделим Floating IP(здесь и далее для Floating-адресов используются серые IP адреса в целях демонстрации), в последствии с которого будем пробрасывать внешние порты на внутренние порты ВМ VM1:

```
(openstack) floating ip create --floating-ip-address 10.11.7.4 --tag port_forwarding_VM1 ext-net
.........skip..........
(openstack) floating ip list --long --any-tags 'port_forwarding_VM1'
+--------------------+--------------------+------------------+------+--------------------+--------------------
+--------+--------+-------------+----------------------+----------+------------+
| ID                 | Floating IP Address | Fixed IP Address | Port | Floating Network   | Project
| Router | Status | Description | Tags                 | DNS Name | DNS Domain |
+--------------------+--------------------+------------------+------+--------------------+--------------------
+--------+--------+-------------+----------------------+----------+------------+
| 4f2d57c4-bb79-42e3 | 10.11.7.4          | None             | None | b3a3eba3-eca0-42bf | 21e81f6de6b8488fac
| None   | DOWN   |             | ['port_forwarding_VM1 | None     | None       |
| -b992-3c96f1653531 |                    |                  |      | -9872-c355ffbefb74 | 9a95c35e16cf82
|        |        |             | ']                   |          |            |
+--------------------+--------------------+------------------+------+--------------------+--------------------
+--------+--------+-------------+----------------------+----------+------------+
```

Выясним, какие порты подключены к VM1 и какие группы безопасности они используют:

```
(openstack) port list --server VM1 --long
+--------------------------------------+------+-------------------+-----------------------------------------
+--------+--------------------------------------+--------------+------+
| ID                                   | Name | MAC Address       | Fixed IP Addresses                      |
Status | Security Groups                      | Device Owner | Tags |
+--------------------------------------+------+-------------------+-----------------------------------------
+--------+--------------------------------------+--------------+------+
| 9b68c54c-2d19-4ad4-a2a1-30574c83647c |      | fa:16:3e:c4:37:f0 | ip_address='192.168.2.79', subnet_id='055 |
ACTIVE | b354e63b-1c67-435e-8aee-81059b5f8fdd | compute:nova |      |
|                                      |      |                   | c922b-0a3b-44c8-b4fb-b6237accb1fd'
|        |                                      |              |      |
+--------------------------------------+------+-------------------+-----------------------------------------
+--------+--------------------------------------+--------------+------+
```

Создадим правило проброса внешнего порта TCP 2222 с Floating IP на внутренний порт TCP 22 ВМ:

```
(openstack) floating ip port forwarding create --internal-ip-address 192.168.2.79 --port 9b68c54c-2d19-4ad4-
a2a1-30574c83647c --protocol tcp --internal-protocol-port 22 --external-protocol-port 2222 10.11.7.4
.........skip..........
(openstack) floating ip port forwarding list 4f2d57c4-bb79-42e3-b992-3c96f1653531
+--------------------------------------+--------------------------------------+--------------------
+---------------+---------------+----------+
| ID                                   | Internal Port ID                     | Internal IP Address | Internal
Port | External Port | Protocol |
+--------------------------------------+--------------------------------------+--------------------
+---------------+---------------+----------+
| 0011665d-774f-4a16-82e2-2ff0c08a597d | 9b68c54c-2d19-4ad4-a2a1-30574c83647c | 192.168.2.79
|            22 |          2222 | tcp      |
+--------------------------------------+--------------------------------------+--------------------
+---------------+---------------+----------+
```

Создадим правило в группе безопасности порта ВМ:

```
(openstack) security group rule create --ingress --protocol tcp --dst-port 22 b354e63b-1c67-435e-8aee-
81059b5f8fdd
+-------------------
+-------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------+
| Field             |
Value
|
+-------------------
+-------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------+
| created_at        | 2020-02-05T12:39:
08Z
|
| description
|
|
| direction         |
ingress
|
| ether_type        |
IPv4
|
| id                | 60118ee5-6876-4e24-92a0-
3d43f69a25d3
|
| location          | Munch({'project': Munch({'domain_id': 'default', 'id':
'21e81f6de6b8488fac9a95c35e16cf82', 'name': 'admin', 'domain_name': None}), 'cloud': 'rustack', 'zone':
None,      |
|                   | 'region_name':
'RegionOne'})
|
| name              |
None
|
| port_range_max    |
22
|
| port_range_min    |
22
|
| project_id        |
21e81f6de6b8488fac9a95c35e16cf82
|
| protocol          |
tcp
|
| remote_group_id   |
None
|
| remote_ip_prefix  | 0.0.0.0
/0
|
| revision_number   |
0
|
| security_group_id | b354e63b-1c67-435e-8aee-
81059b5f8fdd
|
| tags              |
[]
|
| updated_at        | 2020-02-05T12:39:
08Z
|
+-------------------
+-------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------+
```

На этом настройка окончена. Предполагается, что внутри ВМ запущен SSH сервер на стандартном порту 22. Проверим работу механизма Floating IP port forwarding:

```
[andrey@hppro-andrey files]$ ssh -p2222 10.11.7.4
The authenticity of host '[10.11.7.4]:2222 ([10.11.7.4]:2222)' can't be established.
ECDSA key fingerprint is SHA256:w5ZnVVzVqK+ujX7VqwLbi9fTKCmEdhDxnPsYChbeY7g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? ^C
[andrey@hppro-andrey files]$ ssh -p22 10.11.7.4
ssh: connect to host 10.11.7.4 port 22: Connection refused
```

Под капотом Floating IP port forwarding.

При создании правила форвардинга на Floating IP на хостах где запущен neutron-server в сетевом namespace snat-<ID-Роутера>, который связывает внешнюю сеть и виртуальную сети, в iptables создаются цепочки с правилами форвардинга портов для UUID:

```
(openstack) router list --name Router --long
+--------------------------------+--------+--------+-------+---------------------------------+-------------+------
+--------+--------------------------------+--------------------+------+
| ID                             | Name   | Status | State | Project                         | Distributed | HA
| Routes | External gateway info          | Availability zones | Tags |
+--------------------------------+--------+--------+-------+---------------------------------+-------------+------
+--------+--------------------------------+--------------------+------+
| e3266d21-9761-4fcb-8560-ea161 | Router | ACTIVE | UP    | 21e81f6de6b8488fac9a95c35e16c | True        | True
|        | {"enable_snat": true,          | nova               |      |
| 8057f48                       |        |        |       | f82                           |             |
|        | "external_fixed_ips":          |                    |      |
|                               |        |        |       |                               |             |
|        | [{"subnet_id": "85fc9296-eac8 |                    |      |
|                               |        |        |       |                               |             |
|        | -476b-b1f1-b4e2e9f3b788",     |                    |      |
|                               |        |        |       |                               |             |
|        | "ip_address": "10.11.7.3"}],  |                    |      |
|                               |        |        |       |                               |             |
|        | "network_id": "b3a3eba3-eca0- |                    |      |
|                               |        |        |       |                               |             |
|        | 42bf-9872-c355ffbefb74"}      |                    |      |
+--------------------------------+--------+--------+-------+---------------------------------+-------------+------
+--------+--------------------------------+--------------------+------+
# ip net exec snat-e3266d21-9761-4fcb-8560-ea1618057f48 iptables -S -t nat | egrep '0011665d|agent-fip'
-N neutron-l3-agent-fip-pf
-N neutron-l3-agent-pf-0011665d
-A neutron-l3-agent-PREROUTING -j neutron-l3-agent-fip-pf
-A neutron-l3-agent-fip-pf -j neutron-l3-agent-pf-0011665d
-A neutron-l3-agent-pf-0011665d -d 10.11.7.4/32 -p tcp -m tcp --dport 2222 -j DNAT --to-destination
192.168.2.79:22
```