Rapid Access Cloud Virtual Private Network

Creating a virtual private network (VPN) between your desktop or laptop and a VPN service within the Rapid Access Cloud, allows you access to the **private IP address** of instances associated with your project (e.g. 10.0.0.73; 10.1.1.9; etc.). This is best if you need access to the resources you have created in the Rapid Access Cloud for computational experiments for example, but do not need to offer public services to the internet over IPv4, like web applications or email.

The VPN will need to be manually started each time you wish to access the private network and only computers that have connected to the VPN in this manner can access the private network, however multiple computers can access the network at the same time if they each have the VPN configured.

macOS

1. Install Tunnelblick, a free OpenVPN application for macOS.
2. Download the Rapid Access Cloud VPN configuration files. VPN access is configured per region:
    a. Calgary (https://vpn-yyc.cloud.cybera.ca/vpn-yyc-tblk.zip)
    b. Edmonton (https://vpn-yeg.cloud.cybera.ca/vpn-yeg-tblk.zip)
3. Unzip the file locally and double-click the unzipped file vpn-yyc.tblk. This will automatically run Tunnelblick and add the VPN configuration.
4. In the top right corner of your screen, you will see the Tunnelblick icon. Click on it and choose "Connect vpn-yyc".
5. When prompted, enter your RAC username and password.
6. See the section Verifying Connectivity to confirm the VPN connection is working.

If you see the following message, you can safely ignore it:

```
This computer's apparent public IP address was not different after connecting to vpn. This may mean that your VPN is not configured correctly.
```

The reason for this message is because the Rapid Access Cloud VPN is not routing *all* of your traffic through the VPN. Only traffic destined for the Rapid Access Cloud's IP space.

Windows

1. Download and Install the community version of OpenVPN from openvpn.net.
2. Download the Rapid Access Cloud VPN configuration files. VPN access is configured per region:
    a. Calgary (https://vpn-yyc.cloud.cybera.ca/vpn-yyc-win.zip)
    b. Edmonton (https://vpn-yeg.cloud.cybera.ca/vpn-yeg-win.zip)
3. Unzip then copy **all** of the files (ca.crt, client.crt, client.key, and client.ovpn) to `C:\Program Files\OpenVPN\config` .
4. On the Windows Desktop, right-click on the OpenVPN GUI shortcut, select Properties and then the Compatibility tab. Check the box to "Run this program as an administrator".
5. Double-click on the OpenVPN GUI shortcut and an OpenVPN icon should now appear on your taskbar.
6. Right-click on the OpenVPN taskbar icon and choose "connect".
7. When prompted, enter your Rapid Access Cloud username and password.
8. See the section Verifying Connectivity to confirm the VPN connection is working.

Ubuntu Linux

1. Install and configure the openvpn package for your distribution. For example, on Ubuntu 16.04, run the following commands:

```
sudo apt-get update
sudo apt-get install openvpn unzip
```

2. Download the Rapid Access Cloud VPN configuration files. VPN access is configured per region:
    a. Calgary
    b. Edmonton
3. Unzip the file and move the contents to /etc/openvpn/. For example:

```
wget https://vpn-yyc.cloud.cybera.ca/vpn-yyc-ovpn.zip
unzip vpn-yyc-ovpn.zip
sudo mv ca.crt client.conf client.crt client.key /etc/openvpn/
```

4. Start the OpenVPN client service:

```
sudo systemctl start openvpn@client
Enter Auth Username:
Enter Auth Password:
```

   Enter your Rapid Access Cloud username/email address and password to authenticate.

5. See the section Verifying Connectivity to confirm the VPN connection is working.
6. To disconnect from the VPN:

```
sudo systemctl stop openvpn@client
```

Verifying Connectivity

To verify you have successfully connected to the VPN, please do the following

Ping the VPN Gateway

Pinging the VPN Gateway will confirm you have successfully connected and can communicate with the VPN server. Open a command-prompt and run the following:

```
ping 10.254.0.1
```

Ping Your Instance

Each of your instances has a private IPv4 address:

- For the Calgary region, these IP address look like `10.1.x.y`.
- For Edmonton, these IP addresses look like `10.2.x.y`.

Open a command-prompt and run the following:

```
ping 10.1.x.y
```

where `x.y` is the rest of your instance's IP address. For example:

```
ping 10.1.11.44
```

⚠ For the ping to work, make sure your instance's Security Group allows ICMP traffic

Security Groups and the VPN Service

You may need to alter your security groups to allow traffic from the VPN server to reach your instance. You will see Calgary VPN traffic reaching your instance locally from 10.1.8.18, while Edmonton VPN traffic will reach your instance from 10.2.1.9

Example rules:

Allow all ICMP/ping traffic from the local private network

Calgary: Allow ALL ICMP from 10.1.0.0/20
Edmonton: Allow ALL ICMP from 10.2.0.0/20

Allow port 22 (SSH) from only the VPN exit point:

Calgary: Allow TCP Port 22 from 10.1.8.18/32
Edmonton: Allow TCP Port 22 from 10.2.1.9/32