IBM Power Virtual Server Virtual Private Network Connectivity

An IBM Systems Lab Services Tutorial

Faad Ghoraishi

Vess Natchev

ibmsls@us.ibm.com

Table of Contents

Chapter 1: Solution Overview

Introduction

A key client requirement for IBM Power Virtual Server (PowerVS) is the ability to connect to cloud-based workloads from an on-premise environment. Specifically, clients need the capability for multiple users and multiple on-premise systems to connect securely to workloads in PowerVS. Configuring individual user connectivity with a Virtual Private Network (VPN) **client** is fairly easy and documented here: https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-configuring-power. Meanwhile, we would not recommend creating PowerVS workloads with a public IP address for security reasons.

Therefore, the focus of this tutorial will be how to configure a **site-to-site VPN connection** from an on-premise environment to PowerVS. The approach detailed in this document can also be customized for cloud-to-cloud VPN connectivity, as well, with a VPN gateway on each side.

Note that this tutorial uses two separate IBM Cloud locations to simulate the site-to-site VPN connection between an on-premise client environment and IBM Cloud. Therefore, the same configuration method is used for both VPN gateways. With a client environment, the on-premise (or other cloud) VPN gateway should be configured according to its specifications, while this tutorial would be used for the VPN gateway in the IBM Cloud.

Use Cases

Site-to-site VPN Connectivity

We will demonstrate how to configure a site-to-site VPN connection to PowerVS.

Solution Components and Requirements

Components

The following components need to be setup to allow for VPN site-to-site connection. Site-to-site VPN will allow customers to connect their remote datacenter to IBM cloud Power Locations using private IP. If customers wish to use public IP access, then all they

would require is internet access from their datacenter and a Direct Link inside IBM Cloud to the their PowerVS location.

In this scenario we are simulating a remote datacenter to be one of the two PowerVS locations in IBM Cloud. In this case, LON06 is simulating a remote datacenter and TOR01 is the cloud PowerVS location.
Customers who have their own routers in their datacenters, will not need to order two Vyatta routers show in step 2. Instead only need one Vyatta router in the IBM Cloud located in same geo as their PowerVS location geo location in the IBM Cloud.

All steps given shown here for site-to-site GRE and IPsec tunnel provisioning are for Vyatta OS, i.e., vyos.

1. *Order Direct Link Connect Classic to connect each PowerVS location to IBM Cloud*
2. *Order two Vyatta Gateways one in each PowerVS location: allow for PowerVS location-to-PowerVS location communication*
3. *Request a Generic Routing Encapsulation (GRE) tunnel to be provisioned at each PowerVS location to the Vyatta Gateway in that location.*
4. *Configure GRE tunnels in each Vyatta Gateway to connect Vyatta Gateway to each PowerVS location*
5. *Configure an site-to-site IPsec tunnel between the two vyatta gateways.*

Requirements

Order Direct Link Connect Classic

You will need to order Direct Link (DL) Connect Classic to allow your Power VSIs provisioned inside IBM Cloud to communication with Linux/Window VSIs in IBM Cloud and also with all other IBM Cloud services such as VMWare VMs, and Cloud Object Storage (COS). Ordering a DL may take 1-2 weeks to complete. There is no charge for this service as of June 2020.

Order Vyatta Gateways in each datacenter

In order to setup communication between the two PowerVS locations for a site-to-site VPN, you will need to use an IPsec tunnels between the two Vyatta over Public Internet, and a GRE tunnels from PowerVS location to each Vyattas over DL.
You will need to order Vyatta Gateways in each PowerVS location.
We ordered one Vyatta in LON06 and the other in TOR01 PowerVS locations.

Request a Generic Routing Encapsulation (GRE) tunnel

You will need to open a support ticket with Power Systems and request that a GRE tunnel be provisioned in each PowerVS location. They will provision their end of the GRE tunnel and send you the information so you can continue and provision your end on the Vyatta Gateways. You will need to provide the Power location subnets information in each PowerVS location in the ticket.

Configure two GRE tunnels in Vyatta Gateways

We used the following link to configure the GRE.

https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-configuring-power

After the support team finished configuring the GRE tunnel, you will need to configure your end of the GRE tunnel on the two Vyatta Gateways.
You will need two GRE tunnels

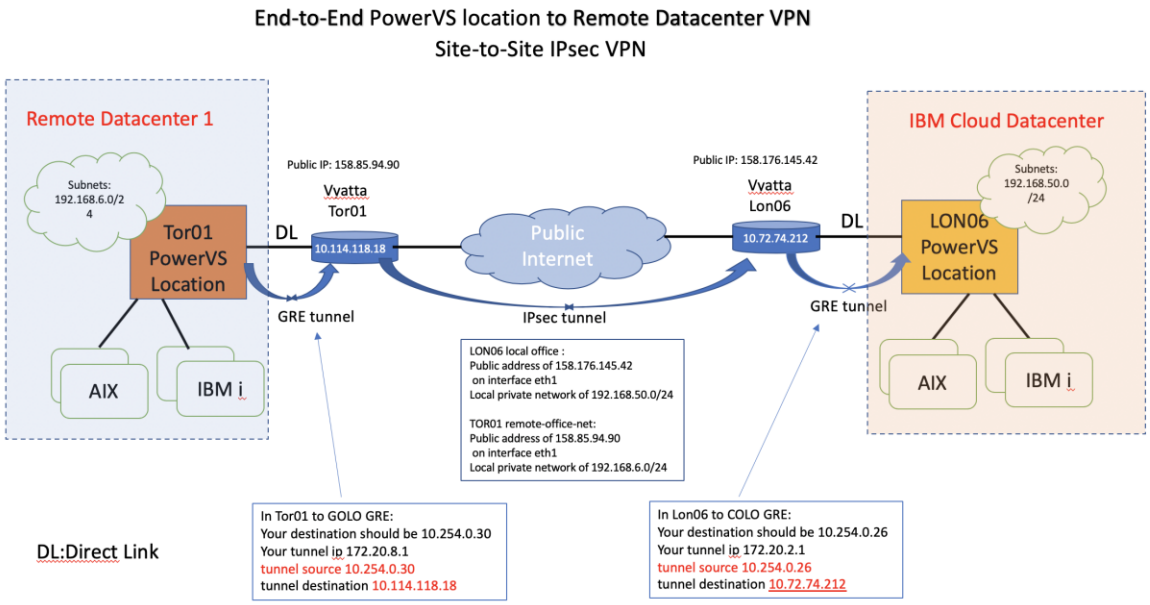
1. GRE tunnel on Vyatta to terminate the PowerVS location GRE in LON06
2. GRE tunnel on Vyatta to terminate the PowerVS location GRE in TOR01

Configure an IPsec tunnels between Vyatta Gateways

We will configure an IPsec tunnel between the two Vyattas over public interface. This will allow communication between the two Vyattas for the Power Locations.

Diagrams

The overall architecture of our deployment is shown in the diagrams below.



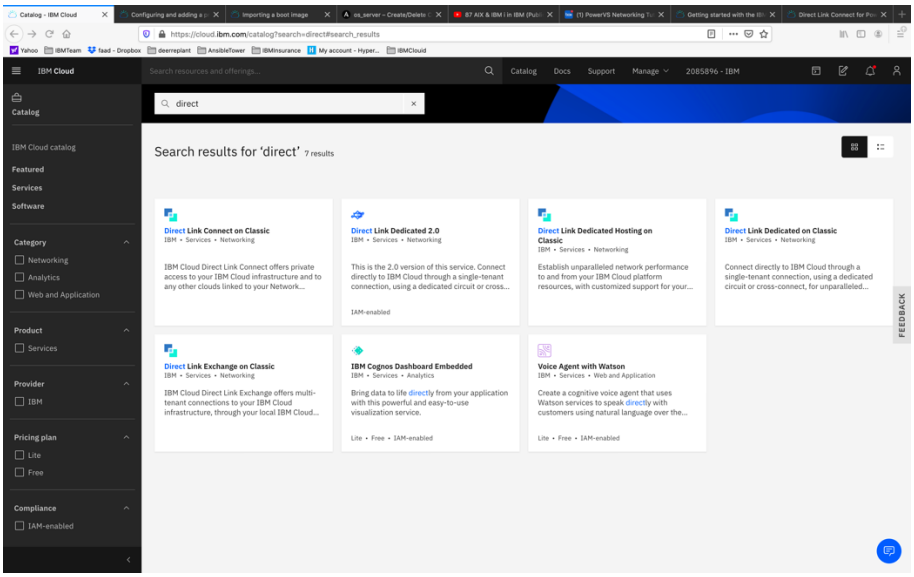
Order Direct Link Connect Classic

You will need to order Direct Link (DL) Connect Classic to allow your Power VSIs in the PowerVS location to communication with Linux/Window VSIs in IBM Cloud and also with all other IBM Cloud services such as Cloud Object Storage and VMware services. This process may take 1-2 weeks to complete.
There are several steps involved in completing DL ordering:

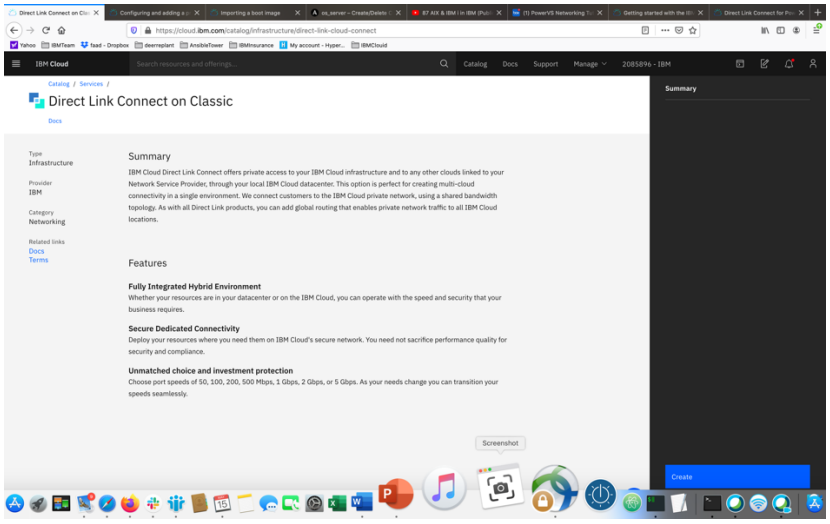
- *Order Direct link connect classic service on IBM Cloud UI – see steps below*
- *Next a support ticket will be created, and Support will send you a word document with questionnaires to be completed concerning various DL settings.*
- *Complete the questionnaires and upload it to support in the ticket.*
- *Support will then request that you create a new support ticket with the Power System so they can complete their side of the DL provisioning. Attach information about the DL in the original ticket to this ticket.*
- *The DL will be provisioned, and you will be notified when complete.*

- *You can now test connection to any Linux/Windows VSI you may have in IBM Cloud and other IBM Cloud services.*

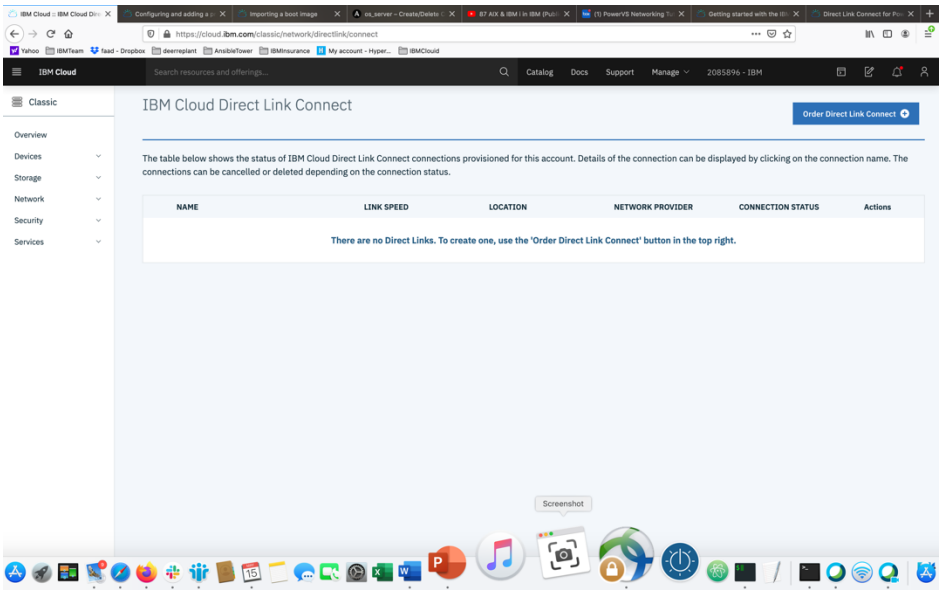
To start the DL order process, go to IBM Cloud UI and log in.
Choose “Catalog” from upper right-hand side, and search for “direct”.



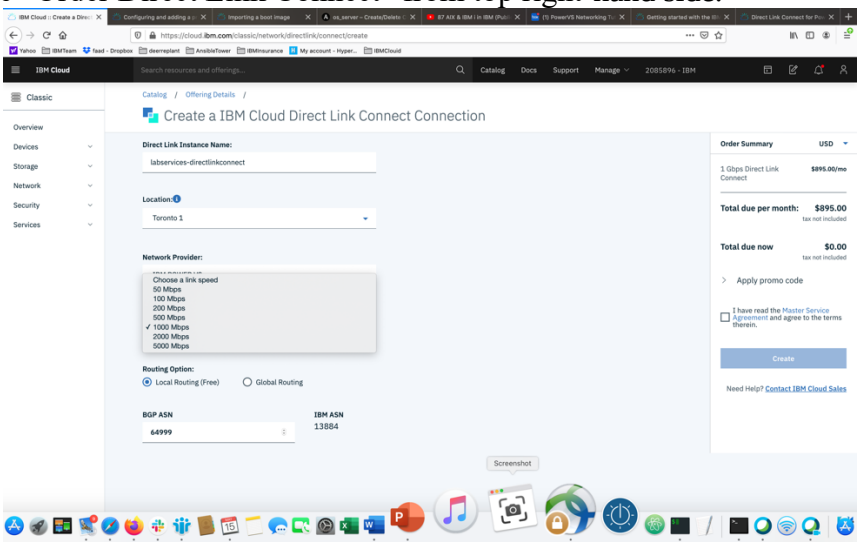
Select “Direct Link Connect on Classic”.



Press “Create”. There are no options to select.



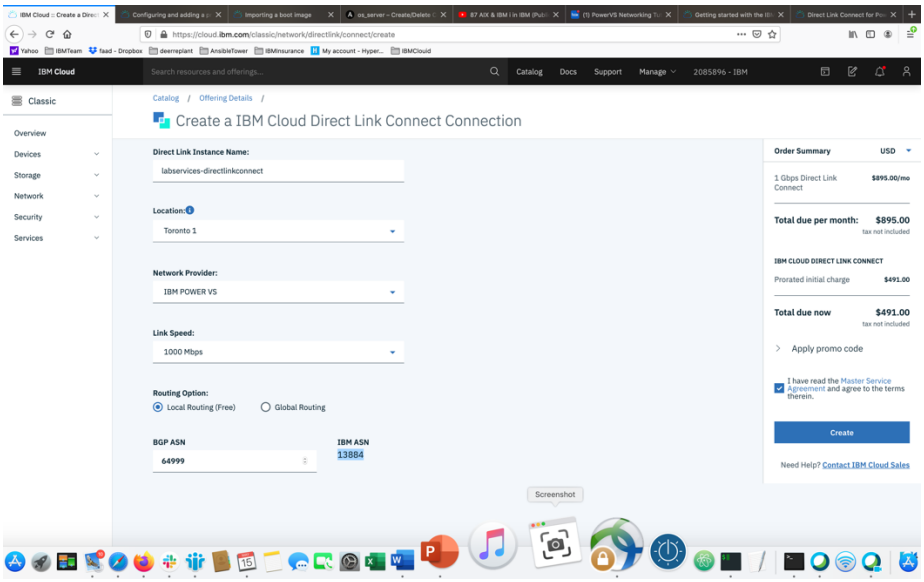
Now choose “Order Direct Link Connect” from top right-hand side.



- *Choose a “name” for the DL.*
- *Choose a location for the DL. This should be the same location as where you created your PowerVS location Service.*
- *Choose “link speed” under network provider menu.*
- *Choose “Local Routing (free)”*

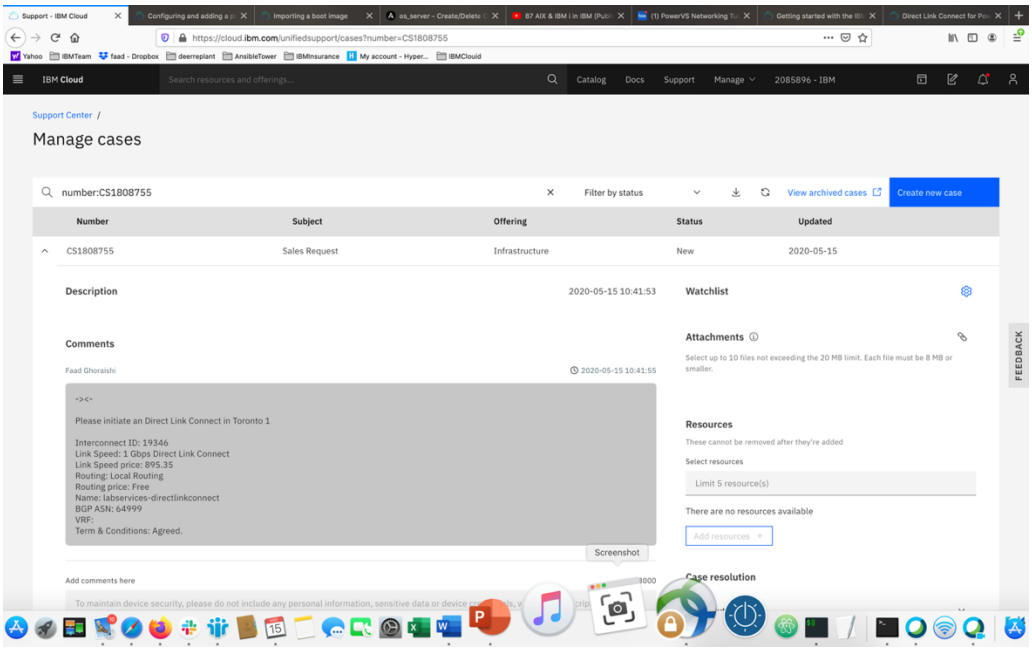
Global routing will require additional charges and will allow for easier PowerVS location-to-PowerVS location communication. You will also need to order a Vyatta Gateway Router to complete your Global routing option via use of a GRE tunnel. Support can help you with this further.

In our case, we decided to use Local Routing and then order a Vyatta Gateway in each PowerVS location and provision a GRE tunnel end-to-end.



- *Check the box to accept the offer and press "Create"*

A support case will be opened with the information required.



After this is complete, you will then be contacted by support and requested to complete and answer some questions in an attached document and send it back as attachment to the same ticket.

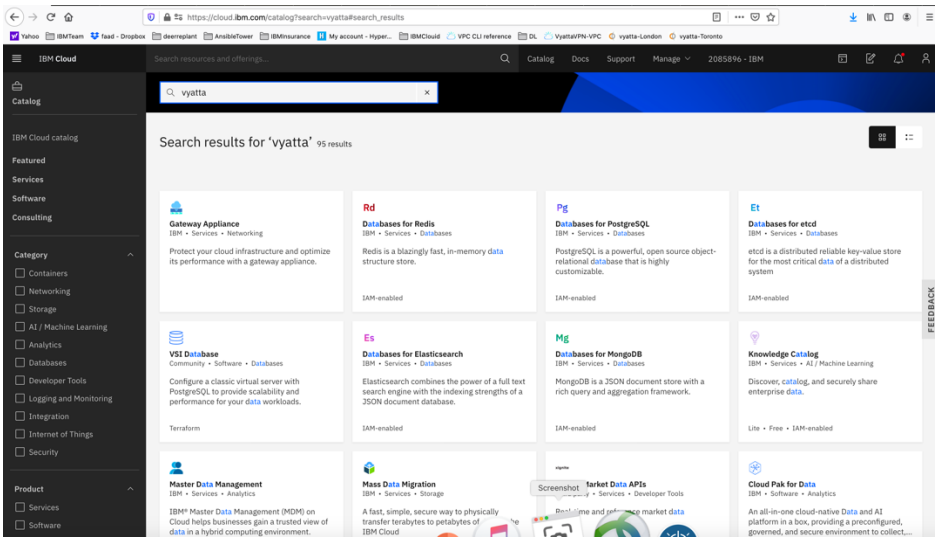
After this step is complete, support will request that you open a new IBM support ticket and address it to the Power System. Include the information in the original DL ticket. This new ticket will be sent to the PowerVS location support to configure their side of the DL connection.

This should be the last step before DL communication works. You can test your connection by pinging IBM Cloud Linux/Windows VSI from your Power VSIs and in reverse.

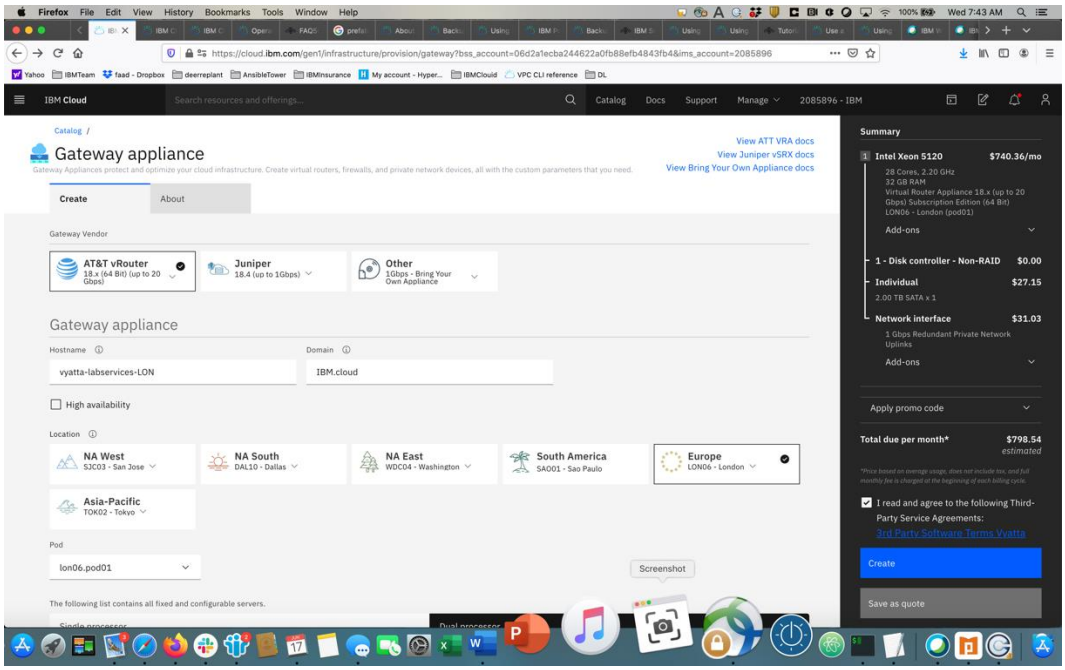
Order Vyatta Gateways in each PowerVS location

In our scenarios we used two Vyatta Gateways, one in each PowerVS location to provide site-to-site VPN for PowerVS location-to-PowerVS location communication using GRE tunnels between Vyatta and PowerVS location and IPsec tunnel between two Vyattas over public internet.

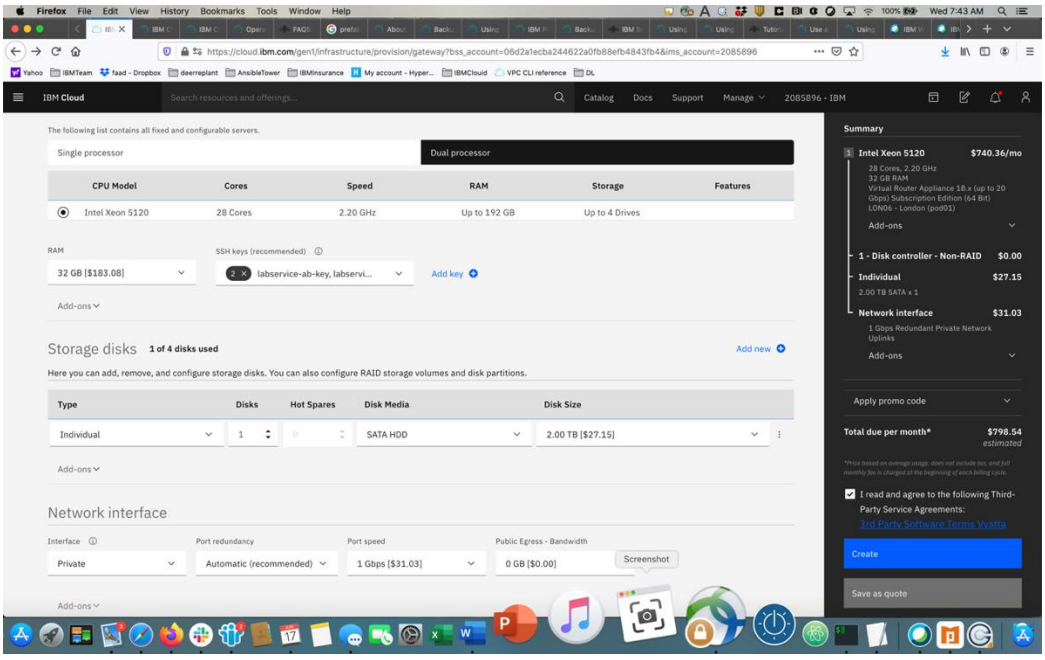
Login to IBM Cloud and click on the “Catalog”, then search for vyatta.



Select “Gateway Appliance” and click on it.

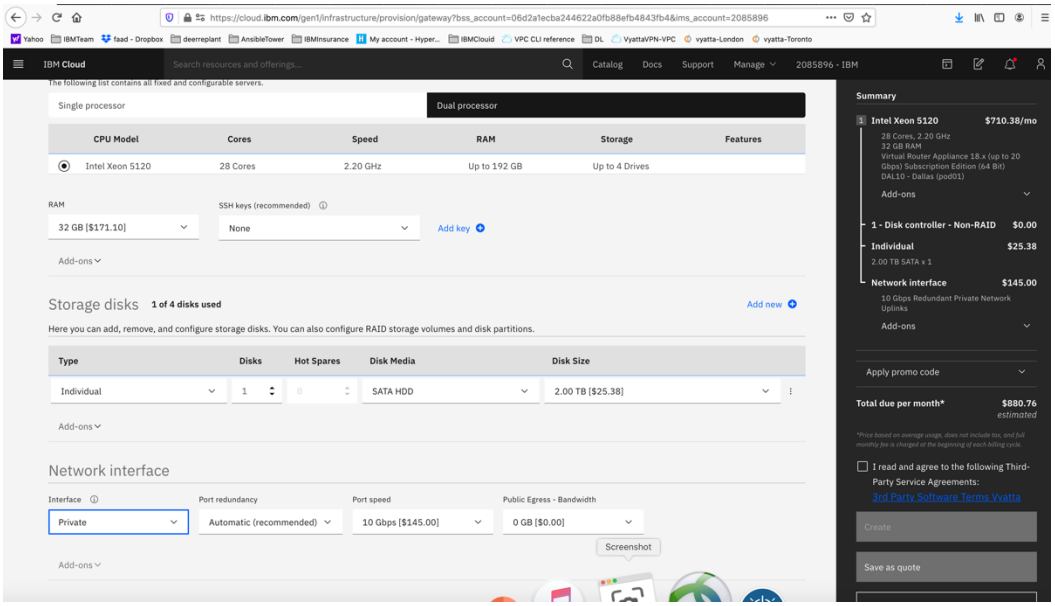


Select “AT&T vRouter”. This is the Vyatta Gateway. You have other choices of Gateways, but we will use Vyatta.
Provide a name for the Gateway and include the PowerVS location name in it so you can distinguish them later.
Select Location to match your PowerVS location.



Choose the following options:

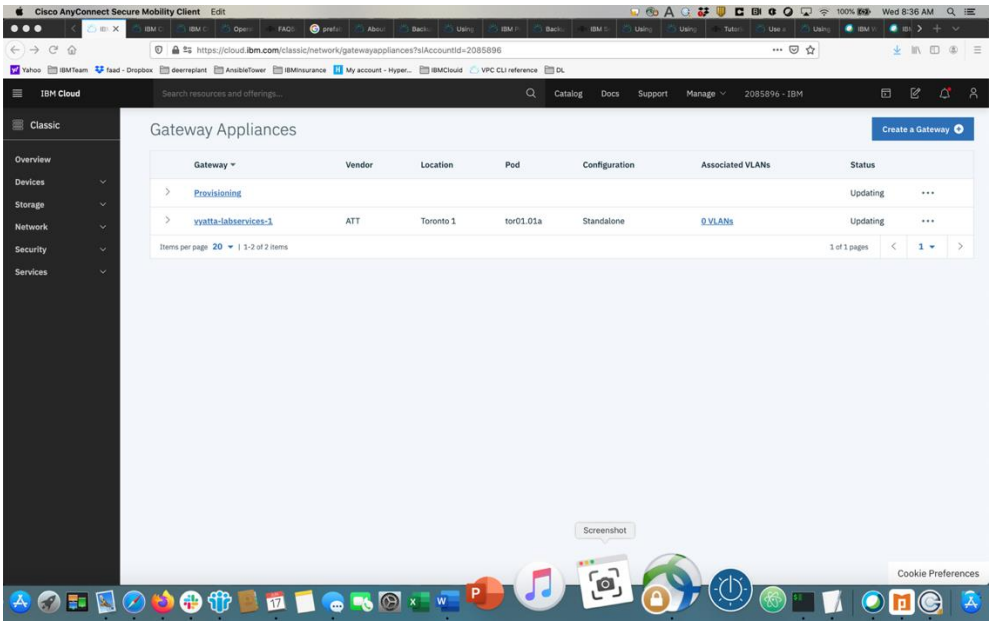
- *Uncheck the High Availability option unless you wish to order one which means you will order two Vyatta Gateways in each PowerVS location. We uncheck this option.*
- *Select the location by pressing on the arrow key in each location to find the exact datacenter where you PowerVS location are located.*
- *You may need to choose the POD if there are several PODs in the selected datacenter location.*
- *Select the CPU single or dual processor. We chose Single Processor.*
- *Select the amount of RAM you wish and add ssh keys if you like to login without password. This can be done later too.*
- *Choose Private network interface unless you wish to use the default which is public/private interface. We chose private network interface only.*



Now check the box to agree with service agreement on the bottom-right side and press “Create”
The vyatta gateway is now being provisioned. This may take several hours.

You will need to do this process in each of the two PowerVS locations.

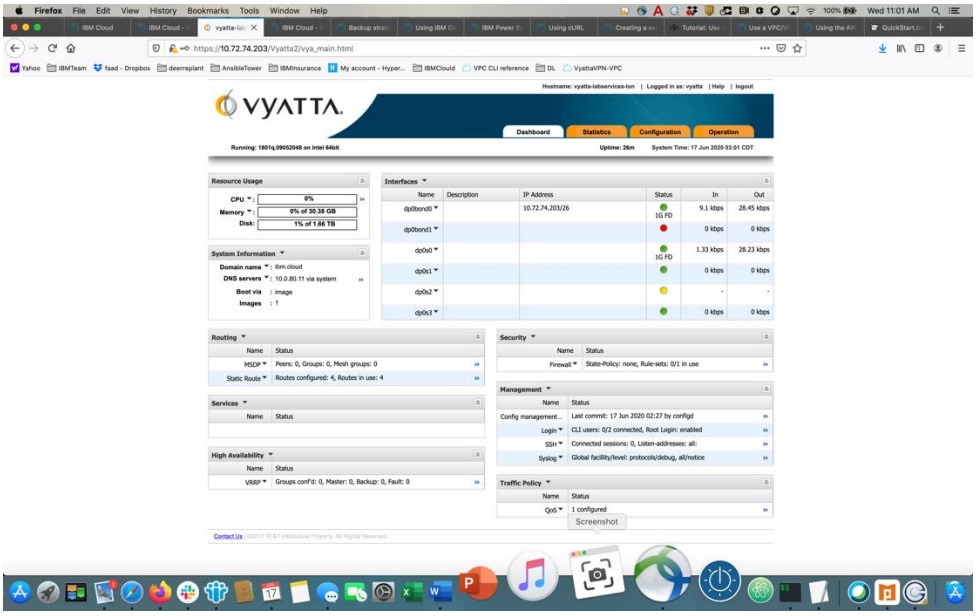
After the Vyatta Gateway is provisioned, you can see it listed under “Devices” where you can find your “vyatta” and “root” user passwords.



To log into the vyatta gateway, use a browser and access it via the link:

https://<ip address of the vyatta gateway>

user: vyatta
password: as show under “devices” in IBM Cloud UI and password tab on the left.



Typically, you will use a command line to ssh to the vyatta for further configuration. You will use the “vyatta” user id to do the configurations.

Request a Generic Routing Encapsulation (GRE) tunnel

You will need to open a support ticket to Power Systems and request that a GRE tunnel be provisioned in each PowerVS location. You will need to provide information on the subnets you created in the PowerVS location. They will provision their end of the GRE tunnel and send you the information you will need so you can continue and provision your end of the GRE tunnel on the Vyatta Gateways.

Power Support team will send you the following information for your GRE tunnels after they complete their end of the GRE tunnel:

TOR01:

TOR:
ASR End:
Tunnel IP -- 172.20.8.2/30
Tunnel Source -- 10.254.0.30
Tunnel Destination-- 10.114.118.18

Vyatta End:
Tunnel IP -- 172.20.8.1/30
Tunnel Source -- 10.114.118.18
Tunnel Destination -- 10.254.0.30 (edited)

LON06:

LON:
ASR END:
Tunnel IP -- 172.20.2.2/30
Tunnel Source -- 10.254.0.26
Tunnel Destination -- 10.72.74.212

Vyatta End:
Tunnel IP -- 172.20.2.1/30
Tunnel Source -- 10.72.74.212
Tunnel Destination -- 10.254.0.26

Setup PowerVS location GRE tunnels in Vyatta Gateways

The following references may help in configuring GRE tunnels:

https://cloud.ibm.com/docs/virtual-router-appliance?topic=solution-tutorials-configuring-IPSEC-VPN

https://docs.huihoo.com/vyatta/6.5/Vyatta-Tunnels_6.5R1_v01.pdf

https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-configuring-power

Open a command window on your Mac/Window.

Note: Prior to login to a 10.x.x.x private IPs in IBM Cloud you will need to start your MotionPro Plus VPN access.

Setup GRE PowerVS location Tunnel in LON06:

userID: vyatta
Password: as show in the GUI
ssh vyatta@10.72.74.212
ssh to LON06 Vyatta Gateway.

We are using the information provided by support for LON06 GRE

LON06:

LON:
ASR END:
Tunnel IP -- 172.20.2.2/30
Tunnel Source -- 10.254.0.26
Tunnel Destination -- 10.72.74.212

Vyatta End:
Tunnel IP -- 172.20.2.1/30
Tunnel Source -- 10.72.74.212
Tunnel Destination -- 10.254.0.26

Run the following commands:
We have chosen to call our tunnel “tun0” on the Vyatta Gateway.

- *configure*
- *set interfaces tunnel tun0 address 172.20.2.1/30*
- *set interfaces tunnel tun0 local-ip 10.72.74.212*
- *set interfaces tunnel tun0 remote-ip 10.254.0.26*
- *set interfaces tunnel tun0 encapsulation gre*
- *set interfaces tunnel tun0 mtu 1300*
- *commit*
- *exit*

```
vyatta@vyatta-ipsec-2-lod06:~$ configure

[edit]
vyatta@vyatta-ipsec-2-lod06# set interfaces tunnel tun0 address 172.20.2.1/30
[edit]
vyatta@vyatta-ipsec-2-lod06# set interfaces tunnel tun0 local-ip 10.72.74.212
[edit]
vyatta@vyatta-ipsec-2-lod06# set interfaces tunnel tun0 remote-ip 10.254.0.26
[edit]
vyatta@vyatta-ipsec-2-lod06# set interfaces tunnel tun0 encapsulation gre
[edit]
vyatta@vyatta-ipsec-2-lod06# set interfaces tunnel tun0 mtu 1300
[edit]
vyatta@vyatta-ipsec-2-lod06# commit
[edit]
vyatta@vyatta-ipsec-2-lod06# exit
logout
vyatta@vyatta-ipsec-2-lod06:~$ show interfaces tunnel
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
tun0             172.20.2.1/30                     u/u
```

You can verify that your GRE tunnel is setup by running the following commands:

- *show interfaces tunnel*
- *Or to get more info:*
- *Show interface tunnel tun0*
- *exit*

```
vyatta@vyatta-ipsec-2-lod06:~$ configure

[edit]
vyatta@vyatta-ipsec-2-lod06# show interfaces tunnel tun0
 tunnel tun0 {
        address 172.20.2.1/30
        encapsulation gre
        local-ip 10.72.74.212
        mtu 1300
        remote-ip 10.254.0.26
 }
```

Setup GRE PowerVS location Tunnel in TOR01:

userID: vyatta
Password: as show in the GUI
ssh vyatta@10.114.118.18

ssh to Tor01 Vyatta Gateway.
TOR01:

TOR:
ASR End:
Tunnel IP -- 172.20.8.2/30
Tunnel Source -- 10.254.0.30
Tunnel Destination-- 10.114.118.18

Vyatta End:
Tunnel IP -- 172.20.8.1/30
Tunnel Source -- 10.114.118.18
Tunnel Destination -- 10.254.0.30 (edited)

Run the following commands:
We have chosen to call our tunnel “tun0” in the Vyatta Gateway same as the other Vyatta Gateway.

- *configure*
- *set interfaces tunnel tun0 address 172.20.8.1/30*
- *set interfaces tunnel tun0 local-ip 10.114.118.18*
- *set interfaces tunnel tun0 remote-ip 10.254.0.30*
- *set interfaces tunnel tun0 encapsulation gre*
- *set interfaces tunnel tun0 mtu 1300*
- *commit*
- *exit*

```
vyatta@vyatta-ipsec-2-tor01:~$ configure

[edit]
vyatta@vyatta-ipsec-2-tor01# set interfaces tunnel tun0 address 172.20.8.1/30
[edit]
vyatta@vyatta-ipsec-2-tor01# set interfaces tunnel tun0 local-ip 10.114.118.18
[edit]
vyatta@vyatta-ipsec-2-tor01# set interfaces tunnel tun0 remote-ip 10.254.0.30
[edit]
vyatta@vyatta-ipsec-2-tor01# set interfaces tunnel tun0 encapsulation gre
[edit]
vyatta@vyatta-ipsec-2-tor01# set interfaces tunnel tun0 mtu 1300
[edit]
vyatta@vyatta-ipsec-2-tor01# commit
[edit]
vyatta@vyatta-ipsec-2-tor01# exit
logout
vyatta@vyatta-ipsec-2-tor01:~$ show interfaces tunnel
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
tun0             172.20.8.1/30                  u/u
```

To show the status:

- *show interfaces tunnel*
- *Or to get more info:*
- *Show interface tunnel tun0*
- *exit*

```
vyatta@vyatta-ipsec-2-tor01:~$ configure

[edit]
vyatta@vyatta-ipsec-2-tor01# show interfaces tunnel tun0
 tunnel tun0 {
        address 172.20.8.1/30
        encapsulation gre
        local-ip 10.114.118.18
        mtu 1300
```

Finally, you need to set static route in each Vyatta to point the traffic to the GRE tunnels.

in TOR01 Vyatta:

- *configure*
- *set protocols static route 192.168.6.0/24 next-hop 172.20.8.2*
- *commit*
- *exit*

in LON06 Vyatta:

- *configure*
- *set protocols static route 192.168.50.0/24 next-hop 172.20.2.2*
- *commit*
- *exit*

Setup site-to-site IPsec tunnel between Two Vyatta Gateways

In this section you will setup a site-to-site IPsec tunnel between the two vyatta gateways to allow for cross Vyatta connection over the public interface. All commands are for Vyatta vyos OS type. Other router/gateway types will have different commands to perform these actions.

In this scenario we are simulating a remote customer datacenter to be one of the two PowerVS locations in IBM Cloud. In this case, LON06 is simulating a remote customer datacenter and TOR01 is the cloud PowerVS location.
Customers who have their own routers in their datacenters, will not need to order two Vyatta routers. Instead only need one Vyatta router in the IBM Cloud located in same geo as their PowerVS location geo location in the IBM Cloud.

TOR01 Vyatta IPsec Configuration:

Local Public IP: 158.85.94.90
Peer Public IP: 158.176.145.42
Remote Subnet Prefix: 192.168.50.0/24
Local Subnet Prefix: 192.168.6.0/24

Need to replace items in color below with you own values on run these commands on the Vyatta gateway in TOR01.

```
configure
set security vpn ipsec esp-group ESP01 pfs 'enable'
set security vpn ipsec esp-group ESP01 proposal 1 encryption
'aes256'
set security vpn ipsec esp-group ESP01 proposal 1 hash
'sha2_512'
set security vpn ipsec esp-group ESP01 mode 'tunnel'
set security vpn ipsec esp-group ESP01 pfs 'dh-group5'
set security vpn ipsec ike-group IKE01 proposal 1 dh-group '5'
set security vpn ipsec ike-group IKE01 proposal 1 encryption
'aes256'
set security vpn ipsec ike-group IKE01 proposal 1 hash
'sha2_512'
set security vpn ipsec site-to-site peer 158.176.145.42
authentication pre-shared-secret 'iamsecret2'
set security vpn ipsec site-to-site peer 158.176.145.42
default-esp-group 'ESP01'
set security vpn ipsec site-to-site peer 158.176.145.42 ike-
group 'IKE01'
set security vpn ipsec site-to-site peer 158.176.145.42 tunnel
1 esp-group 'ESP01'
set security vpn ipsec site-to-site peer 158.176.145.42 local-
address '158.85.94.90'
set security vpn ipsec site-to-site peer 158.176.145.42 tunnel
1 local prefix '192.168.6.0/24'
set security vpn ipsec site-to-site peer 158.176.145.42 tunnel
1 remote prefix '192.168.50.0/24'
commit
exit
```

Below shows the output of all the commands ran. The value of pre-shared-secret is encrypted in this output and shown as "********".

```
vyatta@vyatta-ipsec-2-tor01:~$ show configuration commands | grep ipsec
set security vpn ipsec esp-group ESP01 mode 'tunnel'
set security vpn ipsec esp-group ESP01 pfs 'dh-group5'
set security vpn ipsec esp-group ESP01 proposal 1 encryption 'aes256'
set security vpn ipsec esp-group ESP01 proposal 1 hash 'sha2_512'
set security vpn ipsec ike-group IKE01 proposal 1 dh-group '5'
set security vpn ipsec ike-group IKE01 proposal 1 encryption 'aes256'
set security vpn ipsec ike-group IKE01 proposal 1 hash 'sha2_512'
set security vpn ipsec site-to-site peer 158.176.145.42 authentication pre-shared-secret '********'
set security vpn ipsec site-to-site peer 158.176.145.42 connection-type 'initiate'
set security vpn ipsec site-to-site peer 158.176.145.42 default-esp-group 'ESP01'
set security vpn ipsec site-to-site peer 158.176.145.42 ike-group 'IKE01'
set security vpn ipsec site-to-site peer 158.176.145.42 local-address '158.85.94.90'
set security vpn ipsec site-to-site peer 158.176.145.42 tunnel 1 esp-group 'ESP01'
set security vpn ipsec site-to-site peer 158.176.145.42 tunnel 1 local prefix '192.168.6.0/24'
set security vpn ipsec site-to-site peer 158.176.145.42 tunnel 1 remote prefix '192.168.50.0/24'
```

LON06 IPsec Configuration:

Local Public IP: 158.176.145.42
Peer Public IP: 158.85.94.90
Local Subnet Prefix: 192.168.50.0/24
Remote Subnet Prefix: 192.168.6.0/24

Need to run these commands on the Vyatta gateway in LON06.

- *configure*
- *set security vpn ipsec esp-group ESP01 pfs 'enable'*
- *set security vpn ipsec esp-group ESP01 proposal 1 encryption 'aes256'*
- *set security vpn ipsec esp-group ESP01 proposal 1 hash 'sha2_512'*
- *set security vpn ipsec esp-group ESP01 pfs 'dh-group5'*
- *set security vpn ipsec ike-group IKE01 proposal 1 dh-group '5'*
- *set security vpn ipsec ike-group IKE01 proposal 1 encryption 'aes256'*
- *set security vpn ipsec ike-group IKE01 proposal 1 hash 'sha2_512'*
- *set security vpn ipsec site-to-site peer 158.85.94.90 authentication pre-shared-secret 'iamsecret2'*
- *set security vpn ipsec site-to-site peer 158.85.94.90 default-esp-group 'ESP01'*
- *set security vpn ipsec site-to-site peer 158.85.94.90 ike-group 'IKE01'*
- *set security vpn ipsec site-to-site peer 158.85.94.90 local-address '158.176.145.42'*
- *set security vpn ipsec site-to-site peer 158.85.94.90 tunnel 1 esp-group 'ESP01'*
- *set security vpn ipsec site-to-site peer 158.85.94.90 tunnel 1 local prefix '192.168.50.0/24'*
- *set security vpn ipsec site-to-site peer 158.85.94.90 tunnel 1 remote prefix '192.168.6.0/24'*
- *commit*
- *exit*

Below shows the output of all the commands ran. The value of pre-shared-secret is encrypted in this output and shown as “********”.

```
vyatta@vyatta-ipsec-2-lod06:~$ show configuration commands | grep ipsec
set security vpn ipsec esp-group ESP01 mode 'tunnel'
set security vpn ipsec esp-group ESP01 pfs 'dh-group5'
set security vpn ipsec esp-group ESP01 proposal 1 encryption 'aes256'
set security vpn ipsec esp-group ESP01 proposal 1 hash 'sha2_512'
set security vpn ipsec ike-group IKE01 proposal 1 dh-group '5'
set security vpn ipsec ike-group IKE01 proposal 1 encryption 'aes256'
set security vpn ipsec ike-group IKE01 proposal 1 hash 'sha2_512'
set security vpn ipsec site-to-site peer 158.85.94.90 authentication pre-shared-secret '********'
set security vpn ipsec site-to-site peer 158.85.94.90 connection-type 'initiate'
set security vpn ipsec site-to-site peer 158.85.94.90 default-esp-group 'ESP01'
set security vpn ipsec site-to-site peer 158.85.94.90 ike-group 'IKE01'
set security vpn ipsec site-to-site peer 158.85.94.90 local-address '158.176.145.42'
set security vpn ipsec site-to-site peer 158.85.94.90 tunnel 1 esp-group 'ESP01'
set security vpn ipsec site-to-site peer 158.85.94.90 tunnel 1 local prefix '192.168.50.0/24'
set security vpn ipsec site-to-site peer 158.85.94.90 tunnel 1 remote prefix '192.168.6.0/24'
```

Check the status of the IPsec tunnel by running this command on each vyatta gateway:

- *show vpn ipsec status*

```
vyatta@vyatta-ipsec-2-lod06:~$ show vpn ipsec status
IPSec Process Running PID: 8466

1 Active IPsec Tunnels
```

Check the setting of the IPsec tunnel by running this command:

- *show vpn ipsec sa*

```
vyatta@vyatta-ipsec-2-lod06:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
158.85.94.90                            158.176.145.42

    Tunnel  Id          State  Bytes Out/In   Encrypt       Hash      DH A-Time  L-Time
    ------  ----------  -----  -------------  ------------  --------  -- ------  ------
    1       1           up     0.0/0.0        aes256        sha2_512  2  18898   3600

vyatta@vyatta-ipsec-2-lod06:~$
```

```
vyatta@vyatta-ipsec-2-tor01:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
158.176.145.42                          158.85.94.90

    Tunnel  Id          State  Bytes Out/In   Encrypt       Hash      DH A-Time  L-Time
    ------  ----------  -----  -------------  ------------  --------  -- ------  ------
    1       1           up     0.0/0.0        aes256        sha2_512  2  18889   3600
```

At this point you should have end-to-end connectivity between PowerVS locations and be able to ping between your Power VSIs AIX/IBM i VSIs in each PowerVS location and also from the Power AIX/IBM i VSIs to IBM Cloud services such as Linux/Windows VSI and Object storage.

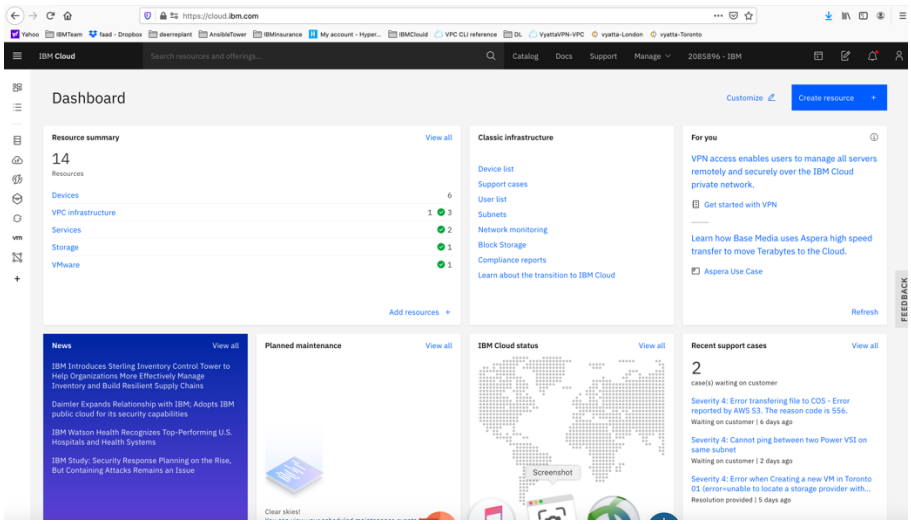
Chapter 2: Implementation

After setting up site-to-site VPN connection, we will verify ping and ssh connectivity between each PowerVS VSIs and from PowerVS VSI to IBM Cloud VSI (Linux VSI).

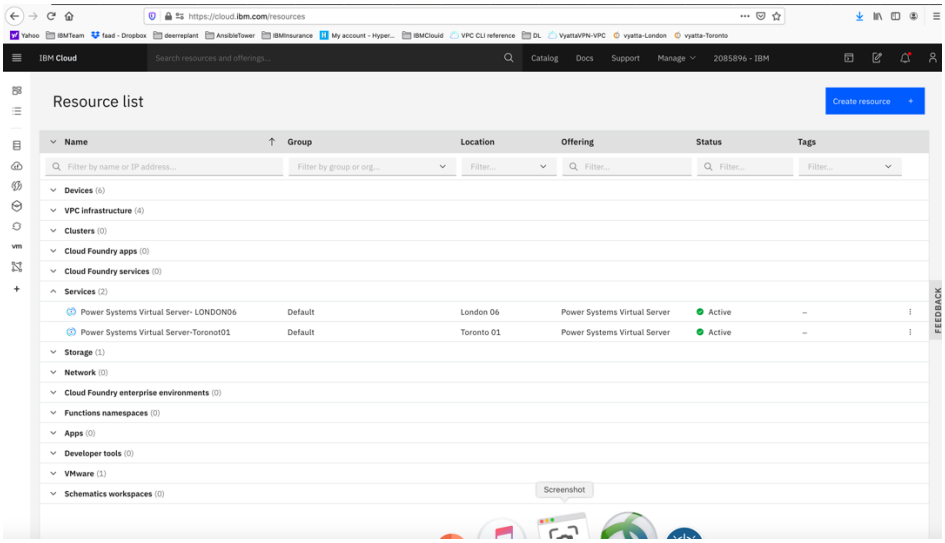
PowerVS and x86 VSI Integration

Provision a PowerVS in the PowerVS location

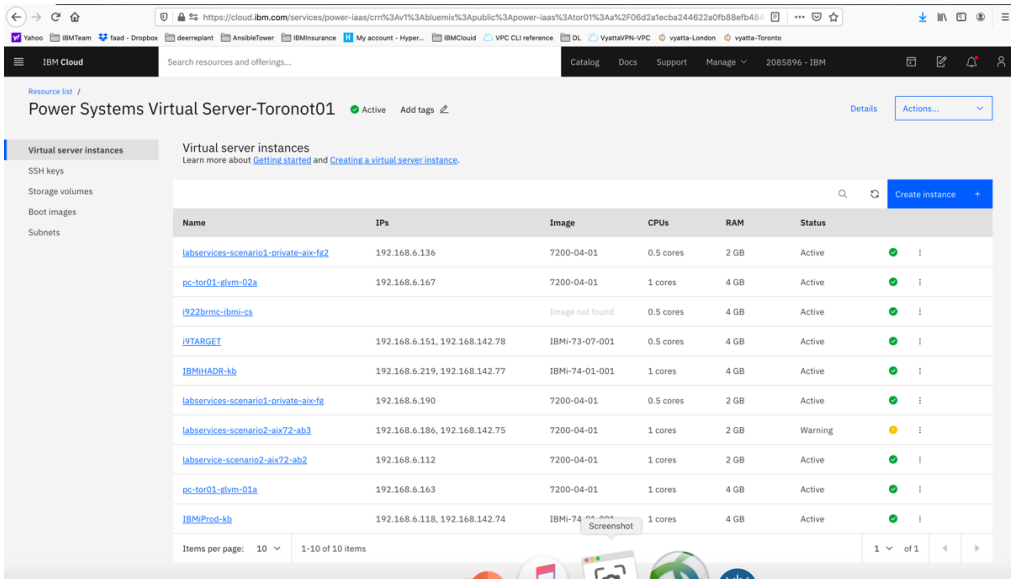
The procedure is similar for both AIX and IBM i VSI provisioning, except for the OS types. Here is a procedure to create an AIX 7.2 VSI. The cost shown are monthly cost, but you are being charged hourly.
Go to the IBM Cloud Catalog and press the “IBM Cloud” on top left side of the UI.



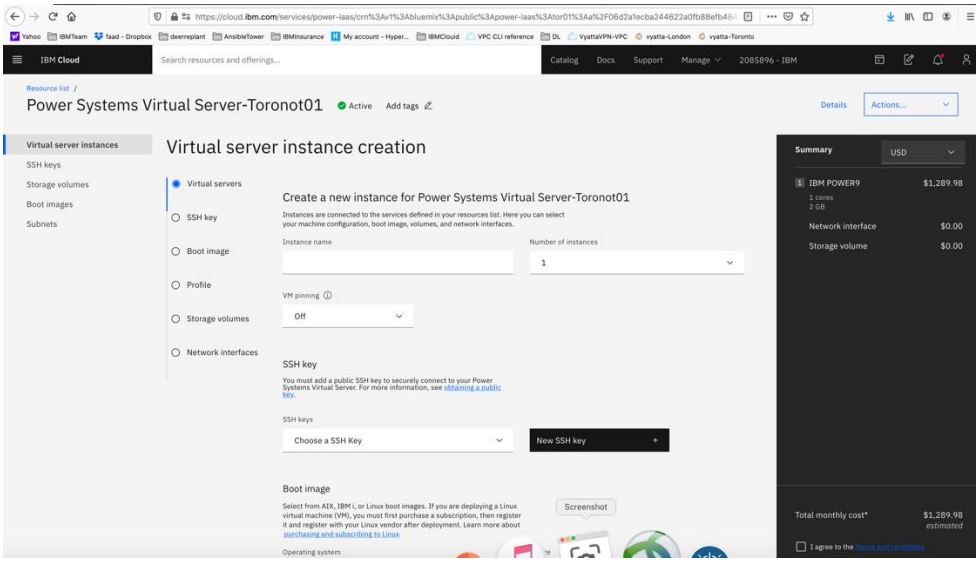
Choose “Services” from the list shown.



Click on the service for each datacenter in which you have created a PowerVS location power service. In this case we will choose Toronot01 service.

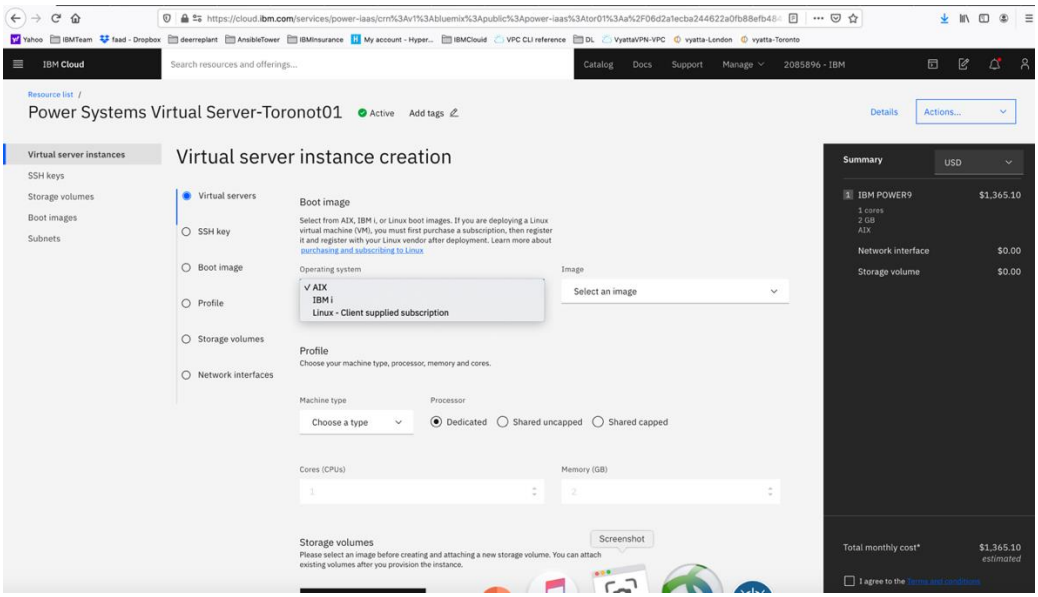


Since we have already provisioned several VSI, we see the list show above. If you are creating VSIs for the first time, your list will be empty.
Press “Create Instance” on upper right-hand side.



This is where you provision AIX or IBM i VSIs.
Choose a name for your VSI, i.e., AIX-72-Tor01 and select how many VSIs you need to configure. The names of the VSI will be appended with a “-1”, “-2” etc. if you select more than one VSI.
You may leave VM pruning and SSH key as is since the VSIs will have no passwords when you create them for the first time.

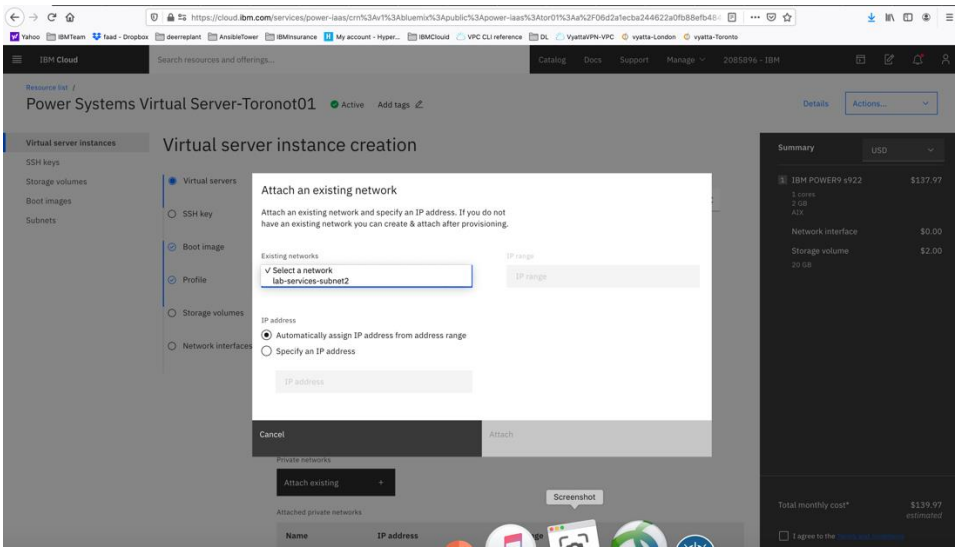
Scroll down to choose other options.



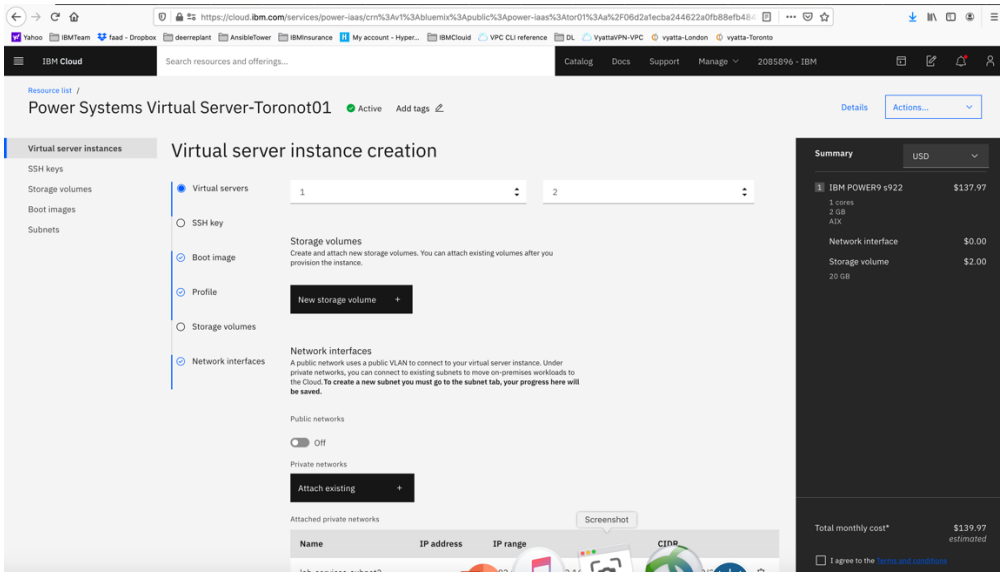
Here you will choose the following options:

- *Operating System – AIX or IBM i or any other image you may have imported.*
- *Image type: AIX 7.1 or 7.2, etc.*
- *Disk types: Type 1 or 3. Type 3 is cheaper option which we selected.*
- *Machine type: S922 or E980*
- *Processor: Dedicated or Shared or Shared Capped. We choose "shared" as its less expensive.*
- *Choose the number of cores and RAM you will need. The minimum core is "0.25".*
- *You can also attach additional volume to the VSI is you wish. We did not do that here and only used the root volume which is included.*

Next you will scroll down to choose your subnet on which these VSIs will be provisioned. It is assumed you have already created one or more subnets prior to this step.
Click on the "Attached Existing ".



Choose the subnet you wish to attach, and the press “Attach”

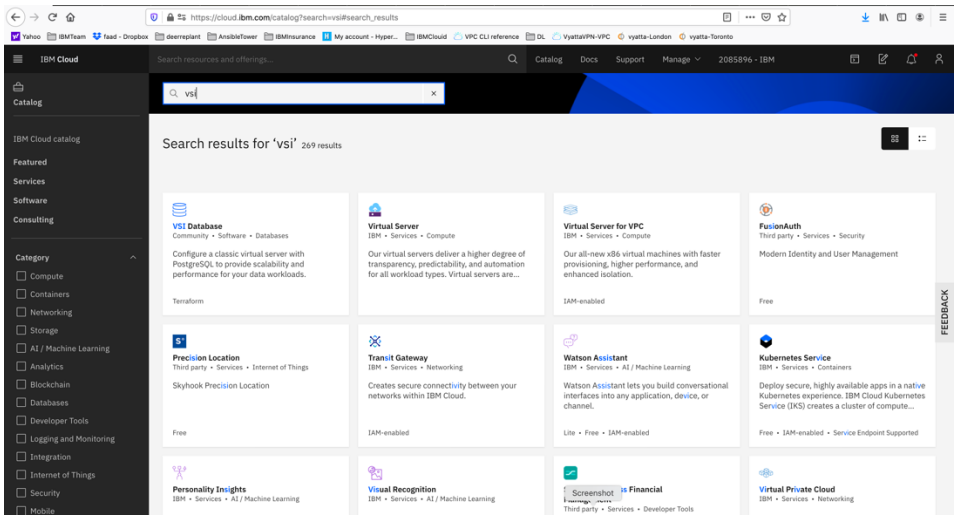


Now check the box “I agree to the ….” And press “create Instance” in lower right-hand side.
Your VSI is now being provisioned.

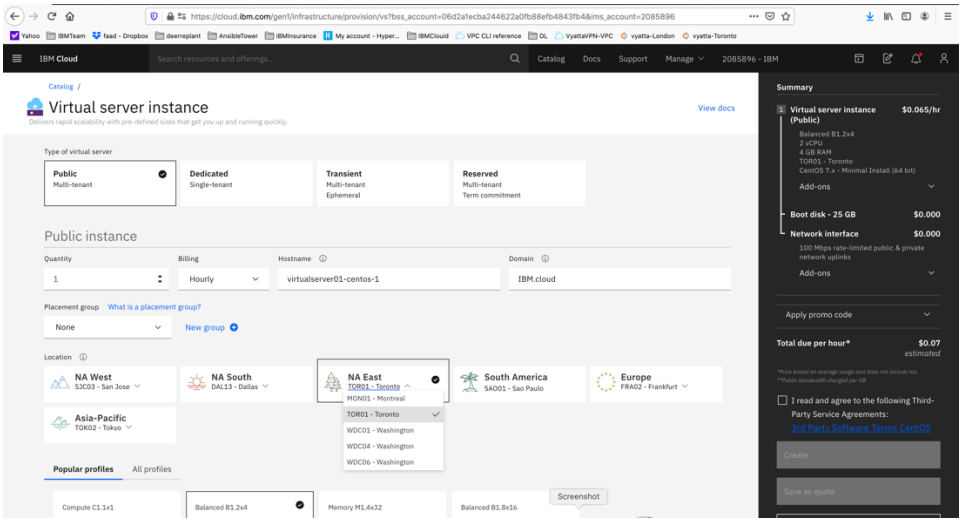
Provision a Linux VSI in IBM cloud

Login to IBM Cloud UI and choose “catalog”

Search for “vsi”

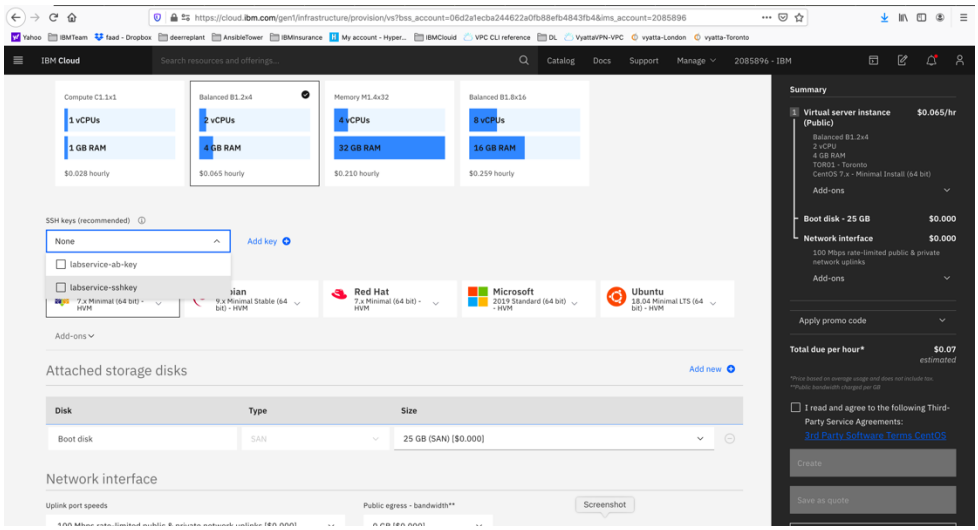


Select “virtual server”

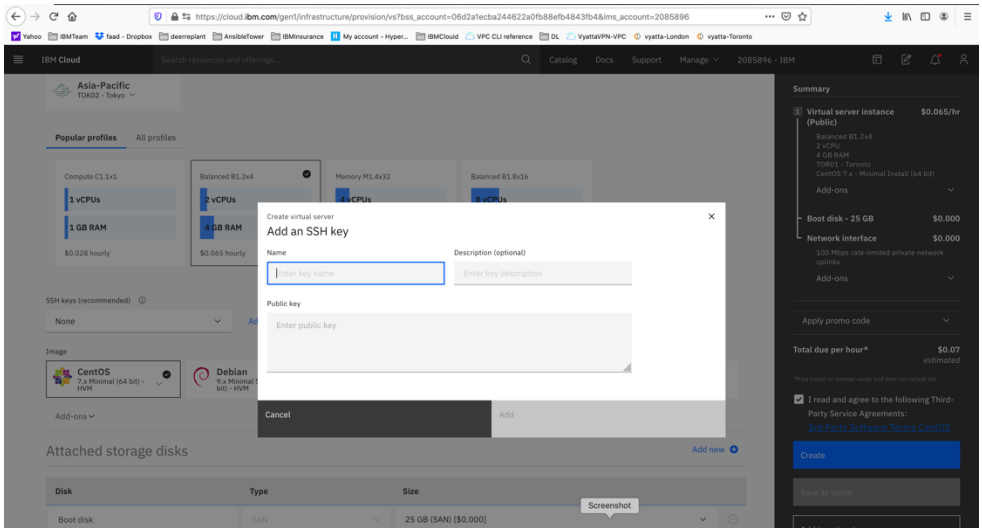


Choose “public” and give the server a Hostname

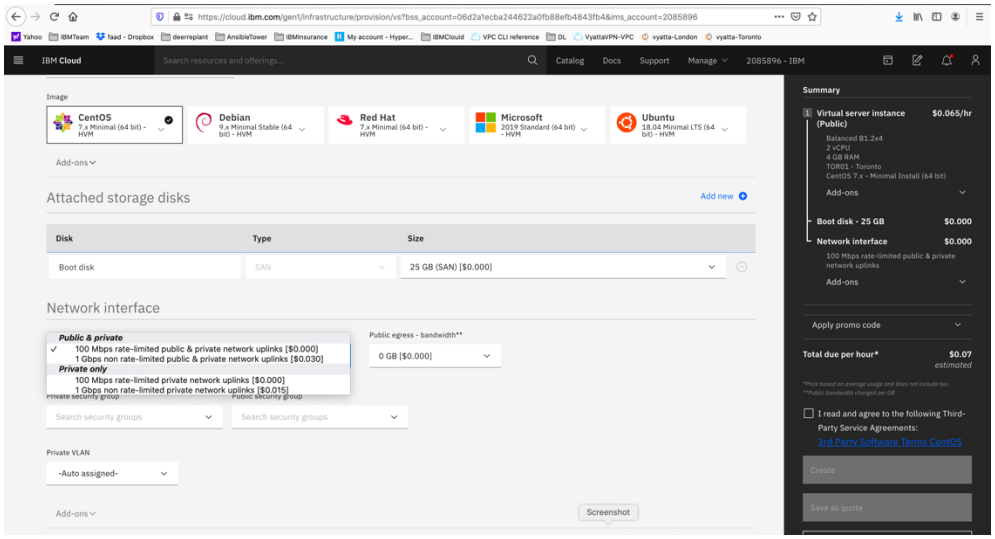
Select Location. In this case we selected Tor01.



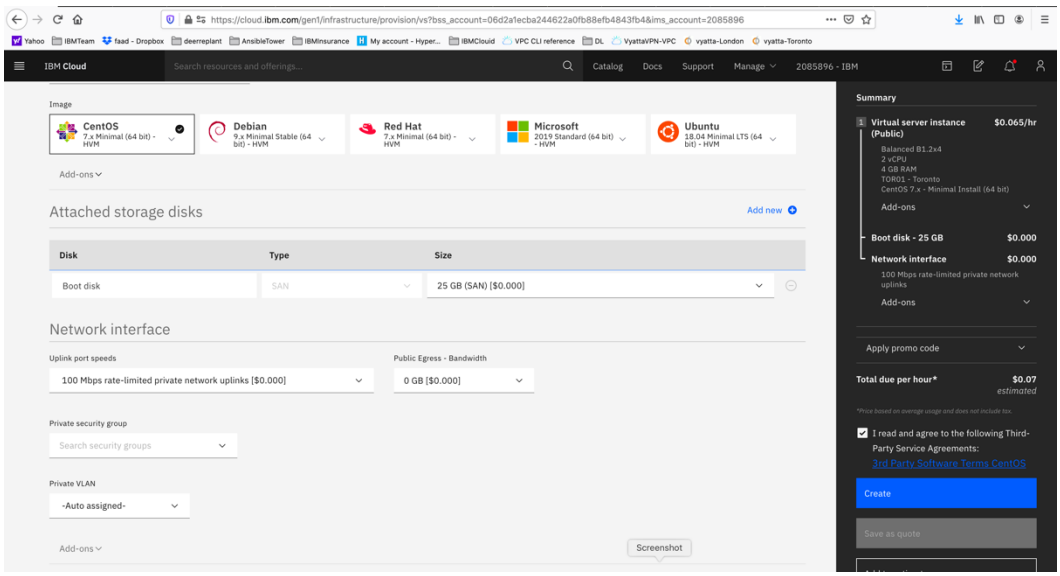
- *Select a profile for your RAM and CPU.*
- *Choose your OS type.*
- *Choose a ssh key if you want to access this VSI via ssh and without a password. You can create an ssh key by clicking on "add key" and enter a name for your profile and your private ssh key which you already may have on your laptop or follow steps to generate an ssh key and then paste it here.*



Choose your network connections under "Network Interface". We only choose Private network in our scenarios.



Accept the agreement on the lower right-hand side and press “Create”



After the VSI is provisioned you can now be able to ping between the Power VSI in the PowerVS location and the VSI in IBM cloud.

If you chose a Public/Private IP for your Linux VSI, then the connection may fail from the PowerVS location VSI. This is due to the fact that the default gateway is now set to a public gateway in your Linux VSI and there is no route back to the PowerVS location VSI.

To correct this, you will need to add a static route to the Linux VSI to tell it how to connect back to the Power VSI PowerVS location.

Run the following command on your Linux VSI:
192.168.6.0/24: is the subnet in your PowerVS location

10.166.112.129: is the private gateway IP of your subnet in PowerVS location which you can find by running “netstat -nr” on you power VSI.

- *ip route add 192.168.6.0/24 via 10.166.112.129*

In order to make this route permanent, you will need to add it to your network setting.

Edit this file:

- *vi /etc/sysconfig/network-scripts/route-eth0*

Add last 3 lines:

[root@labservice-scenaro1-rhel-fg2 network-scripts]# cat route-eth0
Created by cloud-init on instance boot automatically, do not edit.
#
ADDRESS0=10.0.0.0
GATEWAY0=10.166.112.129
NETMASK0=255.0.0.0
ADDRESS1=161.26.0.0
GATEWAY1=10.166.112.129
NETMASK1=255.255.0.0
ADDRESS2=166.8.0.0
GATEWAY2=10.166.112.129
NETMASK2=255.252.0.0
# added to support pinging to PowerVS location for VSI with public IP
ADDRESS3=192.168.6.0
GATEWAY3=10.166.112.129
NETMASK3=255.255.255.0

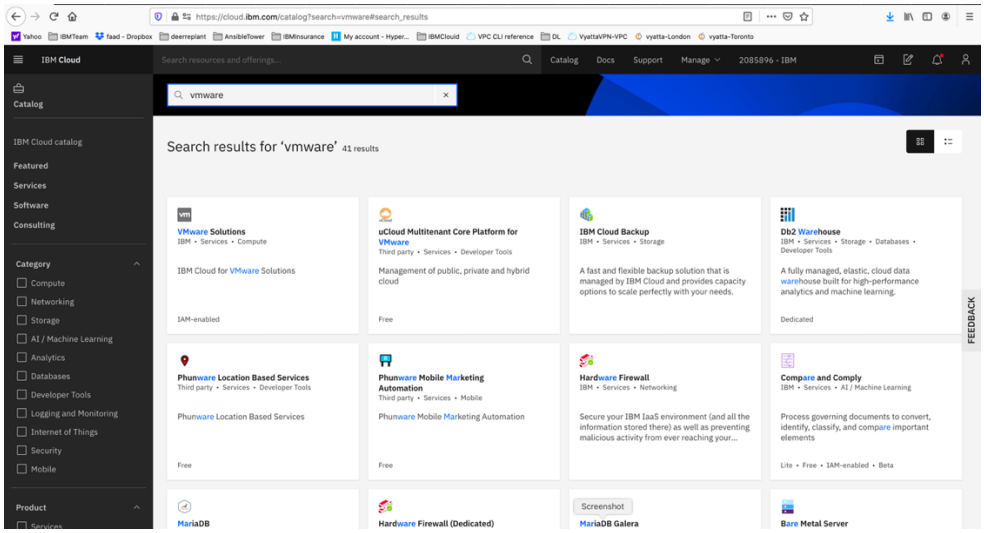
PowerVS and VMware Integration

Create a VMWare Shared

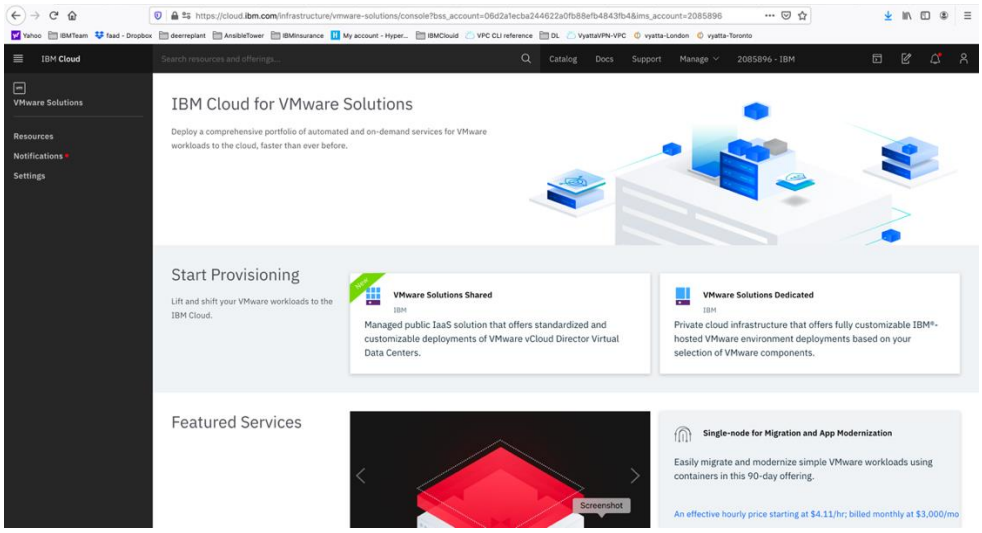
In this section we will first create a VMWare shared and then provision a VM inside the VMWare and test its connectivity to PowerVS.

Login to IBM Cloud and choose “catalog” on upper-right hand side

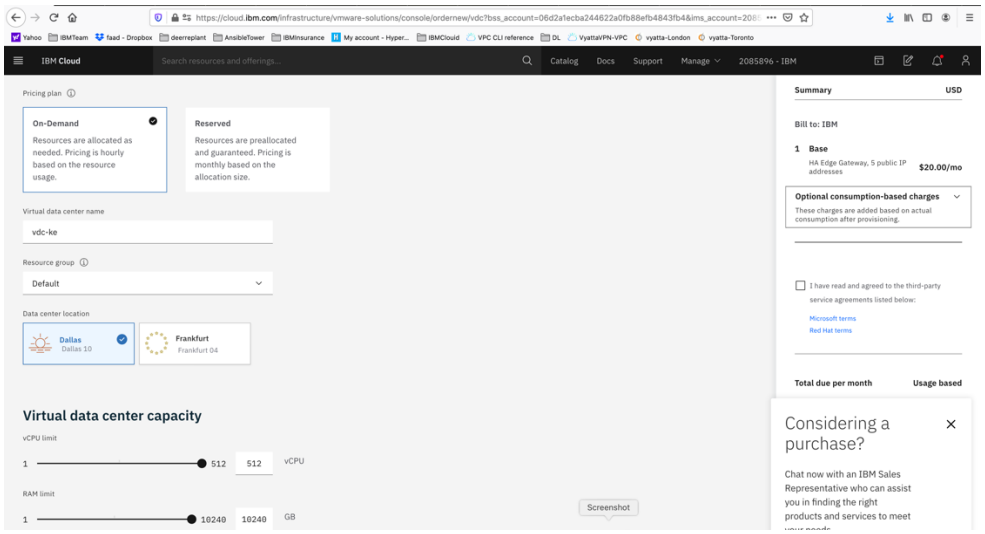
Search for “VMware”



Select “VMware Solutions”

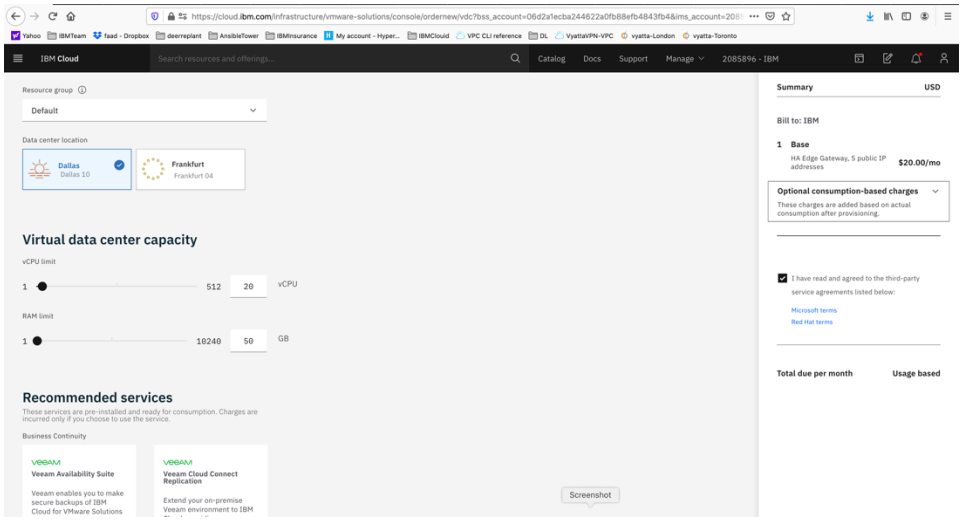


Select “VMware Solution Shared”. This is the less expensive VMware solution.



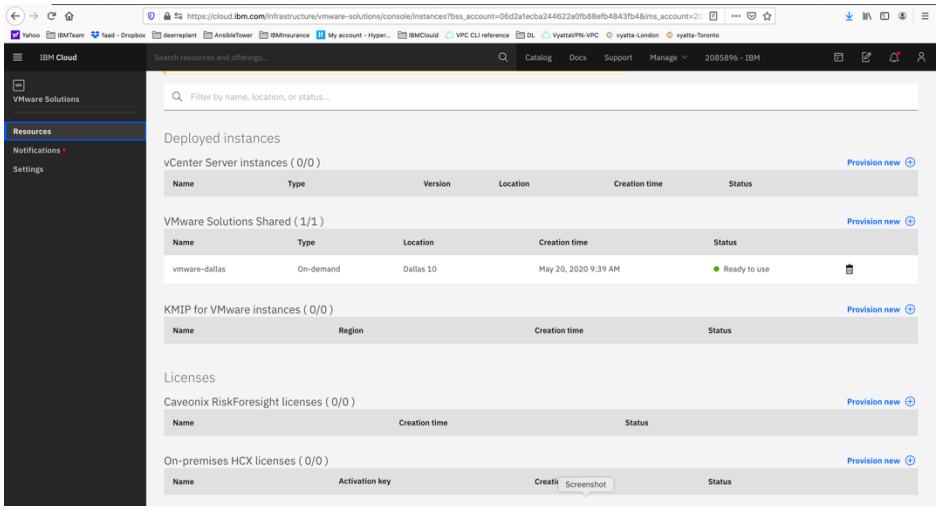
Select:

- *Virtual data center name*
- *Data center location*
- *Virtual data center capacity. We choose 20 vCPU and 50 GB RAM*



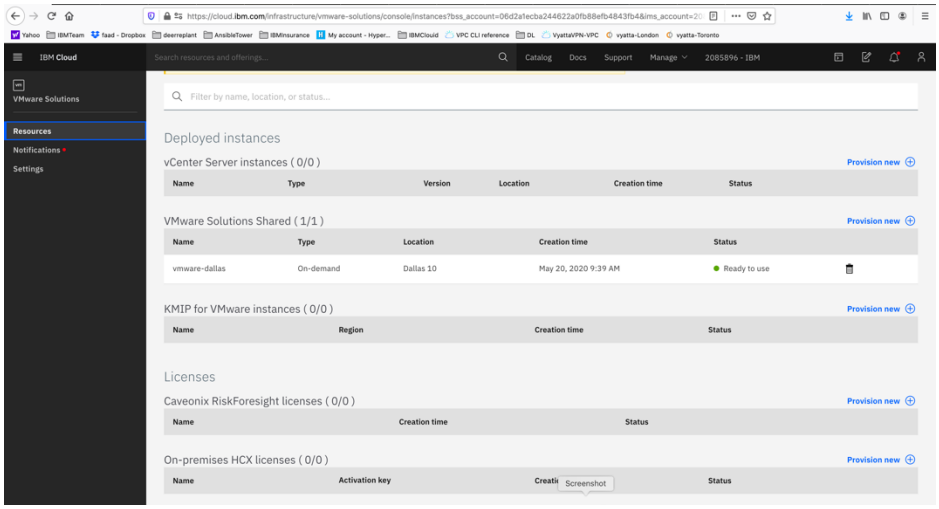
Check the agreement check box and press “create” on lower right-hand side.
You will be provided with a Admin userID and password to allow you to access the configuration website. Store that information on your laptop.

Then under “resources” you should see your VMware Solution Shared name.

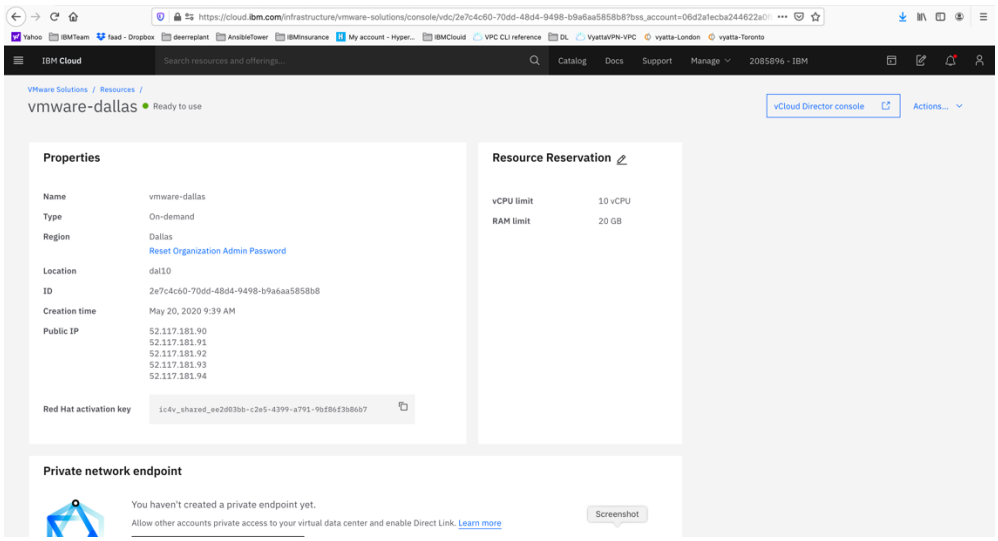


Configure VMware Solution Shared

Click on the name of you VMware Solution Shared below.

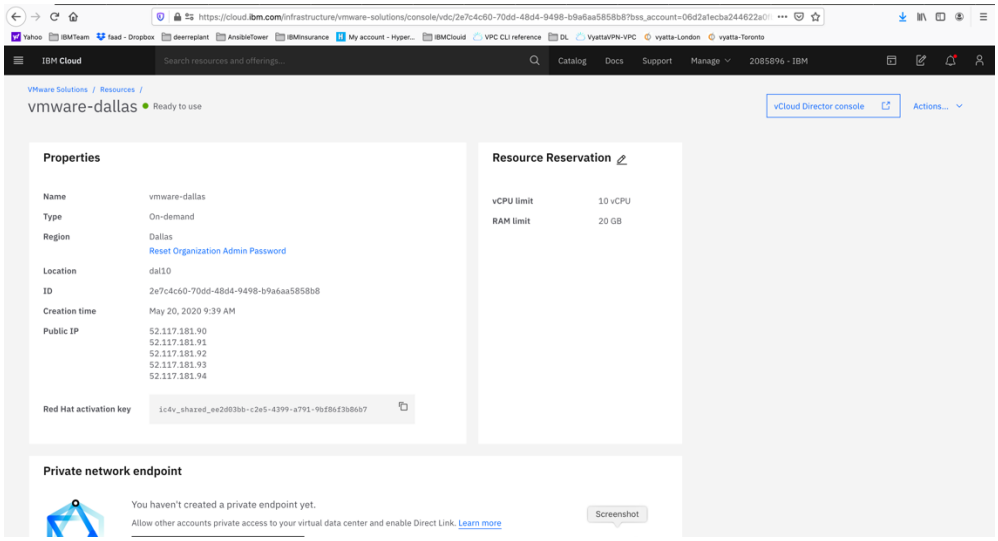


This will show are you VMware settings. There are 5 IPs which are provided by default to be used to assign to your VMs inside the VMware to allow outside network access.

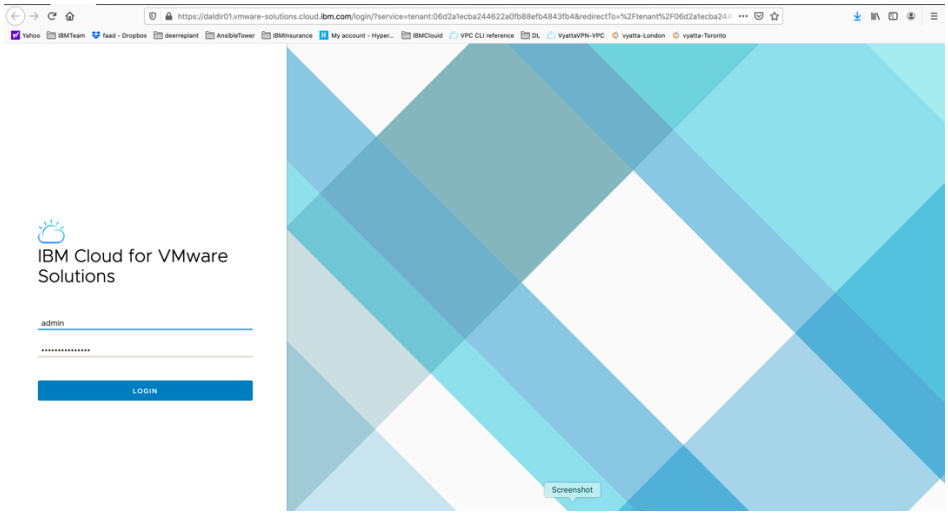


Configure VMware Solution Shared Network

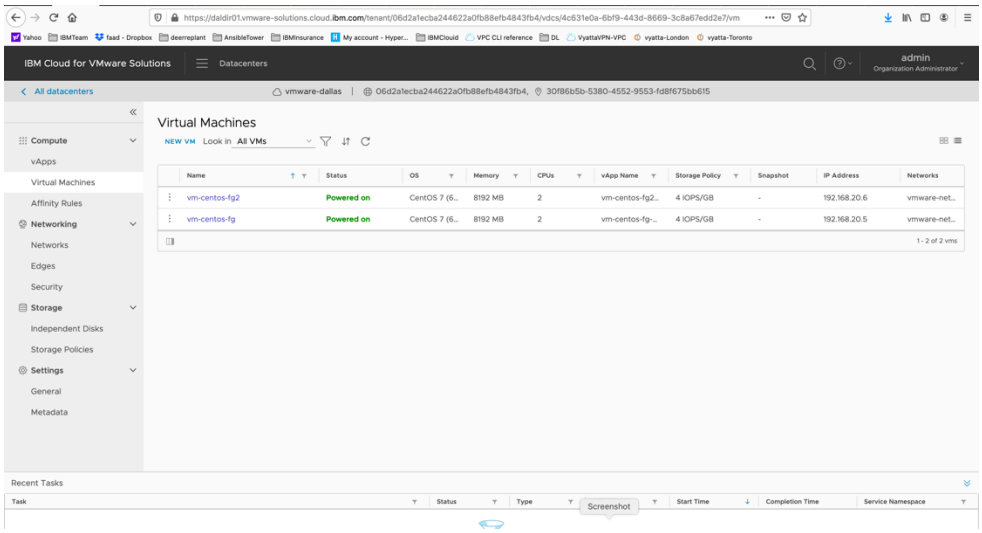
To configure your VMware Solution Shared, press on the “vCloud Director Console” on upper right-hand side.



A browser session will open where you would enter your admin ID and password provided to you when you created the VMware Solution Shared.



Login to the console using admin and password provided.



At this point you need to configure your VMware network before you can provision any VMs. The screen shot above shows that we have already done so and have then provisioned VMs.

Here is a reference site with many training resources on IBM Cloud for VMware Solutions Shared.

https://www.vmware.com/ca/products/cloud-director.html
https://www.ibm.com/demos/collection/VMware-Solutions-on-IBM-Cloud/

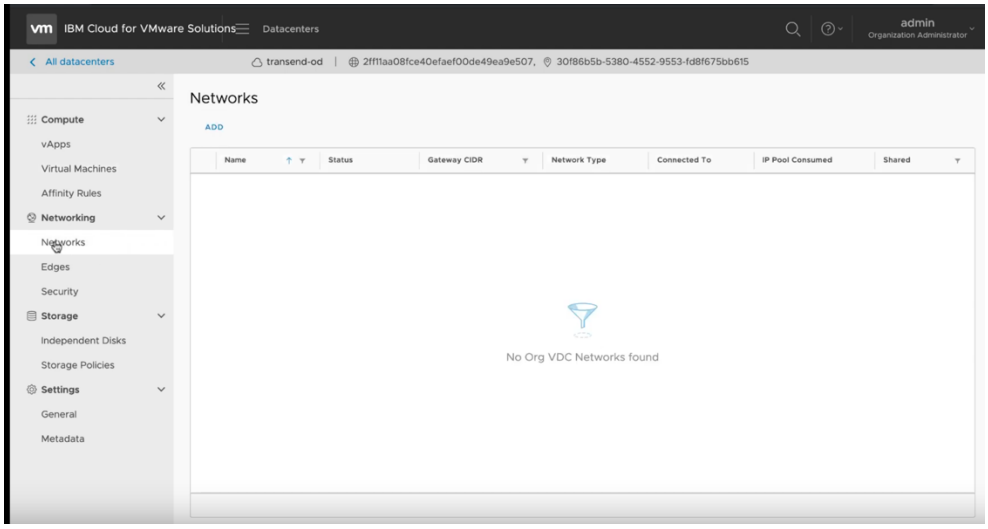
To configure the network including Edge Gateway and NAT and Firewalls, use this video site.

IBM Cloud for VMware Solutions Shared - Setup the Network

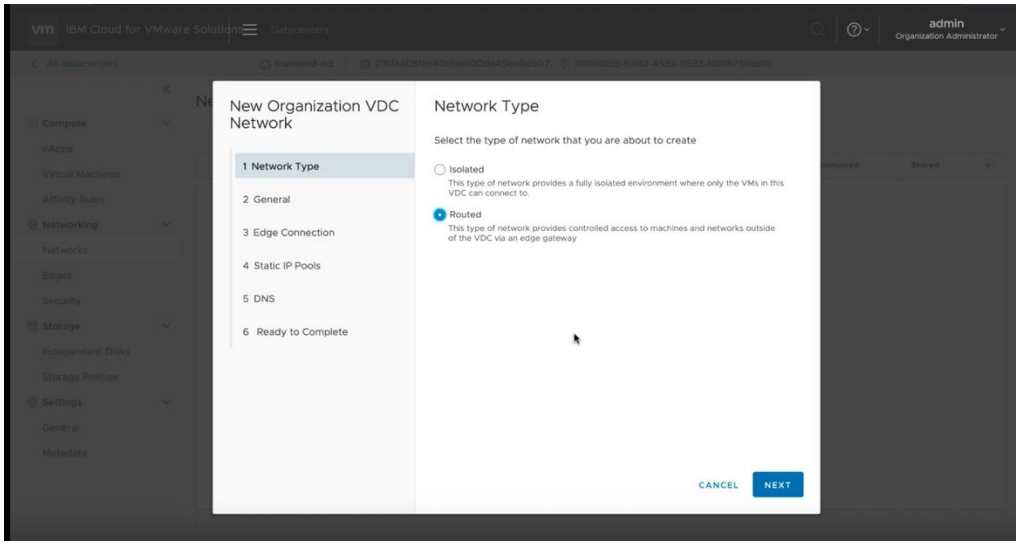
https://www.youtube.com/watch?v=gG0jp3TEtt0

Click on the “network” menu item on the left-hand side.

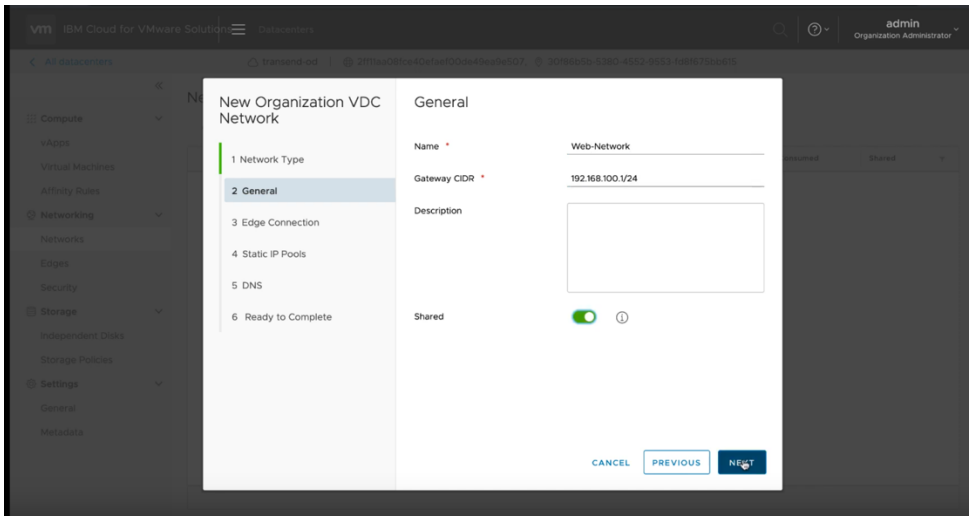
We will now create a network.



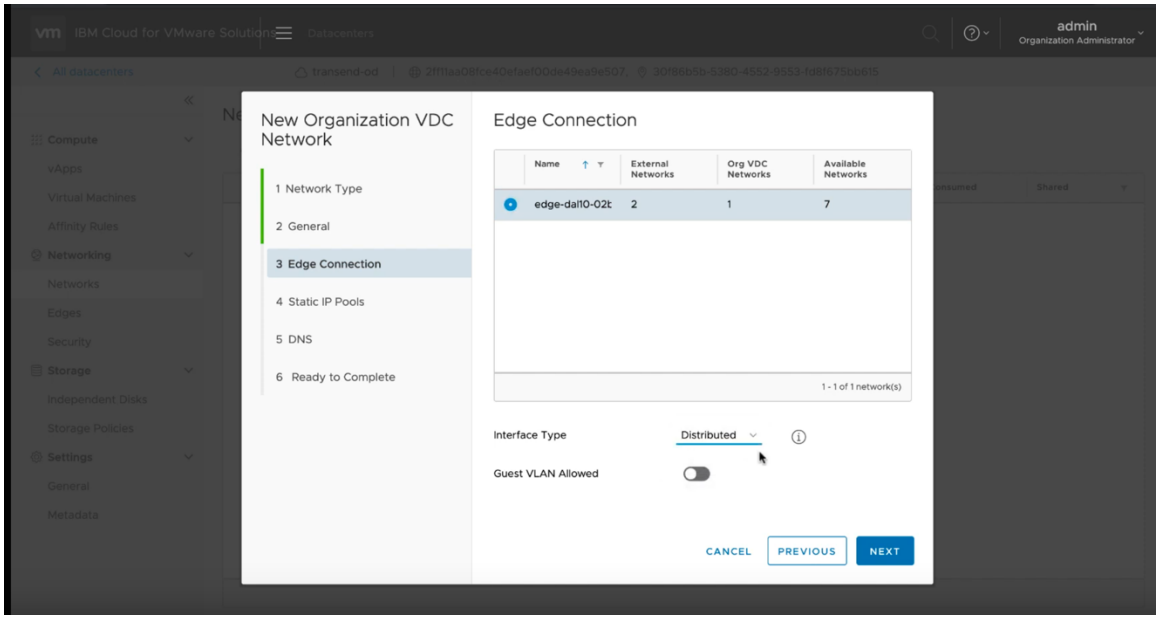
Select “ADD” and then choose “Routed” and press Next



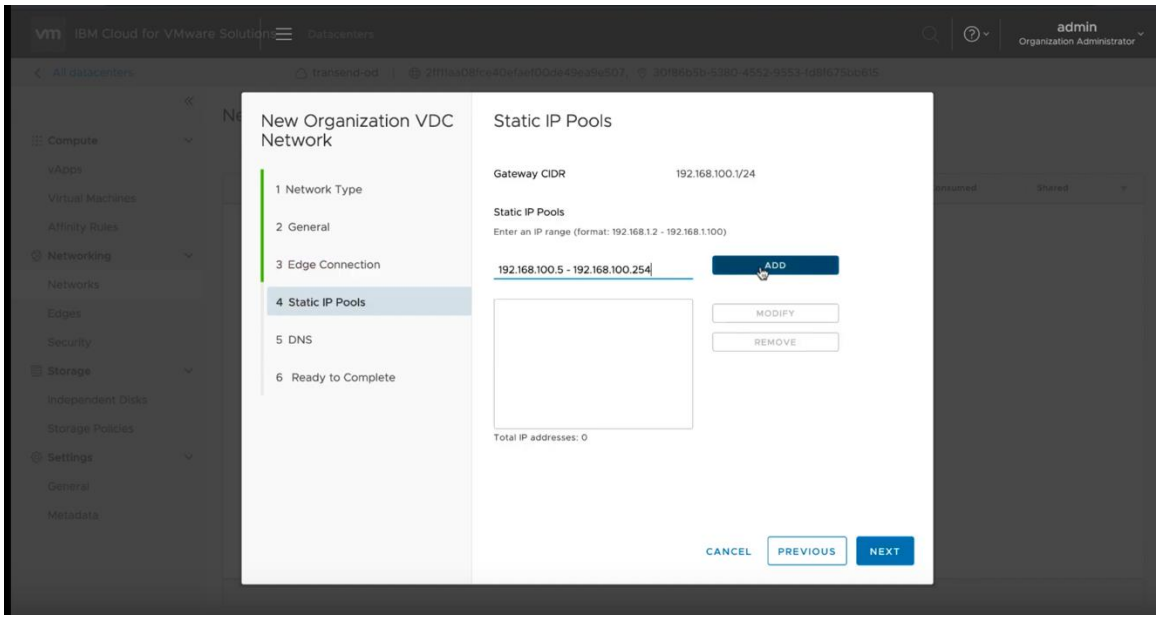
- *Choose a name for your network, i.e. web-network*
- *Select a CIDR range, i.e., 192.168.100.1/24*
- *Choose “Shared” option*
- *Press Next*



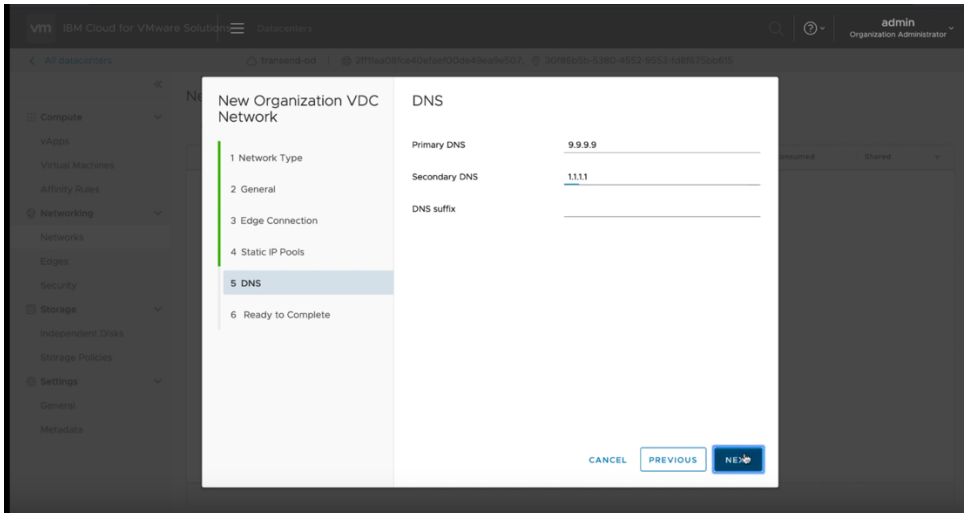
Next select the Edge Gateway name and choose “Distributed” and press NEXT.



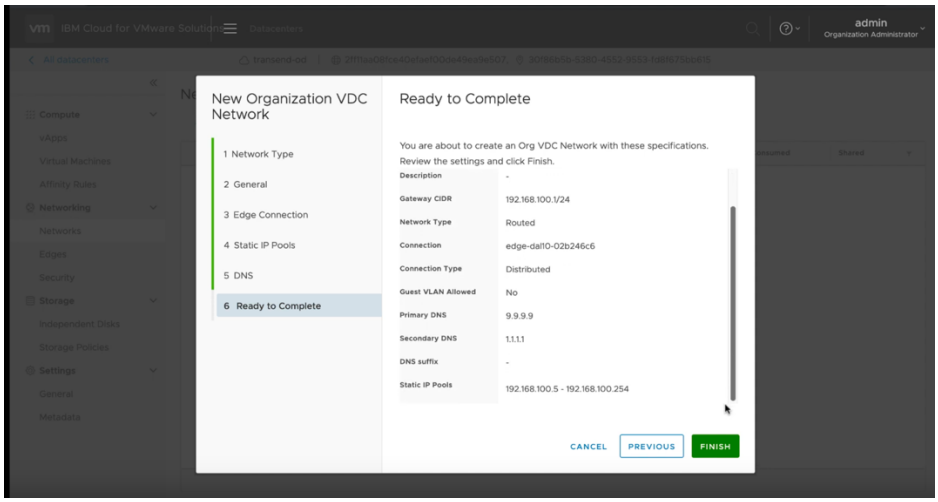
Enter the IP pool range you wish to use. In this case we use a similar range as the CIDR by entering 192.168.100.5 – 192.168.100.254 and then press ADD an then NEXT



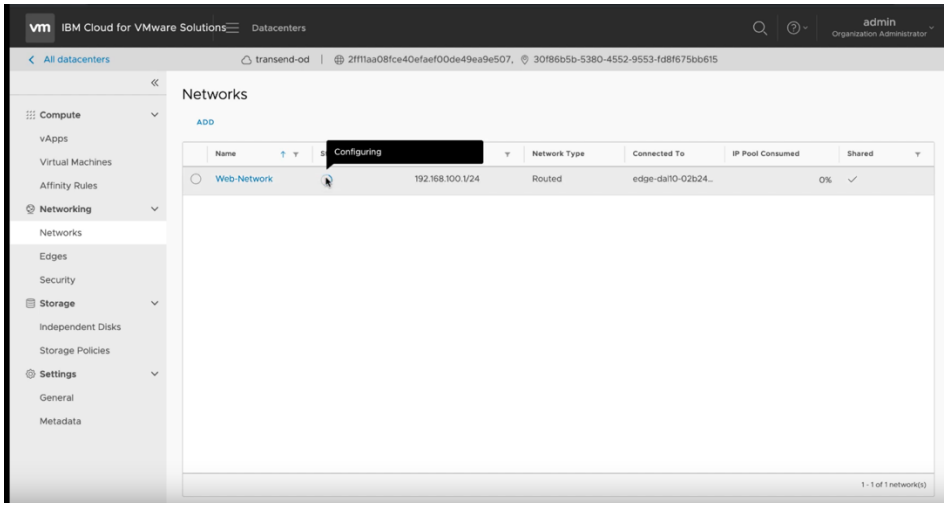
Now enter DNS addresses for external access.
We use 9.9.9.9 and 1.1.1.1 as the two public DNS Primary and Secondary respectively.
Press NEXT



Now you will see the final screen showing your settings.
Press FINISH



Your network is now provisioned successfully.

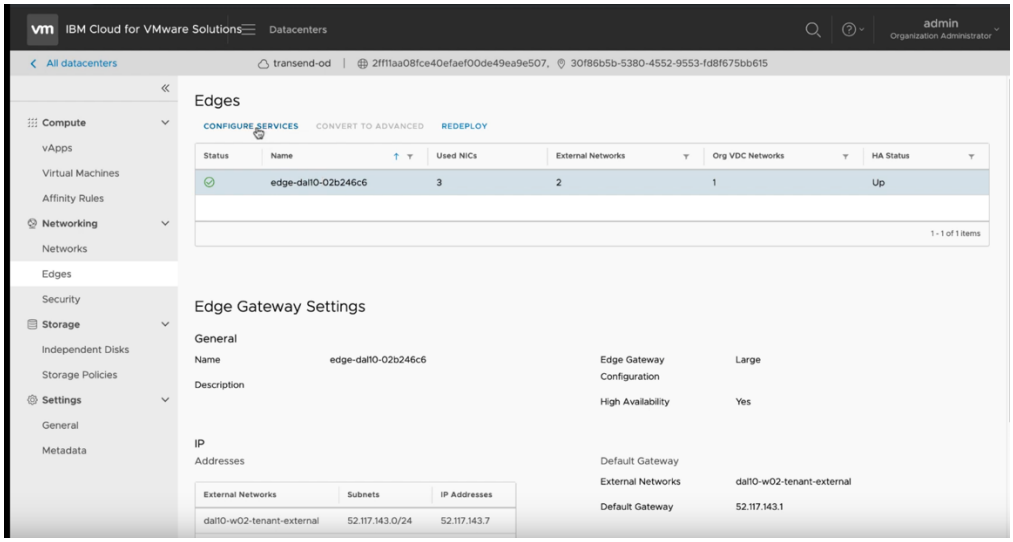


Now we need to create Firewall and Source NAT for Public and Private access to our VMware.

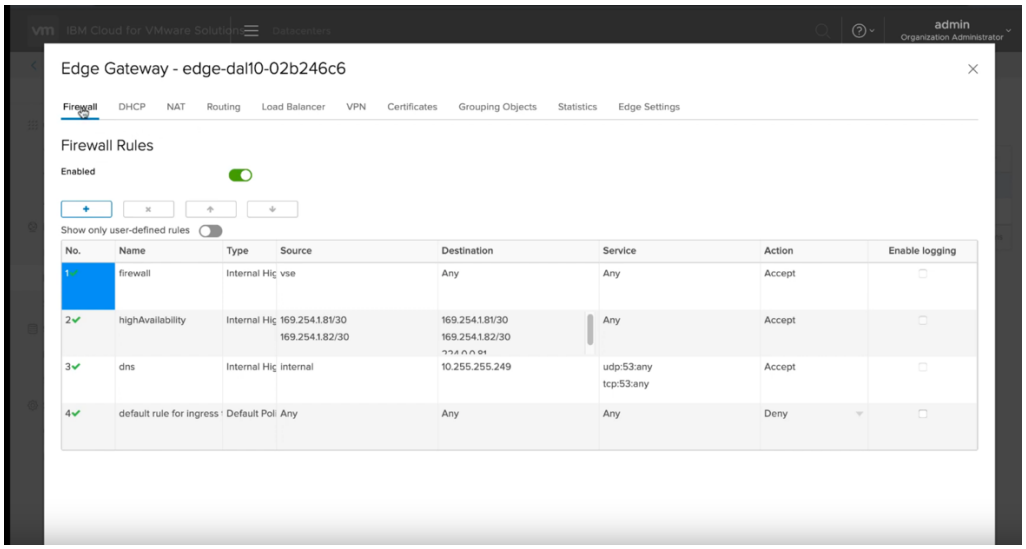
Public Netowrk Access Firewall and Source NAT Configuration

Click on the Edges menu and select the Edge network which was included when you provisioned VMware Shared. The Edge network allows for external access.
You will need to create a Firewall rule and Source NAT (SNAT) to allow access to the external network. For internal access you will need to create a Firewall rule and a Destination NAT (DNAT) rule.
Same procedure will be used later to provide access to the Private network.

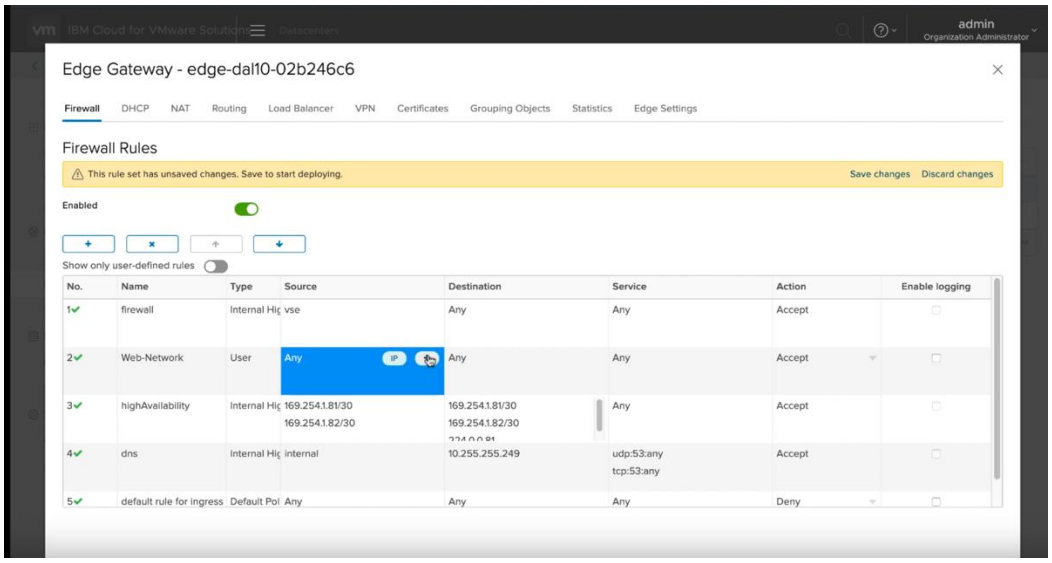
Press “Configure Services”



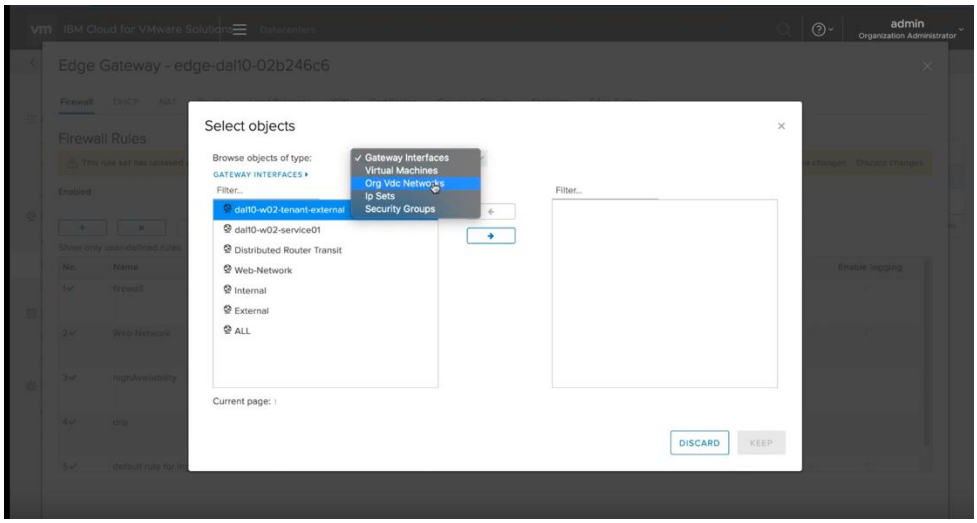
Choose Firewall menu on top.
Choose “+”
A new firewall setting “2” will appear in the list. We will now need to configure this firewall.

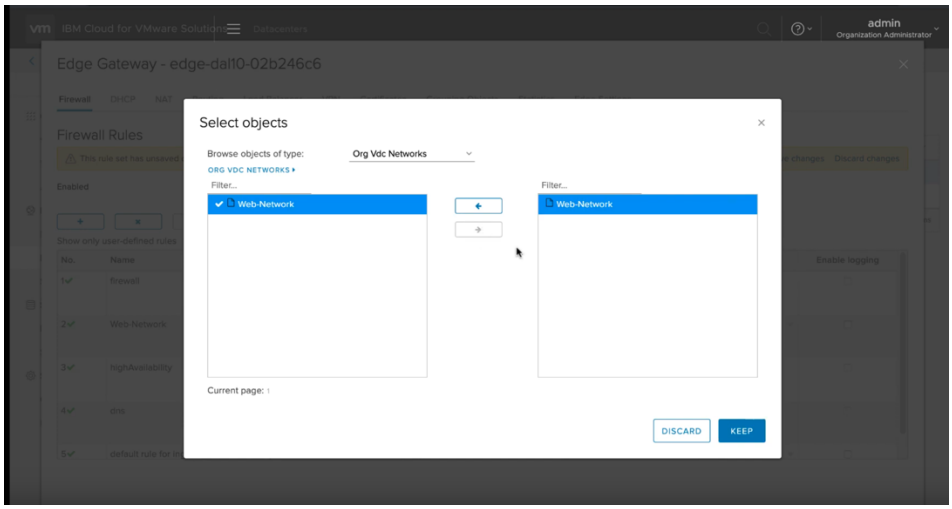


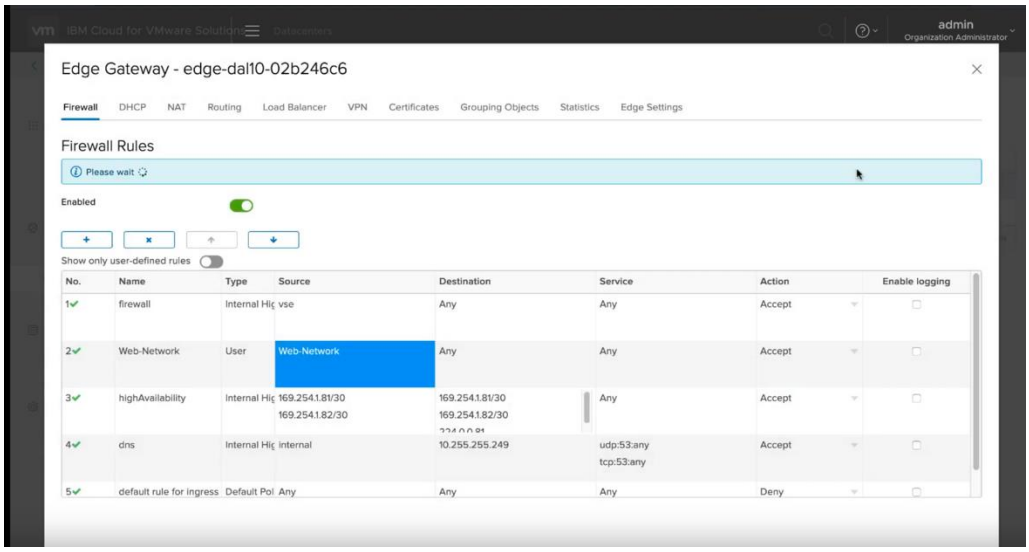
Provide a name for the firewall, i.e. web-network.



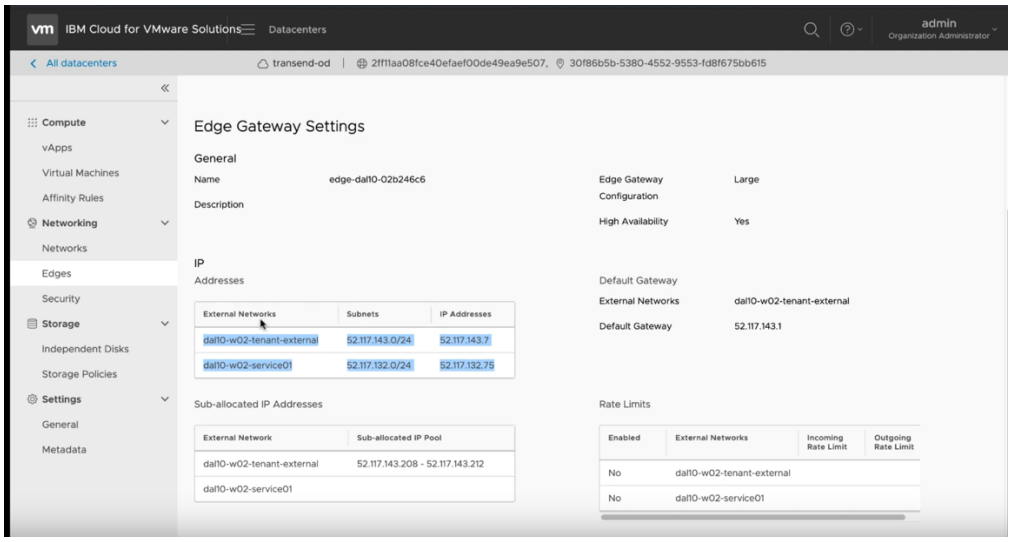
Then choose Source and click on the “+” icon to add a source network.
Choose the network you created before from the list of external networks and press the “+” to add it to the right side.
Then press NEXT

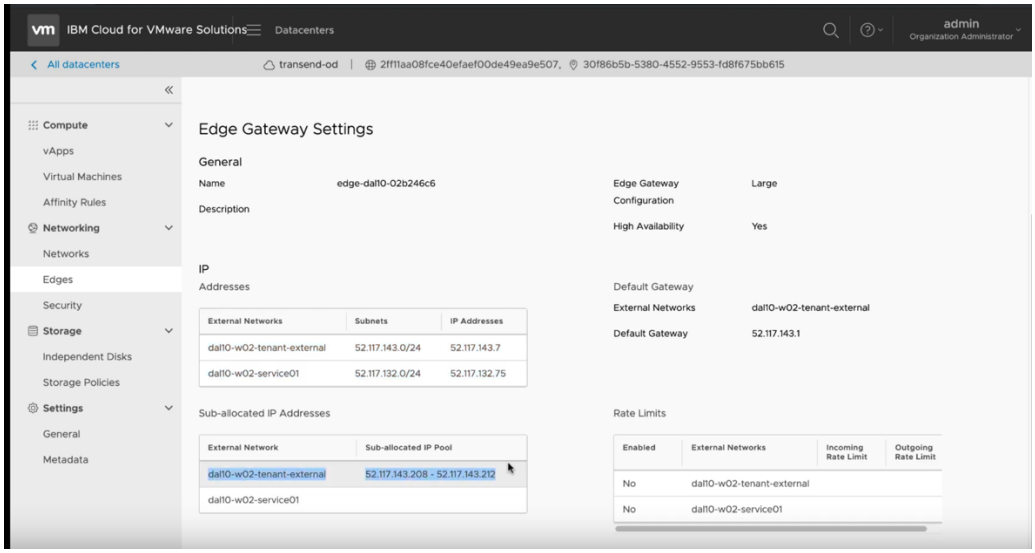




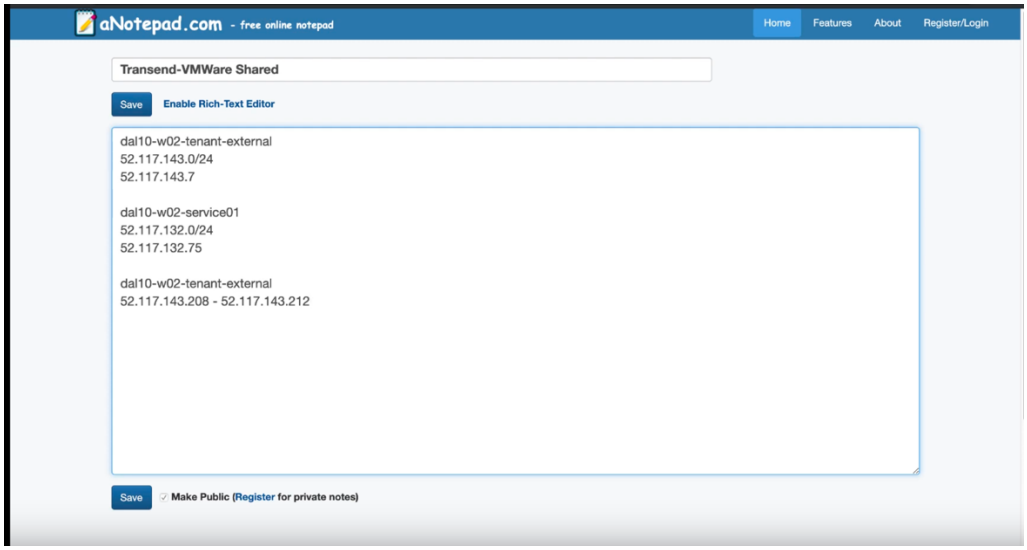


Next, lets capture some IP settings under the Edges tab.
You will need these for the next steps. Save them in a Notepad for future access.

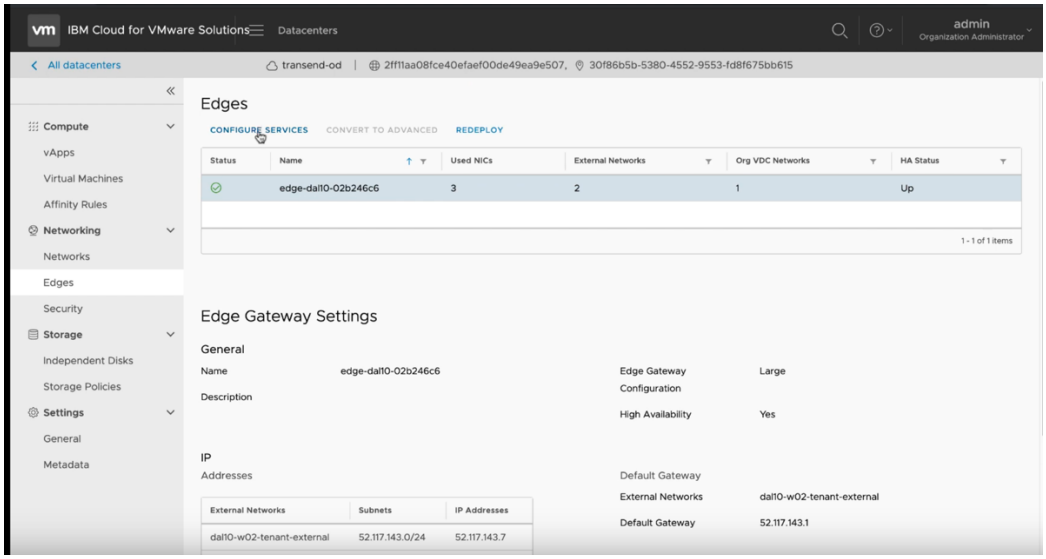




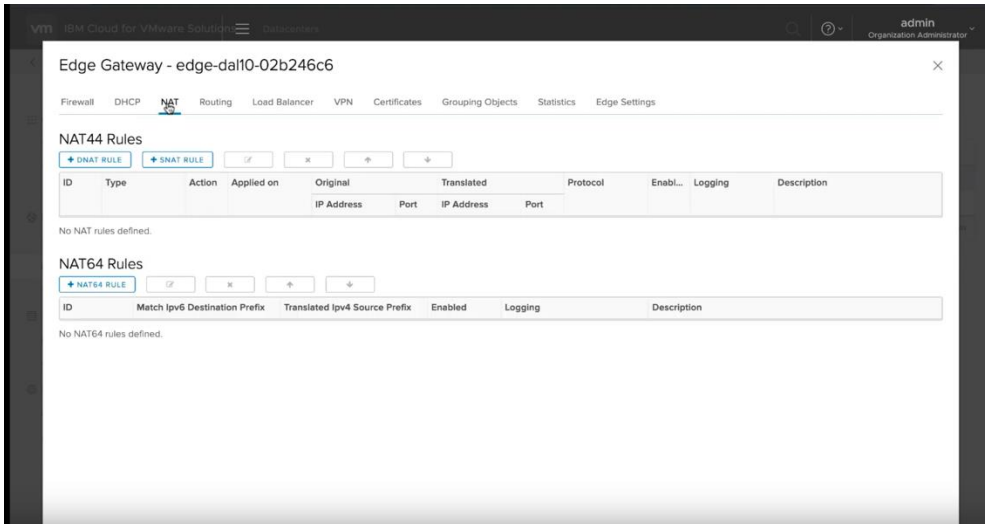
The -external addresses are for external access and the -service01 addresses are for internal access. The last part, sub-allocated IP addresses are 5 IP addresses to be used to assign to your VMs to allow external access. You may request additional IPs if you have more than 5 VMs. You will need to open a ticket with IBM support to get more IPs.



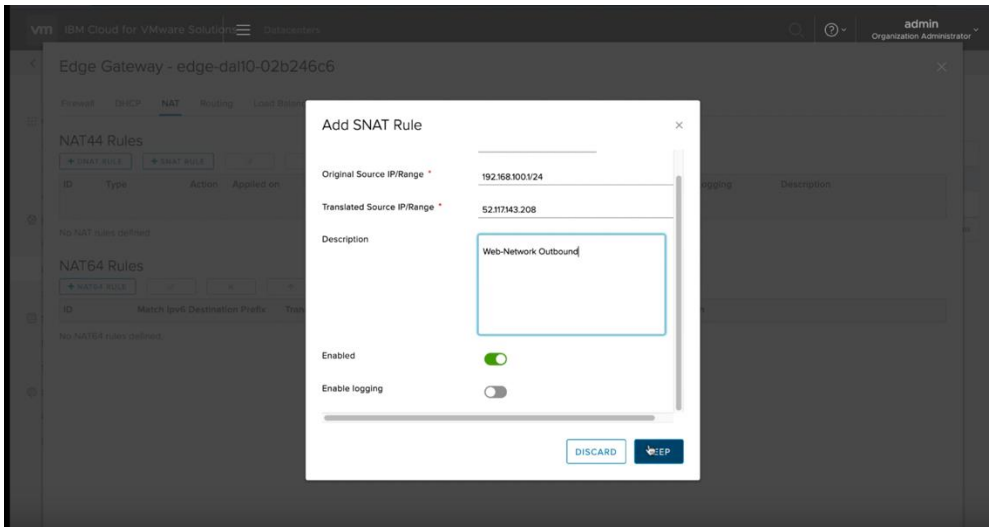
Next go to the Edges menu and press “configure services”.
Now we will configure a Source NAT.



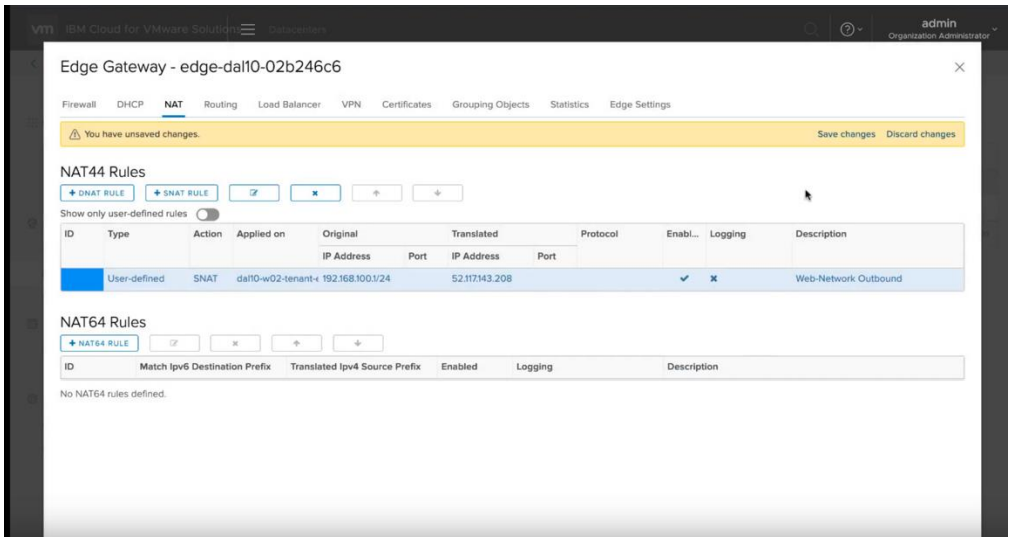
Choose “NAT” from the top menu and let’s create a Source NAT (SNAT)
Press “Add Rule” for the NAT44 Rule SNAT Rule



- *Select the external network option*
- *Enter the CIDR for your network*
- *Select an IP from the list of 5 IPs for external access. We selected the first one 52.117.143.208*
- *Add a description if you wish*



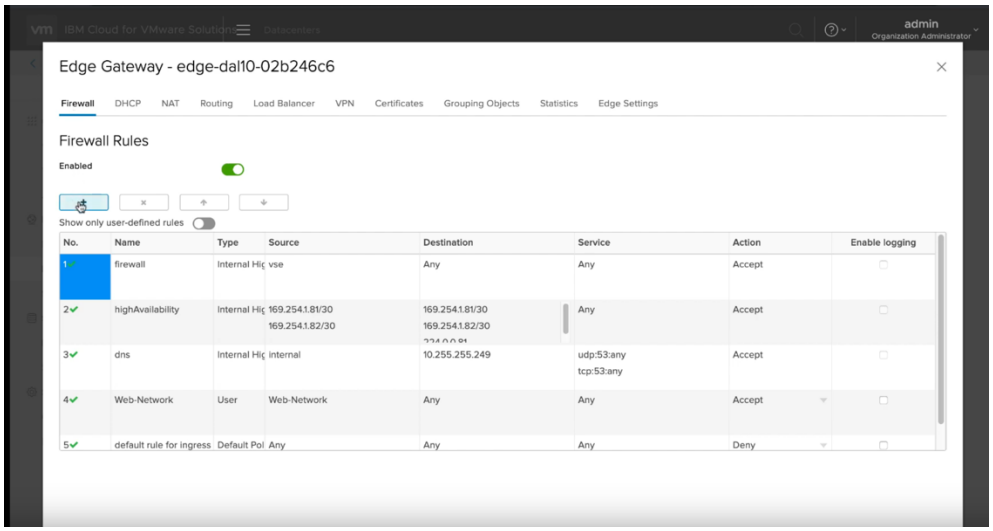
- *Press Next*
- *Press "save changes"*



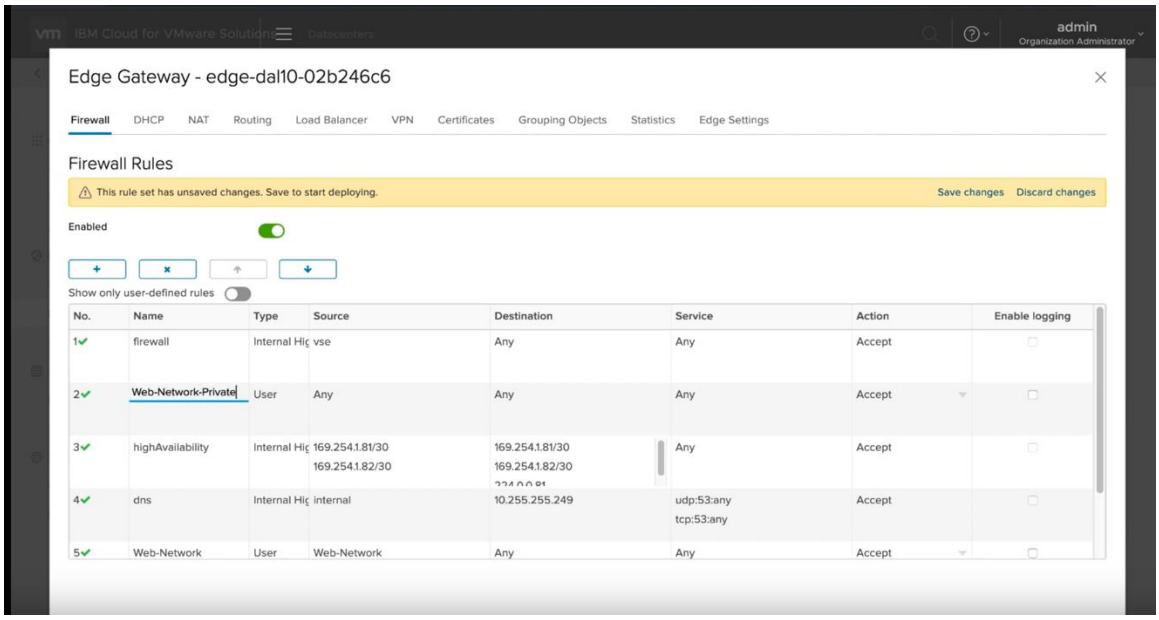
Private Netowrk Access Firewall and Source NAT Configuration

Click on the Edges menu and select the Edge network which was included when you provisioned VMware Shared.

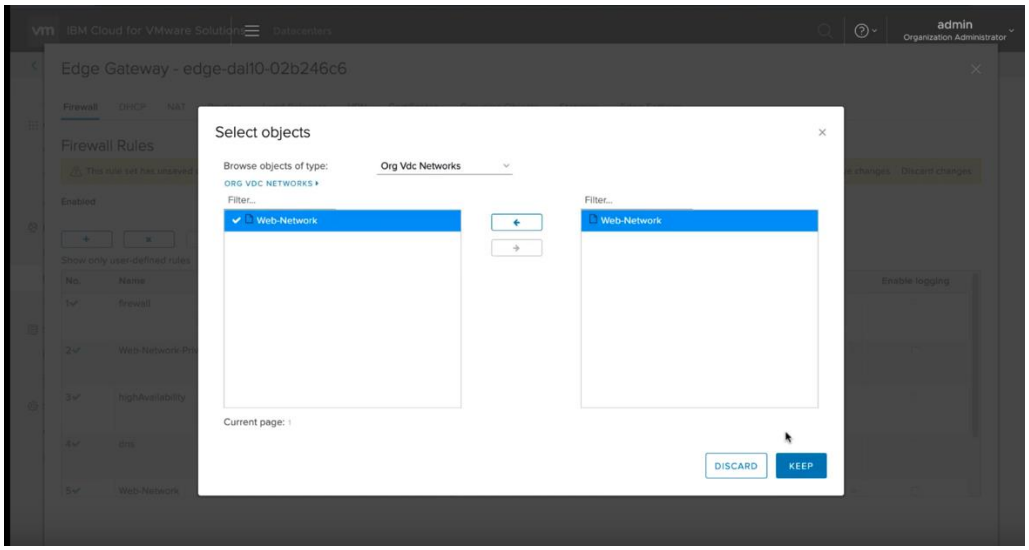
Choose “Firewall” and press the “+”



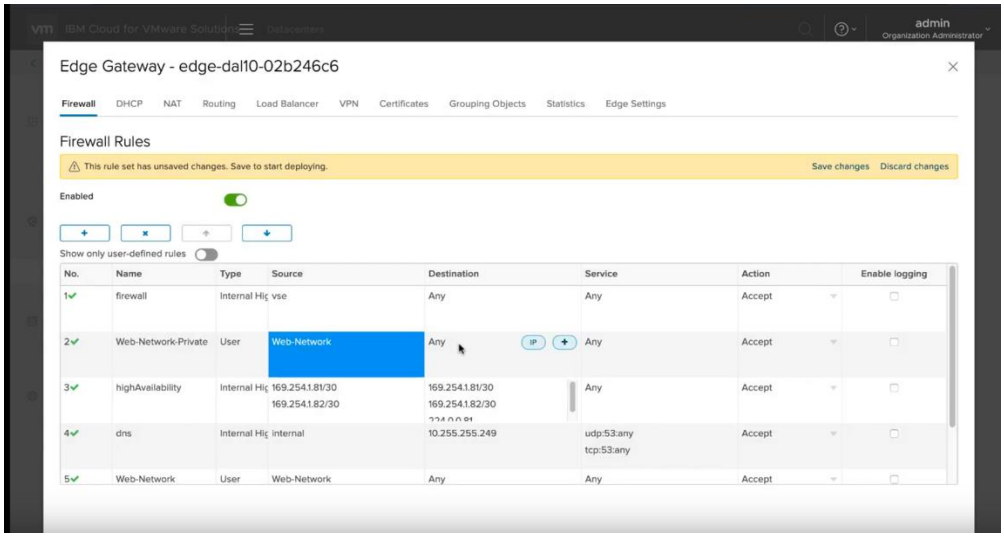
Add a name for the newly created firewall, i.e., web-network-private
Then select the Source and press “+”



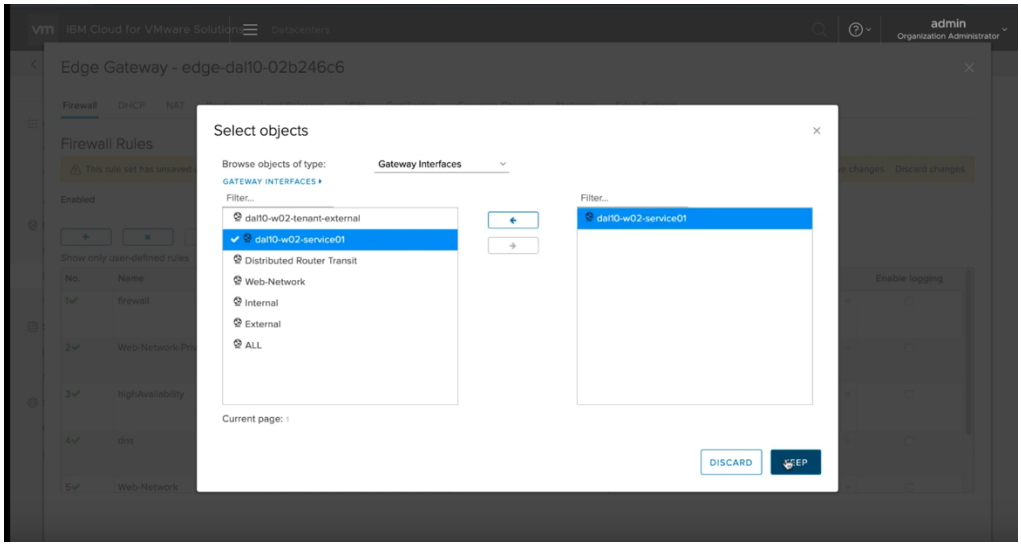
Select the web-network.



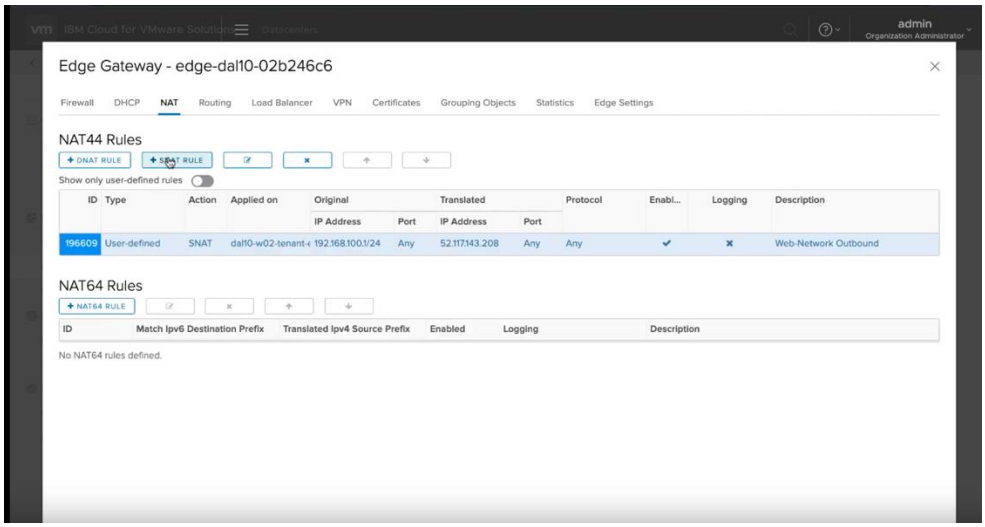
This time we will be targeting the services network in the destination.
Under Destination, press the “+”.



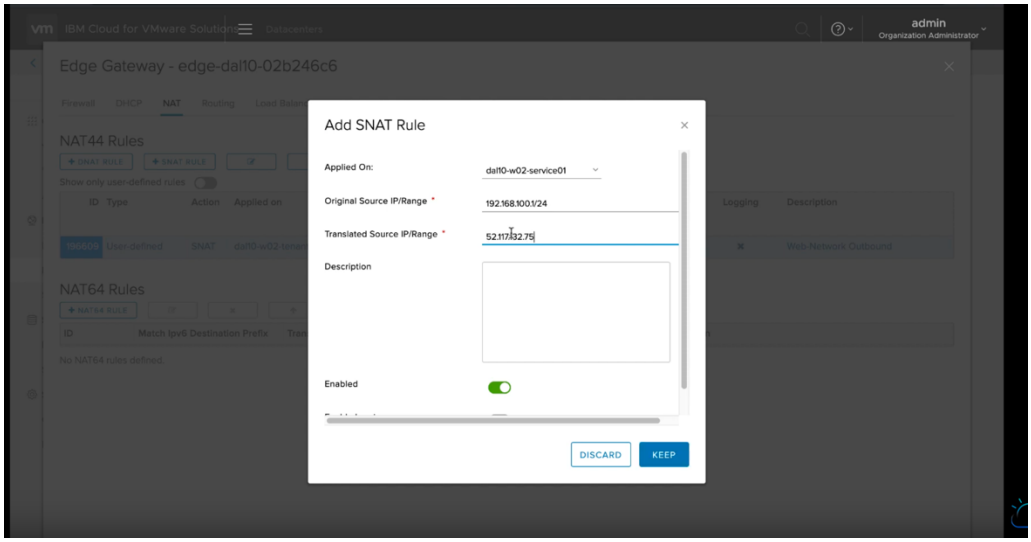
Select the -service01 network and then the “->” to move it the right.
Press Next.

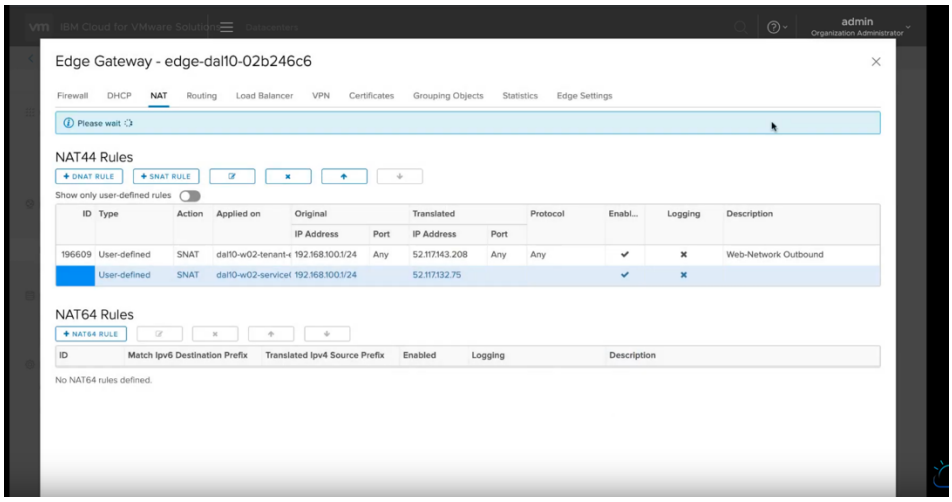


Then press the NAT and select Source NAT.



Select the -service01 network
Add the CIDR for your network
Add an IP from the services IPs, i.e., 52.117.32.75 which you had saved before in notepad.
Press NEXT.





Now you should show two Source NATs, one for external and one for internal network. The internal network will allow you to access IBM Cloud services such as Object Storage Service and Redhat repositories.

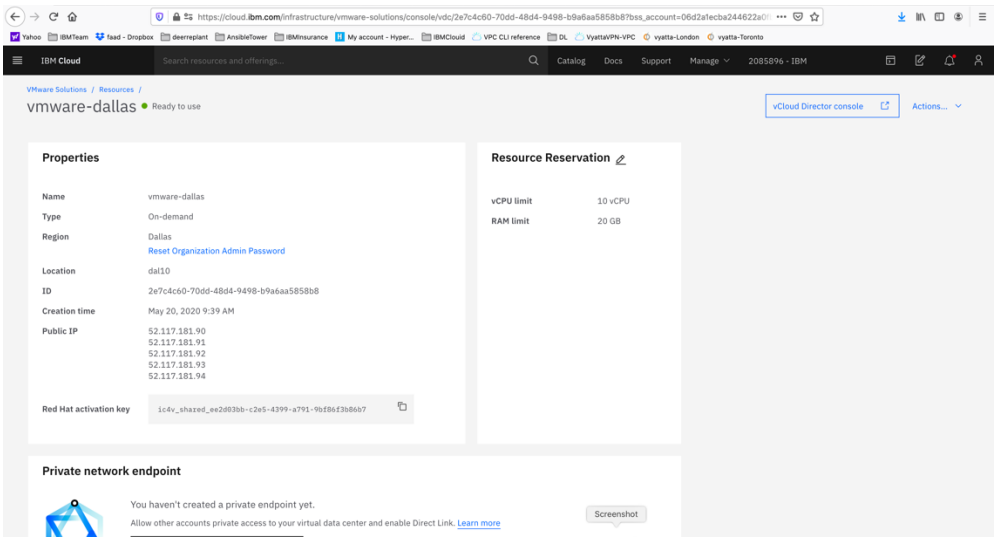
At this point, you can start to provision a VM in your VMware Shared service and be able to access external and internal network.

Provision a VM inside VMware Shared Service

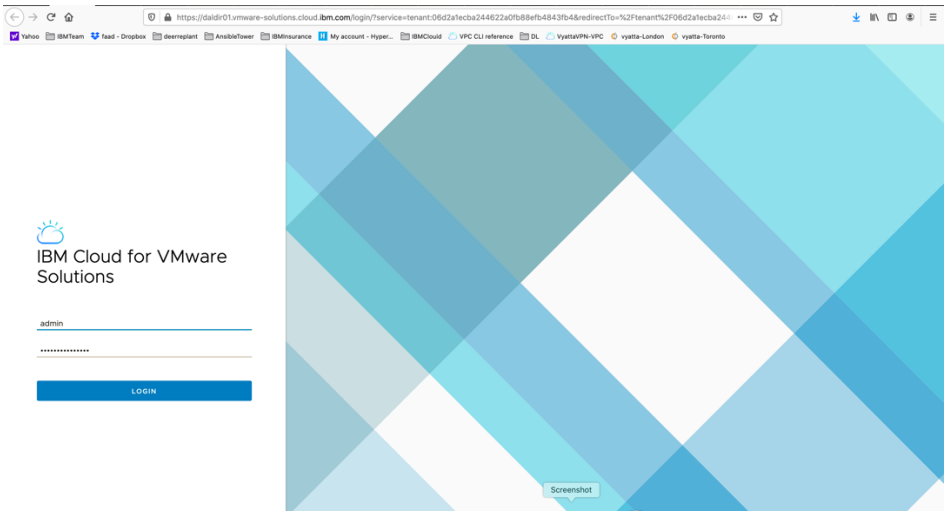
This training video will demo how to provision a VM.

https://www.youtube.com/watch?v=5yl-_60gUUw

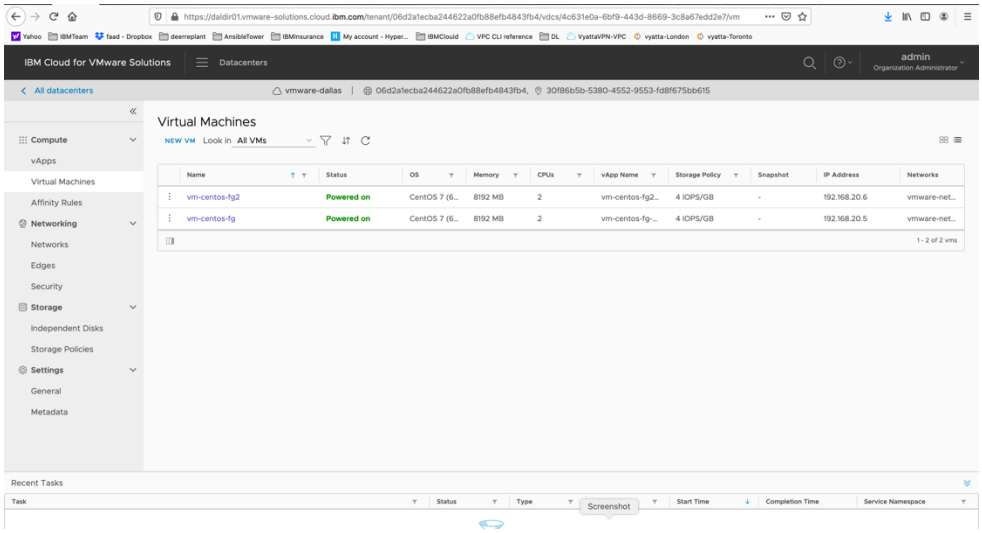
To provision a new VM in your VMware Solution Shared, press on the “vCloud Director Console” on upper right-hand side of your VMware Solution Shared UI in the IBM Cloud.



A browser session will open where you would enter your admin ID and password provided to you when you created the VMware Solution Shared.

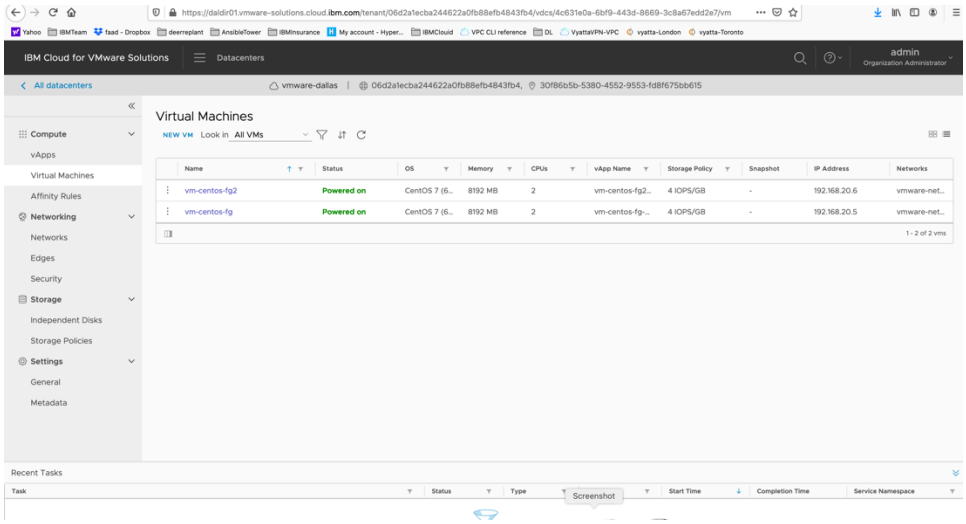


Login to the console using admin and password provided.

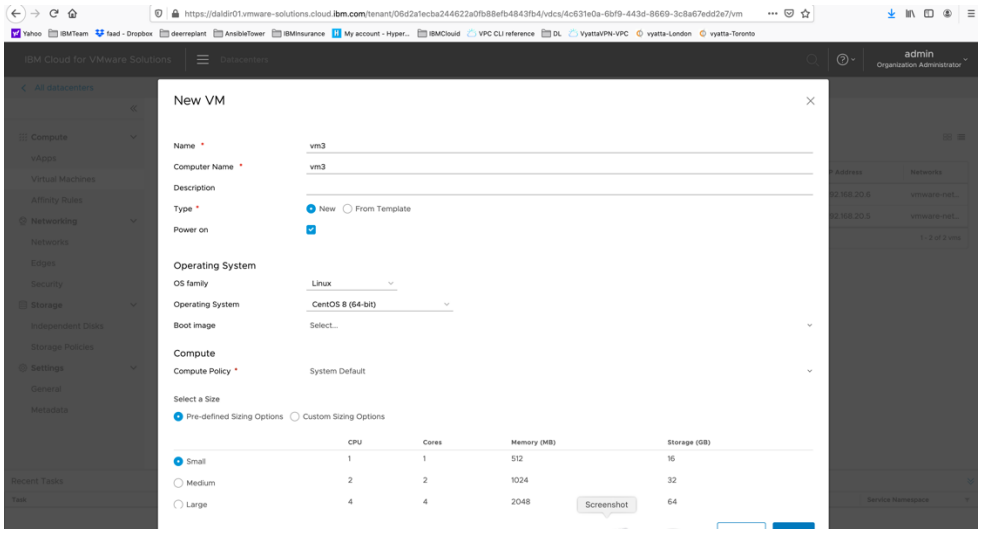


At this point you need to configure you have completed the network configuration. Choose “Virtual Machines”

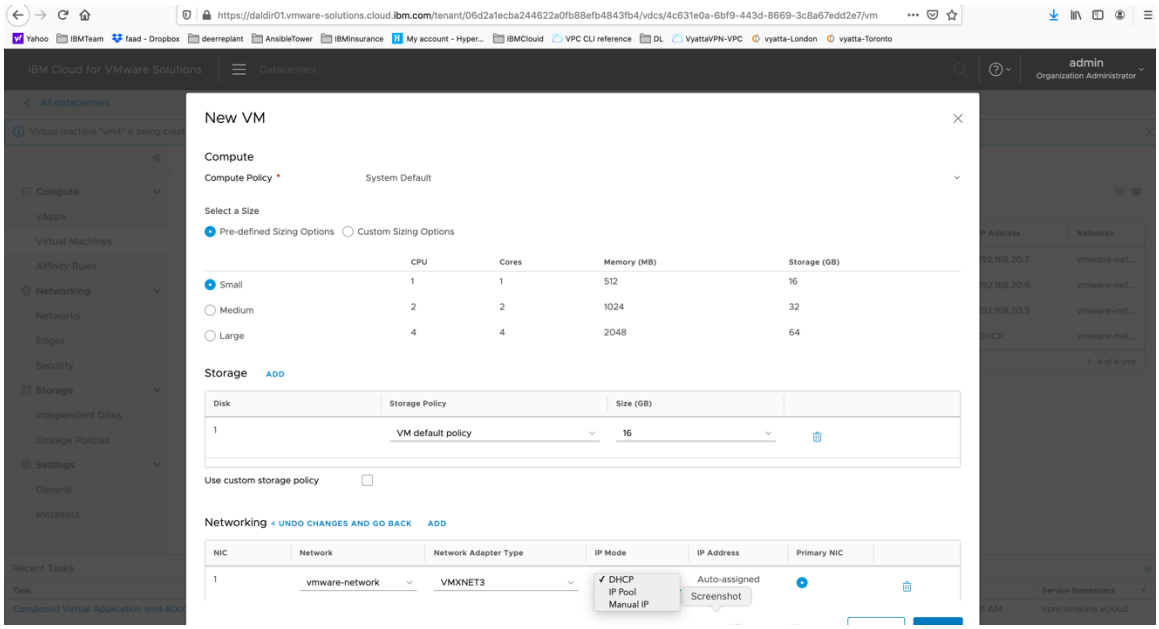
Choose New VM.



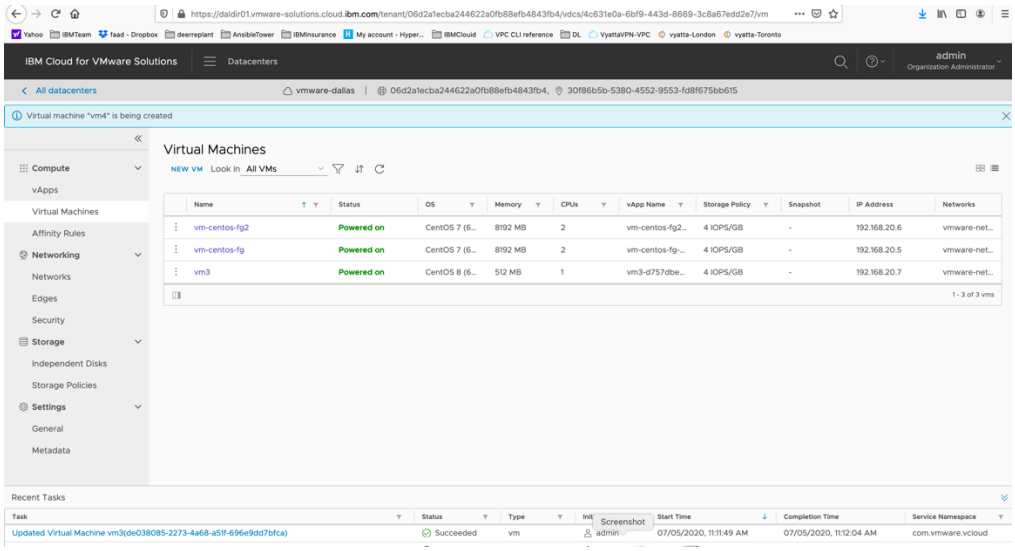
- *Choose a Name which is same as Computer name by default or you can select different names.*
- *Choose “new”*
- *Select the OS Family, Linux in this case*
- *Select Operating system, centos in this case.*
- *Compute Policy select “System Default”*
- *Select a size, we chose small*
- *All other options are kept as default.*



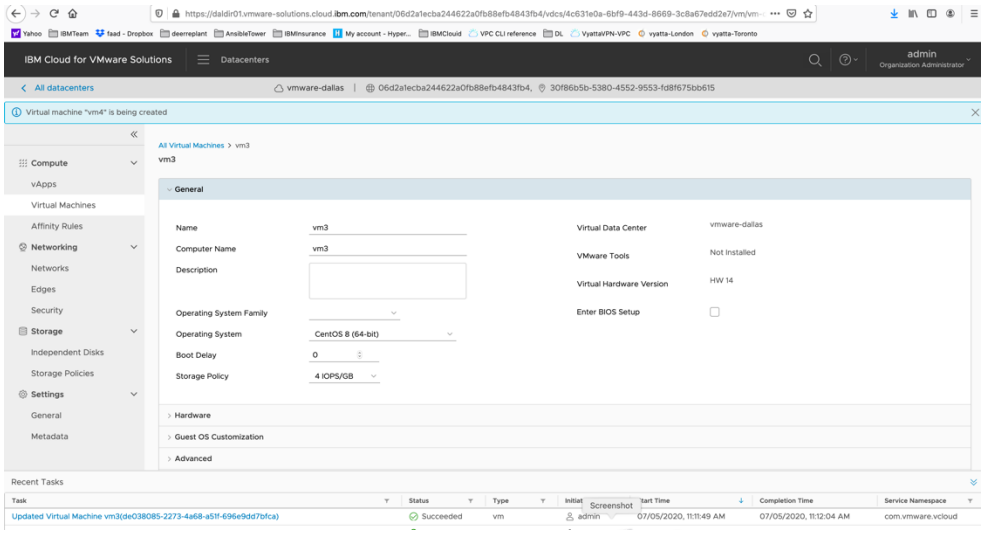
Change the Network from DHCP to IP Pool so the VM will get assigned an IP address from you network.



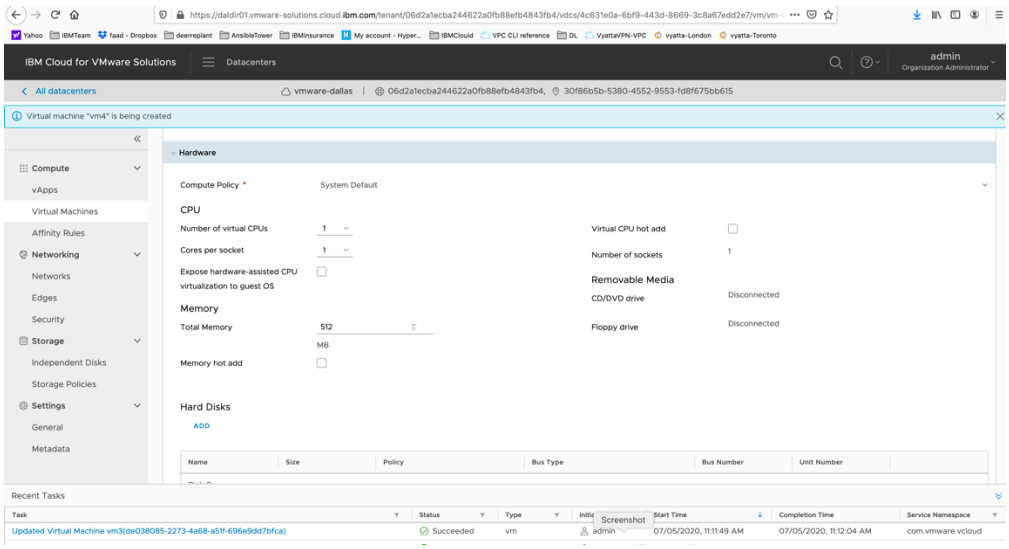
Press OK
Now your VM is being provisioned.



To access the VM, press on the name of the VM you just created.

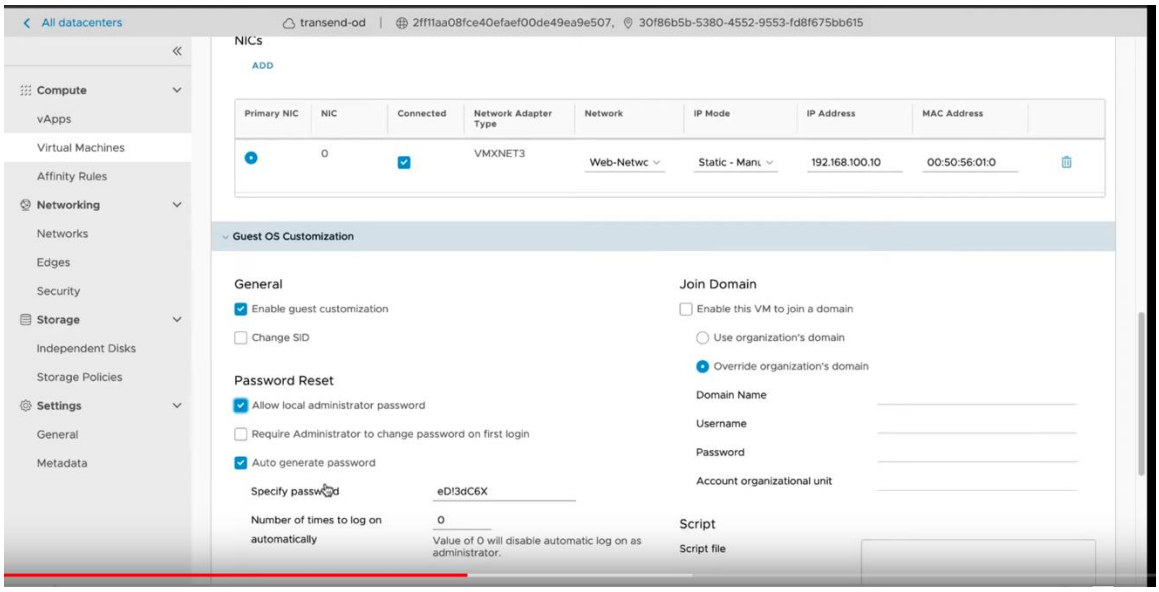


To see more details, expand the Hardware tab.

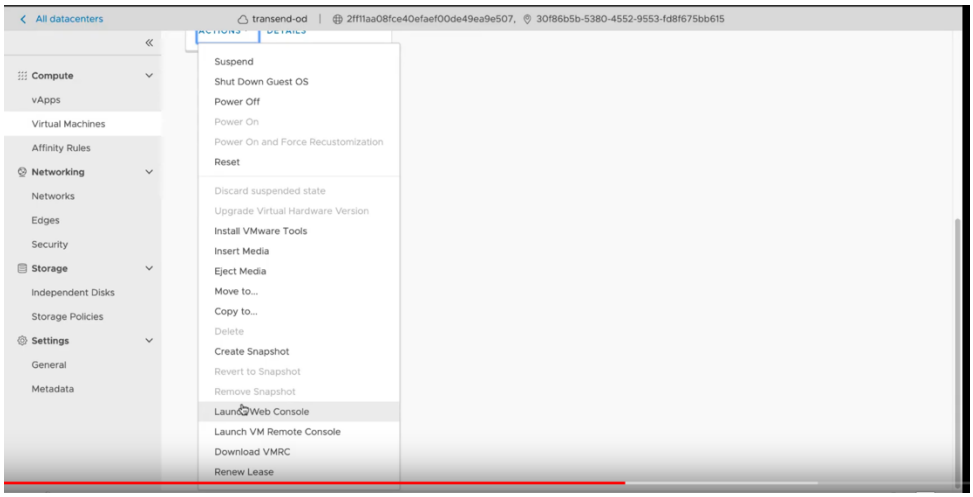


To set a password to access this VM via ssh, expand on the ‘Guess OS customization” and choose:

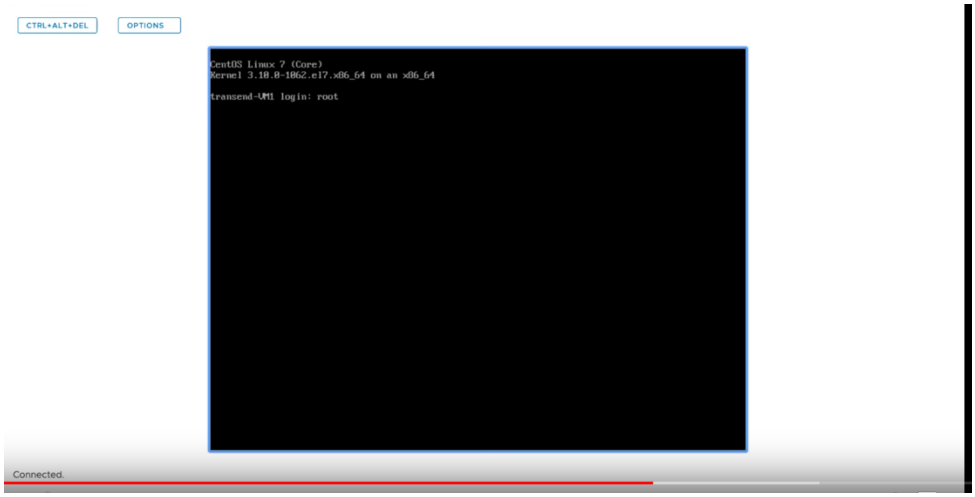
- *Enable Guess Customization*
- *Allow Local Administrator Password*
- *Specify a password or click on Auto Generate Password.*
- *Press Save*
- *Then reboot the VM to get the changes.*
- *Power it on using “Power on and force recustomization” option*



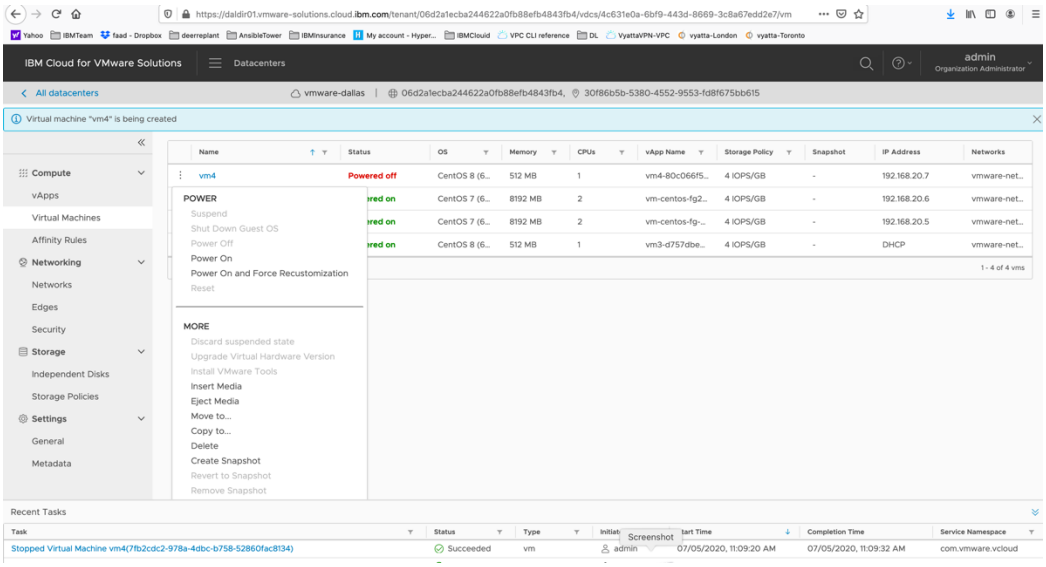
To access the VM, you can use ssh or the provided GUI access via Launch Web Console.



User the root and password you created before to login.



To delete a VM, you will need to power it off first using the list on the vertical "…" icon next to the VM name and then delete it using same menu.

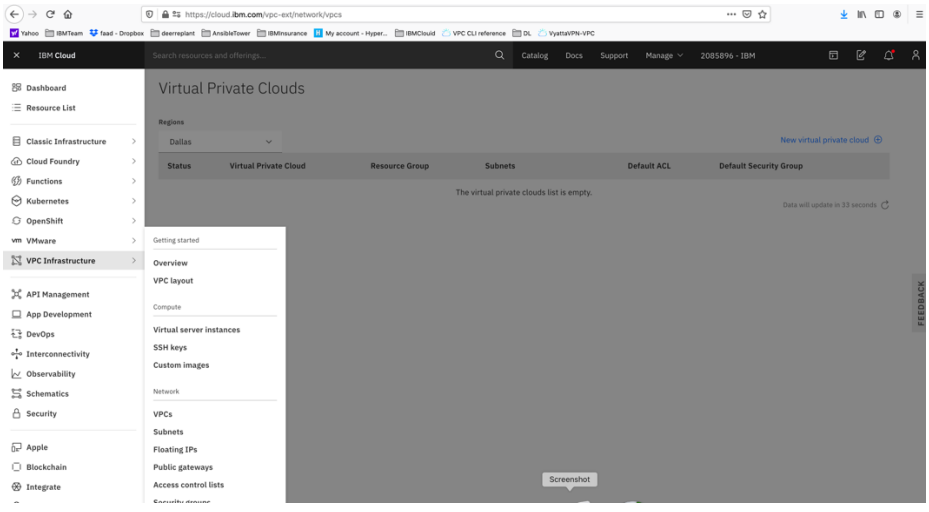


PowerVS and Virtual Private Cloud Integration

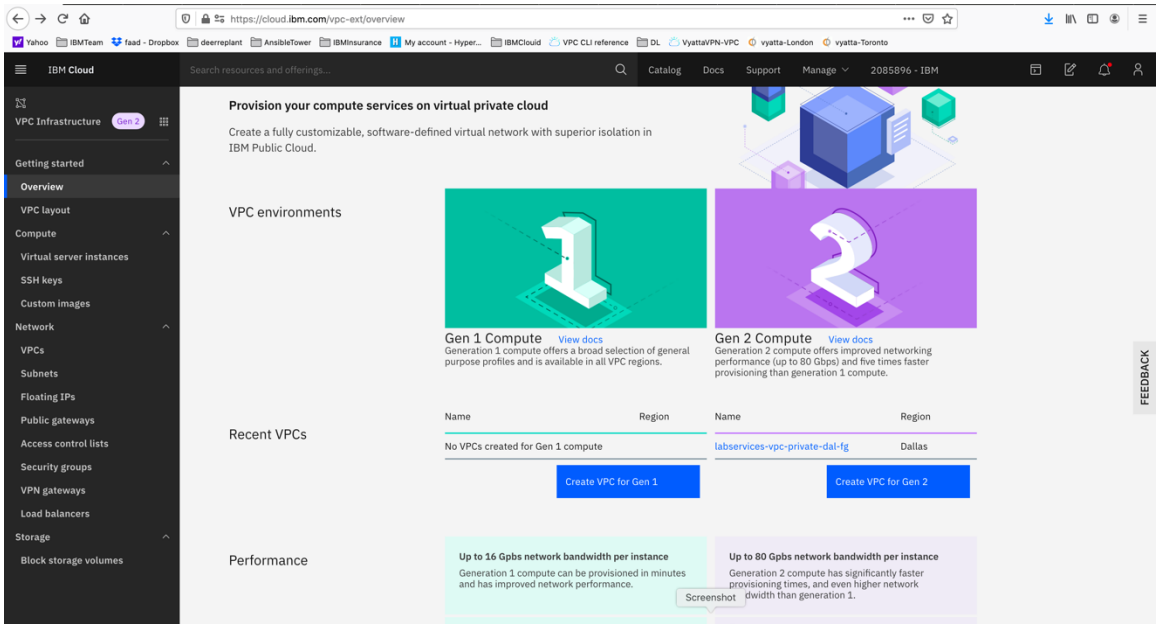
Provision a Gen 2 VPC

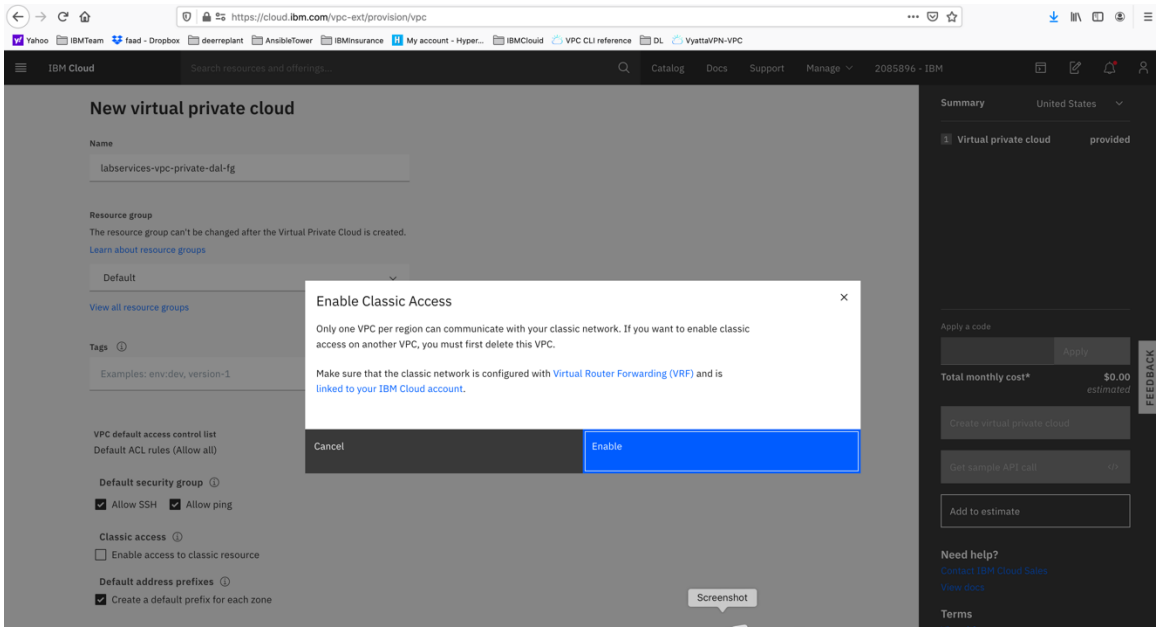
To test the PowerVS connection to a VSI inside a Gen 2 VPC, we first need to create a Gen 2 VPC and then add one or more VPC VSIs to it.

Login to IBM Cloud. On Top left-hand side, click on the triple line icon and choose “VPC Infrastructure” and then “overview”



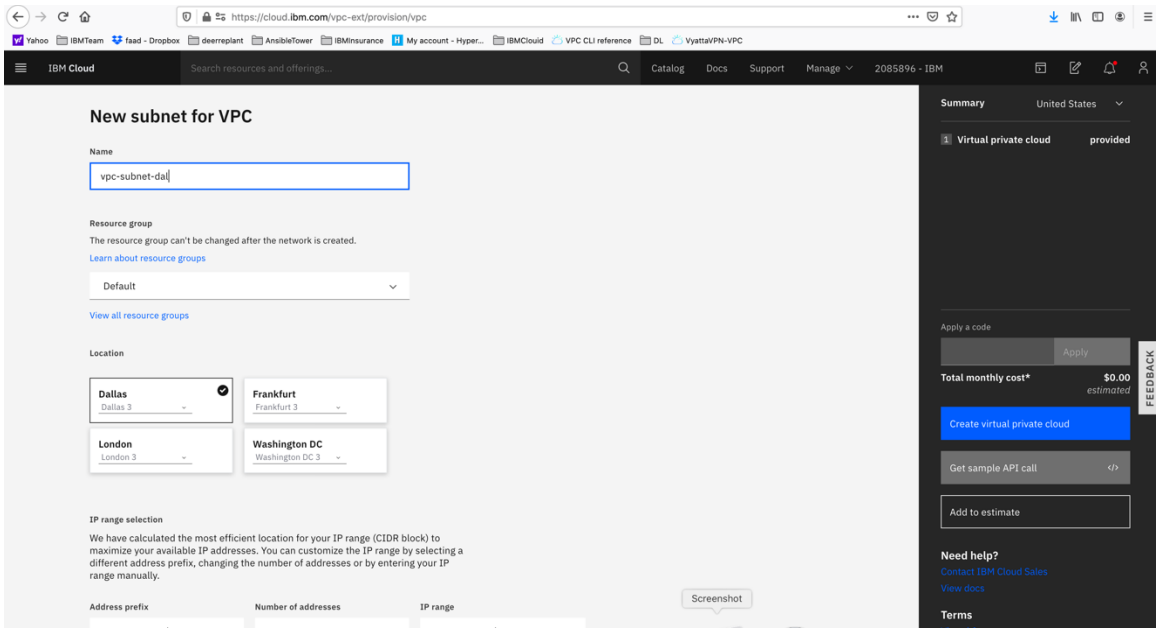
Here you can provision your Gen 2 VPC.
Press “Create VPC Gen 2”

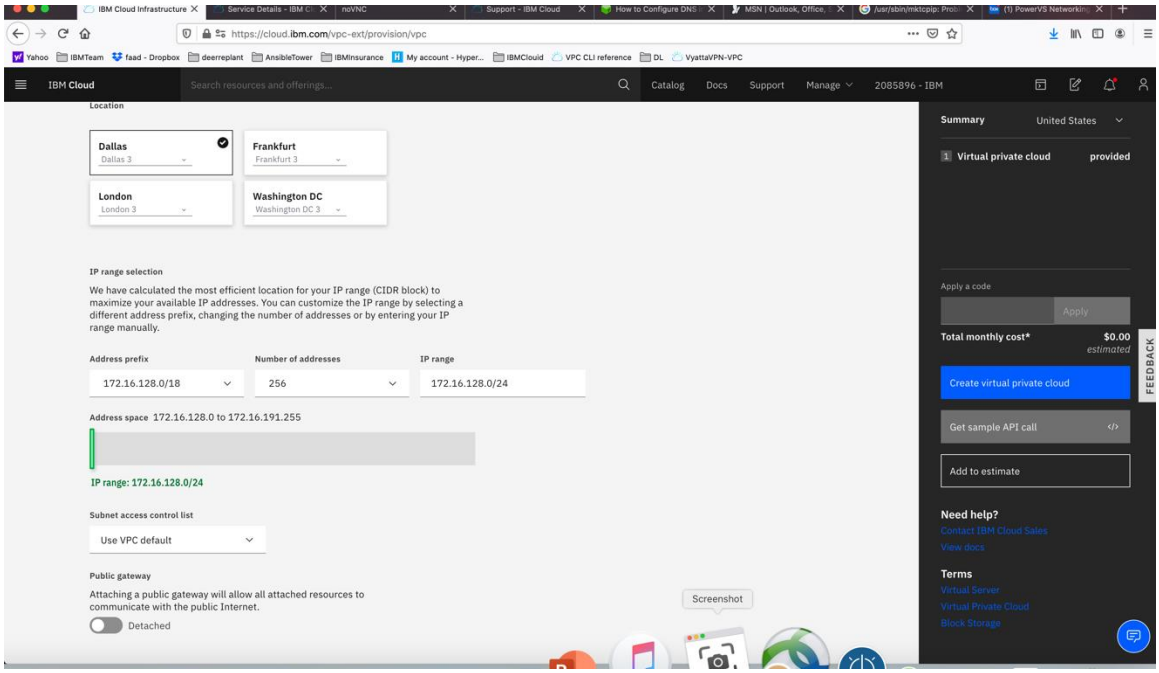




Choose “Enable” to allow your VPC to communicate.

- *Choose a name for your VPC.*
- *Choose the VPC location*
- *Choose a name for your VPC subnet*

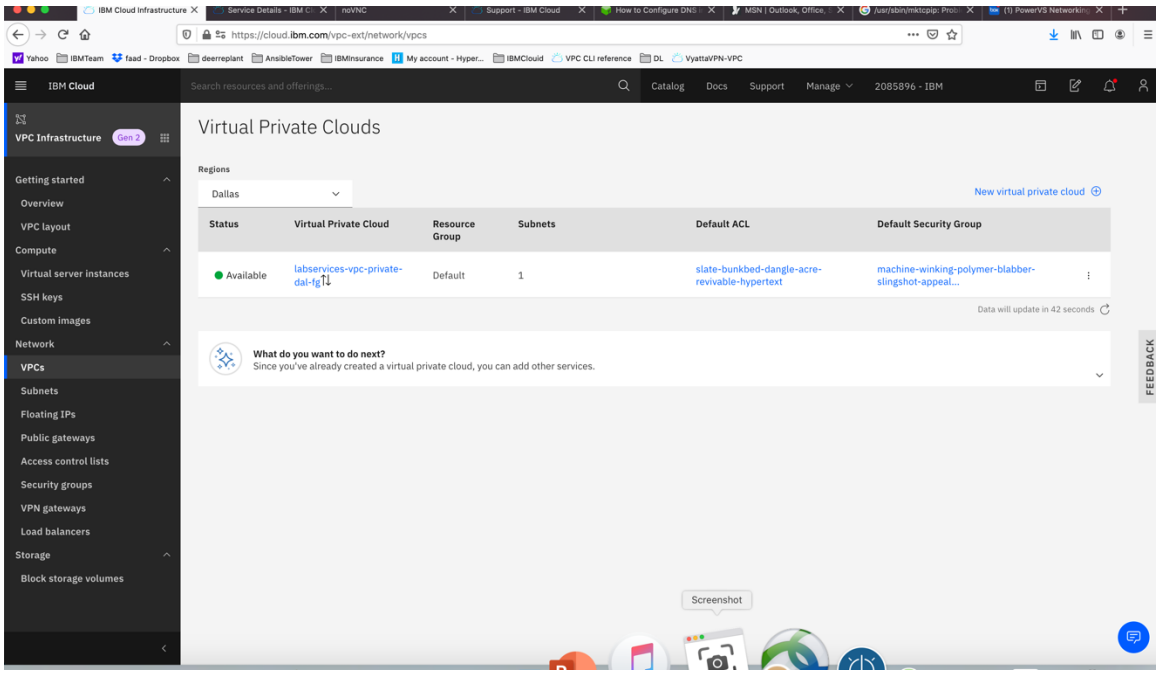




You can keep the IP CIDR it recommends.
At this point, you can choose a Public Gateway to be provisioned to allow access to the internet. We have chosen not to enable Public Gateway and keep the VPC private.

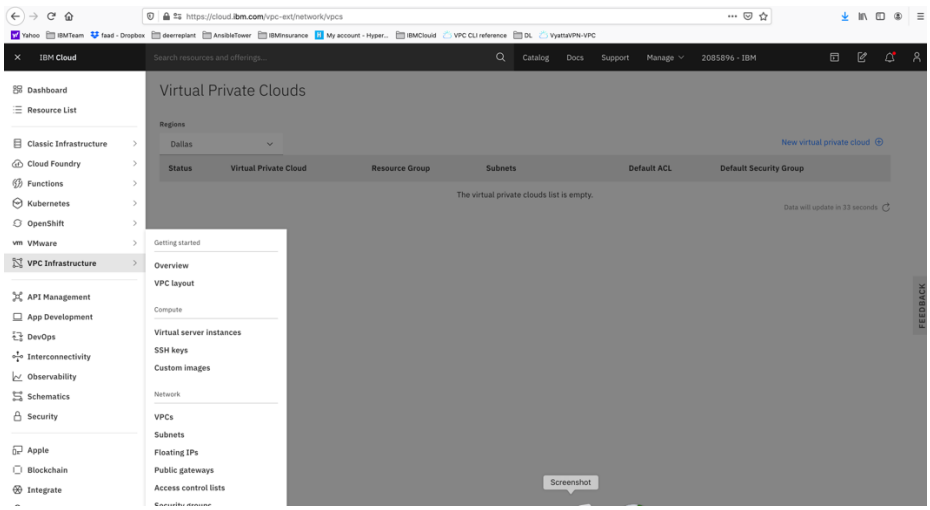
Choose “Create Virtual Private Cloud” on the right-hand side.

Your VPC is now being provisioned.

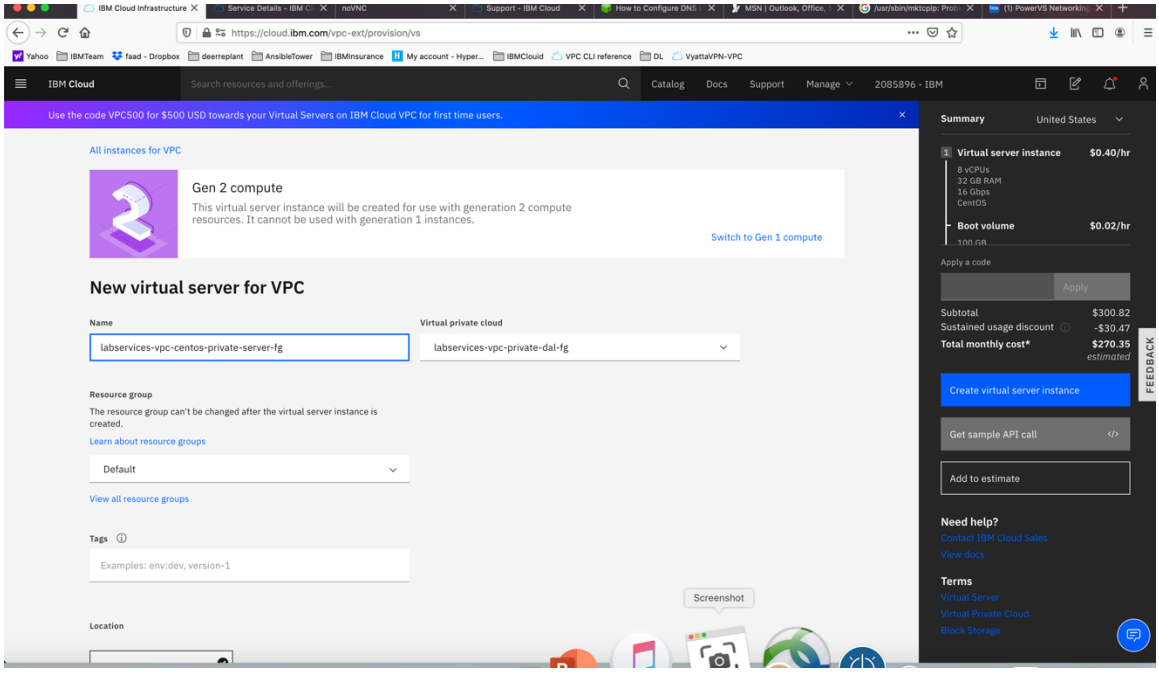


Provision a VPC VSI inside the Gen 2 VPC

Now choose the VPC Gen 2 which you just created.
We will now add some VPC VSI into this VPC.
On Top left-hand side, click on the triple line icon and choose “VPC Infrastructure” and then “virtual server instances”

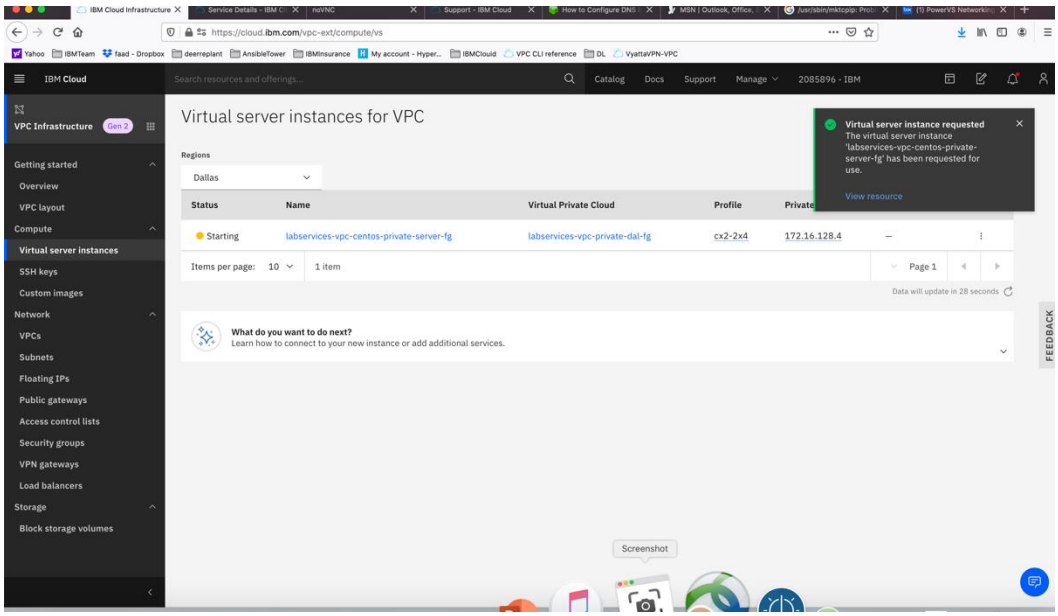


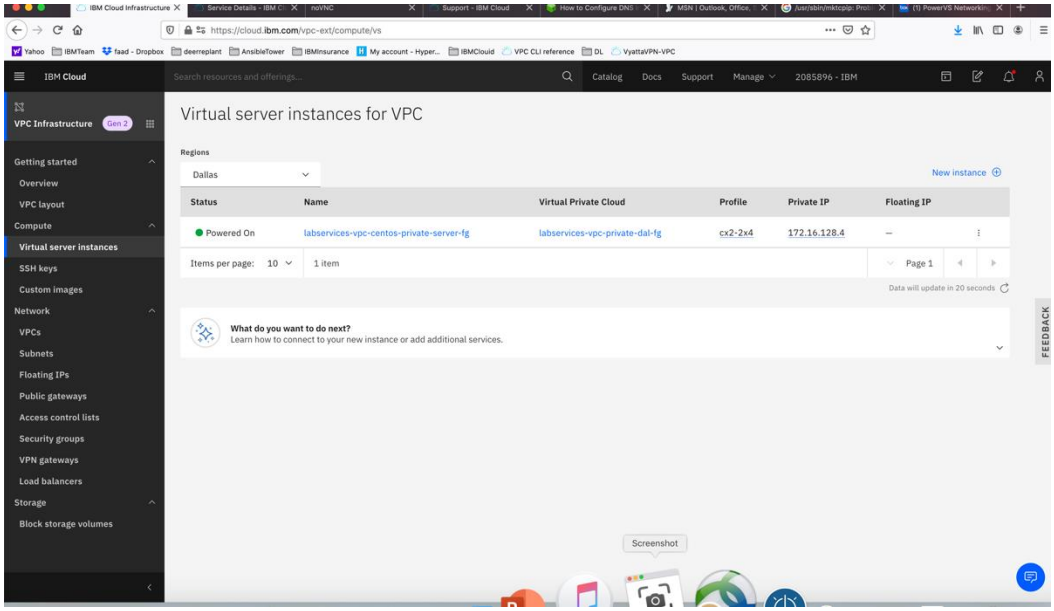
Choose a “new instance”



- *Provide a name for the instance.*
- *Your Virtual private cloud will be automatically chosen.*
- *Check the box under "Classic Access" to "Enable access to classic resources" – this is very critical since all your PowerVSI are under the classic infrastructure and so without this option checked you cannot ping the PowerVSIs.*
- *Select your Operating System and Profile*
- *Your subnet will also be automatically populated.*

Press "Create Virtual Server Instance" on right-hand side.





Your VPC VSI is not active after a few minutes.

Now you can ping the VPC VSI from the Power VSI and vis versa using private IPs.

End of tutorial