Creating a VPN connection between regions

Thanks to the Openstack Neutron VPN as a Service (VPNaaS) feature, you can bridge two different regions via a site-to-site IPSec VPN connection. This is made possible without setting up and configuring a virtual machine in any one of the regions. On the contrary, you can quickly establish such a connection using the Cleura Cloud Management Panel or the OpenStack CLI. Let us demonstrate the process following both approaches.

Prerequisites

Whether you choose to work from the Cleura Cloud Management Panel or with the OpenStack CLI, you need to have an account in Cleura Cloud. If you prefer to work with the OpenStack CLI, then in addition to the Python openstackclient module, you need to install the Python neutronclient module also. Use either the package manager of your operating system or pip:

Debian/Ubuntu Mac OS X with Homebrew Python Package

apt install
python3-

This Python module is unavailable via

neutronclient

Creating a VPN connection between two regions

The Cleura Cloud Management

our favorite web browser, navigate to the Cleura Cloud page, and

pip install
pythonneutronclient

neutronclient

neutronclient

neutronclient

pythonneutronclient

neutronclient

neutronclient

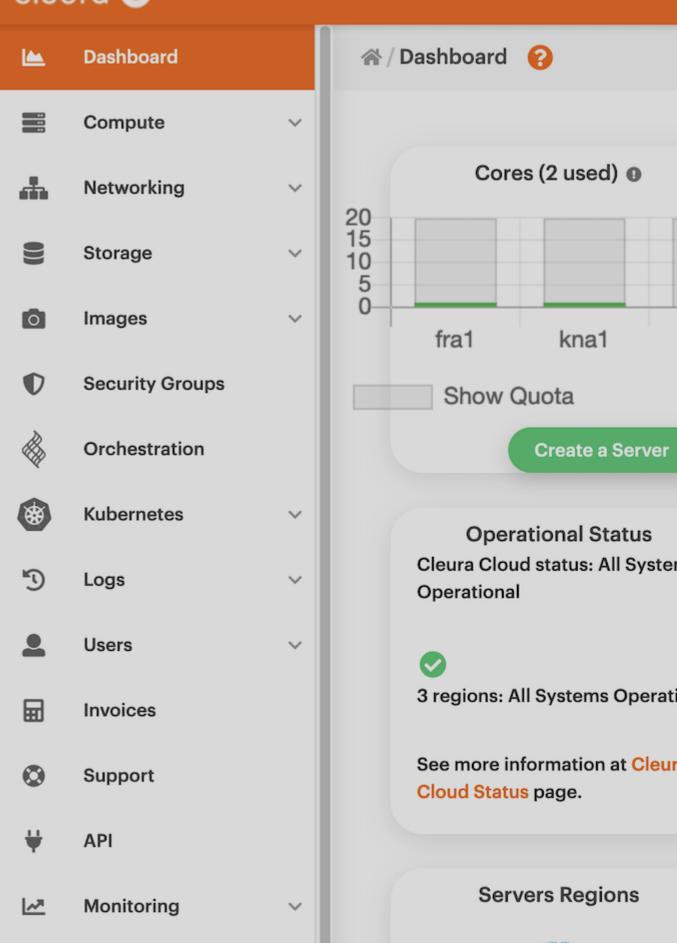
neutronclient

3	aa objeen ee	anoda ana one	k the <i>VPN</i> box.	

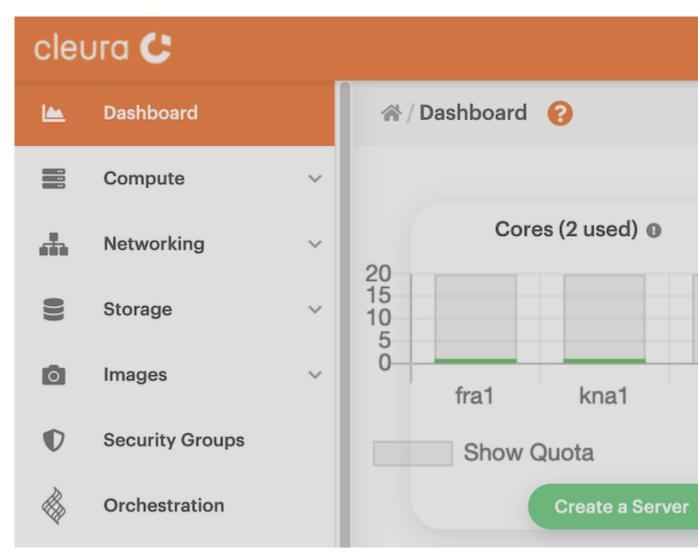
cleura 📞

1

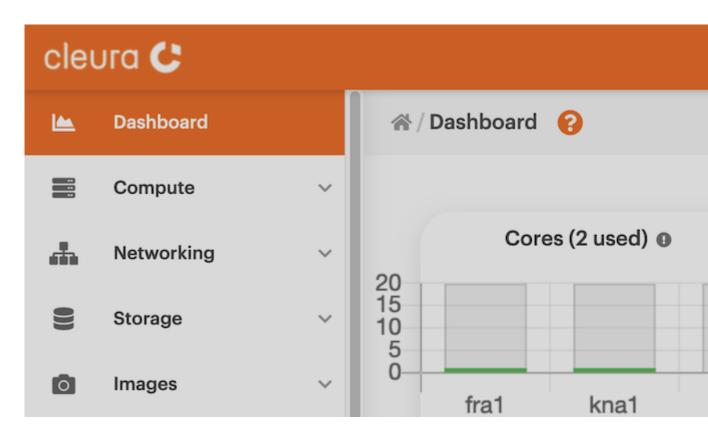
Settings



A new pane titled Create a VPN Service will slide over. Between the two boxes, click the one titled

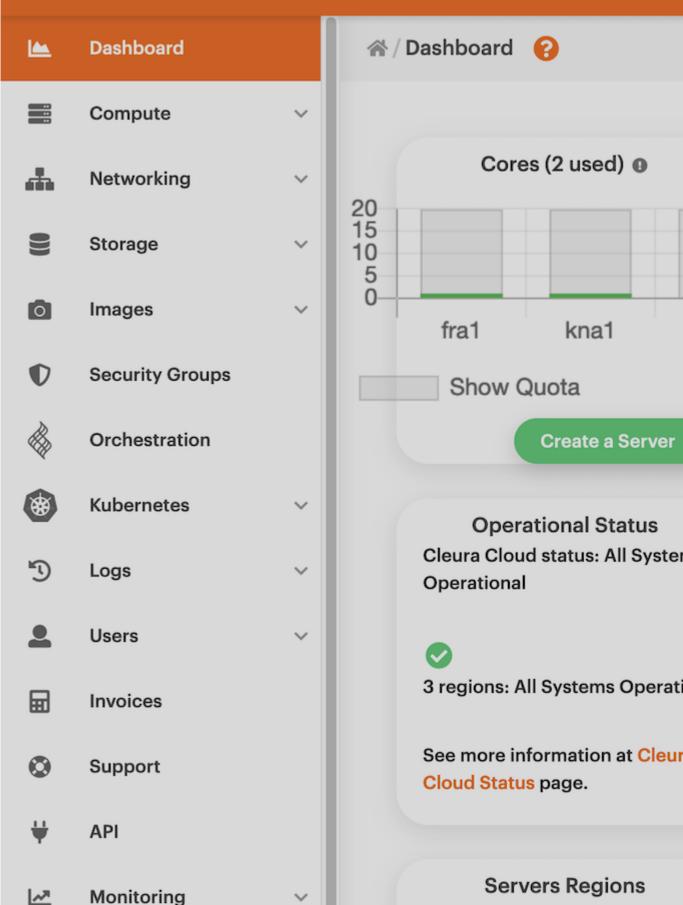


Type in a name for the new site-to-site VPN connection.

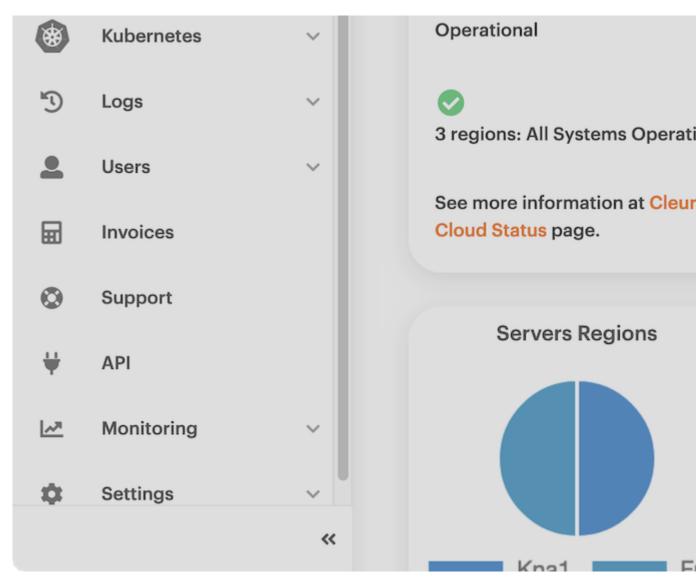


Select a region, project, and network for each of the two data centers involved.

cleura Ċ



Look at the pre-shared key and, optionally, expand the Advanced Options section to see all presets



First, you need to have the RC files of the two regions you will be connecting. In the example that is source the RC file for fral, and before working in knal you need to source the RC file for knal.

It helps to imagine the site-to-site connection schematically, with fral being on the left side and

You also have to decide which subnets from either side you will connect. Additionally, you need to be right side we have subnet subnet-kna1 with CIDR 10.15.20.0/24 and router router-kna1. For convenient

```
SUBNET_FRA1="10.15.25.0/24"
SUBNET_KNA1="10.15.20.0/24"
```

Prepare the left side (region fra1)

Begin by creating a new IKE policy:

openstack vpn ike policy create ike-pol-fra1

Then, create a new IPSec policy:

```
openstack vpn ipsec policy create ipsec-pol-fra1
```

You are ready to create a new VPN service:

openstack vpn service create --router router-fra1 vpn-service-fra1

```
+-----+
| Field | Value |
+-----+
| Description | |
| Flavor | None |
| ID | d74d51f0-182d-4d88-952a-1d593ce696fd |
| Name | vpn-service-fra1 |
| Project | dfc700467396428bacba4376e72cc3e9 |
| Router | 62f885d8-6b13-4161-89d1-003c4fafec55 |
| State | True |
```

Notice in the command output that the Status is PENDING_CREATE. This is expected. Also, jot down

```
EXT_IP_FRA1="198.51.100.50"
```

The site-to-site connection you are about to create needs two end-point groups on the left, and two (remote) subnet. You are now on the left side of the connection (region fral), so begin with the left

...and then move on to creating the left peer end-point group:

| Type | cidr |

| project id | dfc700467396428bacba4376e72cc3e9 |

```
openstack vpn endpoint group create \
--type cidr --value $SUBNET_KNA1 peer-epg-fra1

+-----+
| Field | Value | |
+-----+
| Description | | |
| Endpoints | ['10.15.20.0/24'] | |
| ID | a96bb9ef-d0ec-4174-93ae-a8e655910f94 | |
| Name | peer-epg-fra1 | |
| Project | dfc700467396428bacba4376e72cc3e9 |
```

Prepare the right side (region kna1)

Before establishing a site-to-site VPN connection between the two regions, you must make similar these are all the adjusted commands with the respective outputs:

Create a new IKE policy:

```
openstack vpn ike policy create ike-pol-kna1
```

Create a new IPSec policy:

openstack vpn ipsec policy create ipsec-pol-kna1

Create a new VPN service:

openstack vpn service create --router router-kna1 vpn-service-kna1

For convenience, set the value of parameter <code>external_v4_ip</code> to a shell variable:

```
EXT_IP_KNA1="203.0.113.101"
```

Create a local end-point group:

```
openstack vpn endpoint group create \
--type subnet --value subnet-kna1 local-epg-kna1

+-----+
| Field | Value | |
+-----+
| Description | |
| Endpoints | ['421d8fd2-dd7f-4f7c-9a51-42ef4a866dd9'] |
```

Create a peer (remote) end-point group:

```
openstack vpn endpoint group create \
--type cidr --value $SUBNET_FRA1 peer-epg-kna1
```

```
+-----+
| Field | Value |
+-----+
| Description | |
| Endpoints | ['10.15.25.0/24'] |
| ID | 2e627315-02f0-4d68-8683-14230b166060 |
| Name | peer-epg-kna1 |
| Project | 94109c764a754e24ac0f6b01aef82359 |
```

Instantiate a pre-shared key

Before establishing a site-to-site IPSec VPN connection, you must have a randomly generated pre-s

```
PRE_SHARED_KEY=$(openssl rand -hex 24)
```

The above is just an example. The key should not necessarily be a hexadecimal string, nor do you h

```
PRE_SHARED_KEY=$(pwgen 64 1)
```

Establish a left-to-right connection (region fra1)

To create a VPN connection from left to right, i.e., from region fra1 to region kna1, issue the follow

```
openstack vpn ipsec site connection create \
--vpnservice vpn-service-fra1 \
--ikepolicy ike-pol-fra1 \
--ipsecpolicy ipsec-pol-fra1 \
--local-endpoint-group local-epg-fra1 \
--peer-address $EXT_IP_KNA1 \
--peer-id $EXT_IP_KNA1 \
--peer-endpoint-group peer-epg-fra1 \
--psk $PRE_SHARED_KEY \
vpn-conn-to-kna1
```

```
Field
              | Value
+-----+-----
| Authentication Algorithm | psk
Description
                | 15ec761f-1642-49b6-b5a2-e43624c5752d
               | bi-directional
Initiator
|\ Local\ Endpoint\ Group\ ID\ |\ 51895e0e\text{-}fa3a\text{-}43d3\text{-}8037\text{-}5eea073fb77f}
| Local ID
| MTU
                | 1500
Name
                | vpn-conn-to-kna1
| Peer Address
                 | 203.0.113.101
| Peer CIDRs
| Peer Endpoint Group ID | a96bb9ef-d0ec-4174-93ae-a8e655910f94
| Peer ID
          | 203.0.113.101
              | de12db260ee1b9c0b9e624d910c9a9dbddec13dc24d60332 |
| Pre-shared Key
| Project | dfc700467396428bacba4376e72cc3e9
| Route Mode
               static
State
               True
```

Establish a right-to-left connection (region kna1)

Similarly, to create a VPN connection from right to left, i.e., from region kna1 to region fra1, issue

```
openstack vpn ipsec site connection create \
--vpnservice vpn-service-kna1 \
--ikepolicy ike-pol-kna1 \
--ipsecpolicy ipsec-pol-kna1 \
--local-endpoint-group local-epg-kna1 \
--peer-address $EXT_IP_FRA1 \
--peer-id $EXT IP FRA1 \
--peer-endpoint-group peer-epg-kna1 \
--psk $PRE_SHARED_KEY \
vpn-conn-to-fra1
| Authentication Algorithm | psk
Description
                | ID
                | 7705afc7-d0ff-444a-9474-3614e21d2399
                  | 6af4f52c-6522-483d-bb70-b144657489f3
| IKE Policy
| IPSec Policy
                   | 8f9c2219-a931-46eb-b3f5-22d76cbc89d0
                 | bi-directional
Initiator
| Local Endpoint Group ID | c1937c3d-77e7-4f2c-842d-70b5e10df9a8
Local ID
| MTU
                  | 1500
Name
                  | vpn-conn-to-fra1
| Peer Address
                    | 198.51.100.50
| Peer CIDRs
Peer Endpoint Group ID | 2e627315-02f0-4d68-8683-14230b166060
            | 198.51.100.50
                     | de12db260ee1b9c0b9e624d910c9a9dbddec13dc24d60332 |
Pre-shared Key
                 | 94109c764a754e24ac0f6b01aef82359
| Project
| Route Mode
                   static
| State
                 | True
                 | PENDING_CREATE
Status
                    | bb1a307d-6f8f-4a0a-83db-7c705403485d
| VPN Service
                | {'action': 'hold', 'interval': 30, 'timeout': 120} |
| dpd
| project id
                  | 94109c764a754e24ac0f6b01aef82359
```

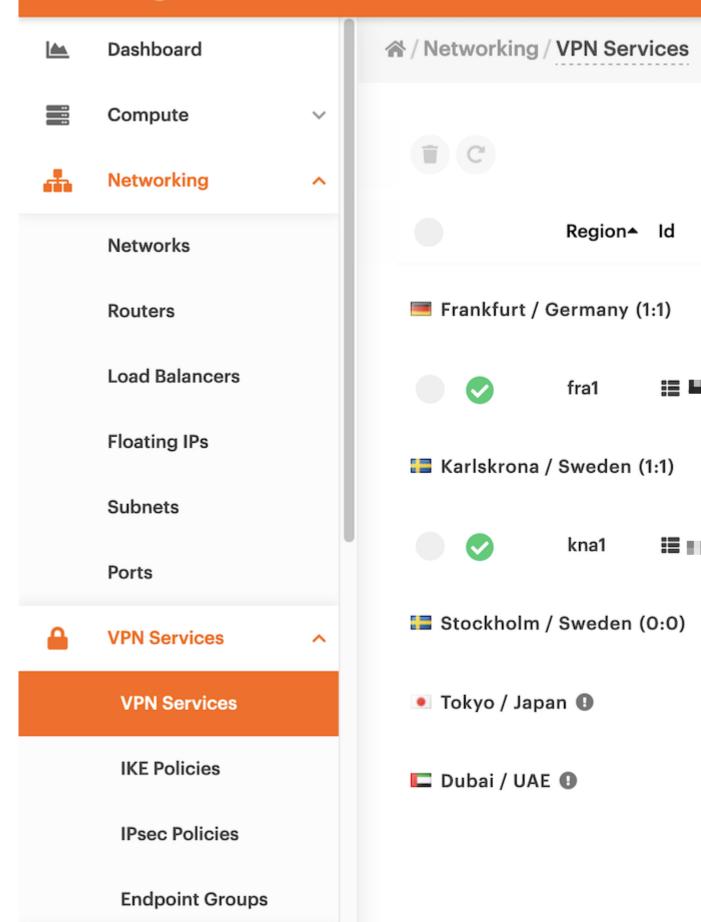
Viewing VPN connections and getting details

No matter if you use the Cleura Cloud Management Panel or the OpenStack CLI, you may at any time list all VPN connections and get relevant details.

Claura Cloud Management Panel OnenStack CII

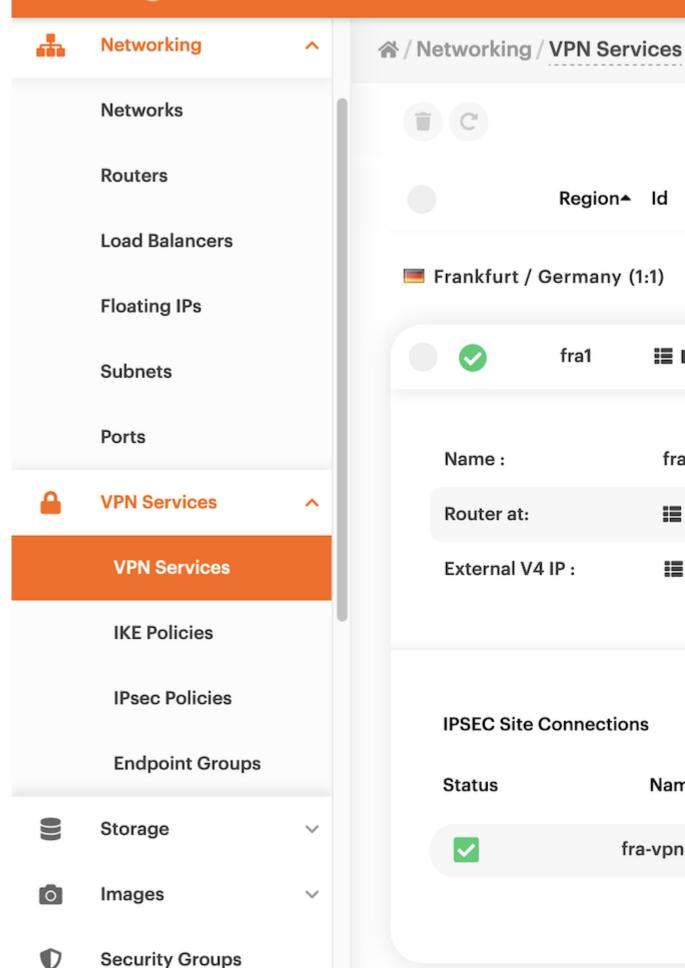
In the vertical pane on the left-hand side of the Cleura Cloud Management Panel, expand the *Netw* region to the other.

cleura Ċ





cleura Ċ



fra-

= 1

III :

Name

fra-vpn-l

You can list all IPSec VPN connections working from any of the two regions involved. See, for exan

If you want more information regarding a specific connection, type something like this:

```
openstack vpn ipsec site connection show vpn-conn-to-kna1
```

Testing the site-to-site VPN connection

One way to test the VPN connection is to have two servers (e.g., server-fra1 and server-kna1), each on a different region (e.g., fra1 and kna1 respectively), ping

each other using private IP addresses. With no VPN connection between the two regions, pinging should not be possible:

```
ubuntu@server-fra1:~$ ping -c 3 10.15.20.148
PING 10.15.20.148 (10.15.20.148) 56(84) bytes of data.

--- 10.15.20.148 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2050ms

ubuntu@server-kna1:~$ ping -c 3 10.15.25.58
PING 10.15.25.58 (10.15.25.58) 56(84) bytes of data.

--- 10.15.25.58 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2045ms
```

On the other hand, with a VPN connection established between the two regions, pinging should be all possible:

```
ubuntu@server-fra1:~$ ping -c 3 10.15.20.148

PING 10.15.20.148 (10.15.20.148) 56(84) bytes of data.
64 bytes from 10.15.20.148: icmp_seq=1 ttl=62 time=32.8 ms
64 bytes from 10.15.20.148: icmp_seq=2 ttl=62 time=32.5 ms
64 bytes from 10.15.20.148: icmp_seq=3 ttl=62 time=32.6 ms

--- 10.15.20.148 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 32.544/32.624/32.761/0.096 ms
```

```
ubuntu@server-kna1:~$ ping -c 3 10.15.25.58
PING 10.15.25.58 (10.15.25.58) 56(84) bytes of data.
64 bytes from 10.15.25.58: icmp_seq=1 ttl=62 time=33.3 ms
64 bytes from 10.15.25.58: icmp_seq=2 ttl=62 time=32.5 ms
64 bytes from 10.15.25.58: icmp_seq=3 ttl=62 time=32.6 ms
--- 10.15.25.58 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 32.533/32.832/33.336/0.358 ms
```

Disabling an active connection

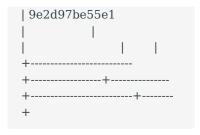
You may, at any time, disable an active site-to-site VPN connection.

OpenStack CLI

Cleura Cloud Management Panel
Currently, there is no way
to disable an active
connection from the
Cleura Cloud Management
Panel. If you want to
disable an active
connection, please use the
OpenStack CLI.

All you have to do is get on either side of the connection and disable the VPN connection across the other side. Suppose you are on the left side of the connection (region fra1), and for whatever reason, you want to disable the site-to-site connection between left and right (regions fra1 and kna1). First, you might want to remember the name of the VPN connection to the right:

openstack vpn ipsec site connection list



That would be vpn-conn-tokna1, and according to the command output above, it is active. To disable it, type the following:

openstack vpn ipsec site connection set --disable vpn-conn-to-kna1

Check if it is really disabled:

openstack vpn ipsec site connection show vpn-connto-kna1 -c Status

```
+-----+
| Field | Value |
+-----+
| Status | DOWN |
+-----+
```

It looks like it is disabled — or DOWN.

You will probably have to wait several seconds before seeing a status change. If you are impatient, try something like this:

watch "openstack vpn ipsec site connection show vpn-conn-to-kna1 c Status" Hit CTRL+C as soon as you see the status change you expect.

Now, get on the right side of the connection (region kna1), optionally look for the name of the VPN connection to the left (in our example, that would be vpn-conn-to-fra1), and check its status:

openstack vpn ipsec site
connection show vpn-connto-fra1 -c Status

abled site-to-site connection is now disabled, select a
server from one region and try to ping a server in another region. Suppose, for

```
+-----+
| Field | Value |
|------+
| Status | DOWN |
| +------+
| ubuntu@server-fra1:~$ ping -c 3 10.15.20.148
```

```
ubuntu@server-fra1:~$ ping -c 3 10.15.20.148
PING 10.15.20.148 (10.15.20.148) 56(84) bytes of data.
--- 10.15.20.148 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2055ms
```

```
ubuntu@server-kna1:~$ ping -c 3 10.15.25.58
PING 10.15.25.58 (10.15.25.58) 56(84) bytes of data.
--- 10.15.25.58 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2050ms
```

Enabling an inactive connection

You can easily enable an inactive site-to-site VPN connection.

Cleura Cloud Management Panel

OpenStack CLI

Currently, there is no way to enable an inactive connection from the Cleura Cloud Management Panel. If you want to re-enable an inactive connection, please use the OpenStack CLI.

Make sure you hop on the side where you initially disabled the connection. According to the example scenario we described in the previous section, that would be the left side (region fra1), and the name of the disabled connection would be vpn-conn-to-kna1. Make sure the connection status is DOWN:

openstack vpn ipsec site connection show vpn-conn-to-kna1 -c Status

+-----+ | Field | Value | +-----+ | Status | DOWN | +-----+

Note that if you issued a similar command from the

right side of the connection (region kna1), you would also get a DOWN status. Being on the left side, all you have to do to enable the inactive connection is type the following:

openstack vpn ipsec site connection set -enable vpn-conn-tokna1

Check the connection status — it should be ACTIVE:

openstack vpn ipsec site connection show vpn-conn-to-kna1 -c Status

+-----+ | Field | Value | +-----+ | Status | ACTIVE | +-----+

You get the same status by issuing a similar command from the right side.

Again, since you may have to wait several seconds before seeing the status change you expect, try something like this:

watch "openstack vpn ipsec site connection show vpn-conn-to-kna1 -c Status"

server from one region and try to ping a server in another region. Suppose, for example, that a re-enabled connection involves regions fra1 and kna1, and that we have servers server-fra1 (in fra1) and server-kna1 (in kna1). With the VPN connection between the two regions now re-established, pinging should be possible:

```
ubuntu@server-fra1:~$ ping -c 3 10.15.20.148

PING 10.15.20.148 (10.15.20.148) 56(84) bytes of data.
64 bytes from 10.15.20.148: icmp_seq=1 ttl=62 time=32.6 ms
64 bytes from 10.15.20.148: icmp_seq=2 ttl=62 time=32.6 ms
64 bytes from 10.15.20.148: icmp_seq=3 ttl=62 time=32.7 ms

--- 10.15.20.148 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 32.619/32.634/32.662/0.019 ms
```

```
ubuntu@server-kna1:~$ ping -c 3 10.15.25.58
PING 10.15.25.58 (10.15.25.58) 56(84) bytes of data.
64 bytes from 10.15.25.58: icmp_seq=1 ttl=62 time=32.8 ms
64 bytes from 10.15.25.58: icmp_seq=2 ttl=62 time=32.6 ms
64 bytes from 10.15.25.58: icmp_seq=3 ttl=62 time=33.4 ms
--- 10.15.25.58 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 32.560/32.899/33.357/0.336 ms
```

Last update: 2022-11-27 Created: 2022-11-27 Authors: Christos Varelas