IBM Cloud 用戶實作研習營

IBM Cloud Virtual Private Cloud (VPC) 使用教學

2019/8/7

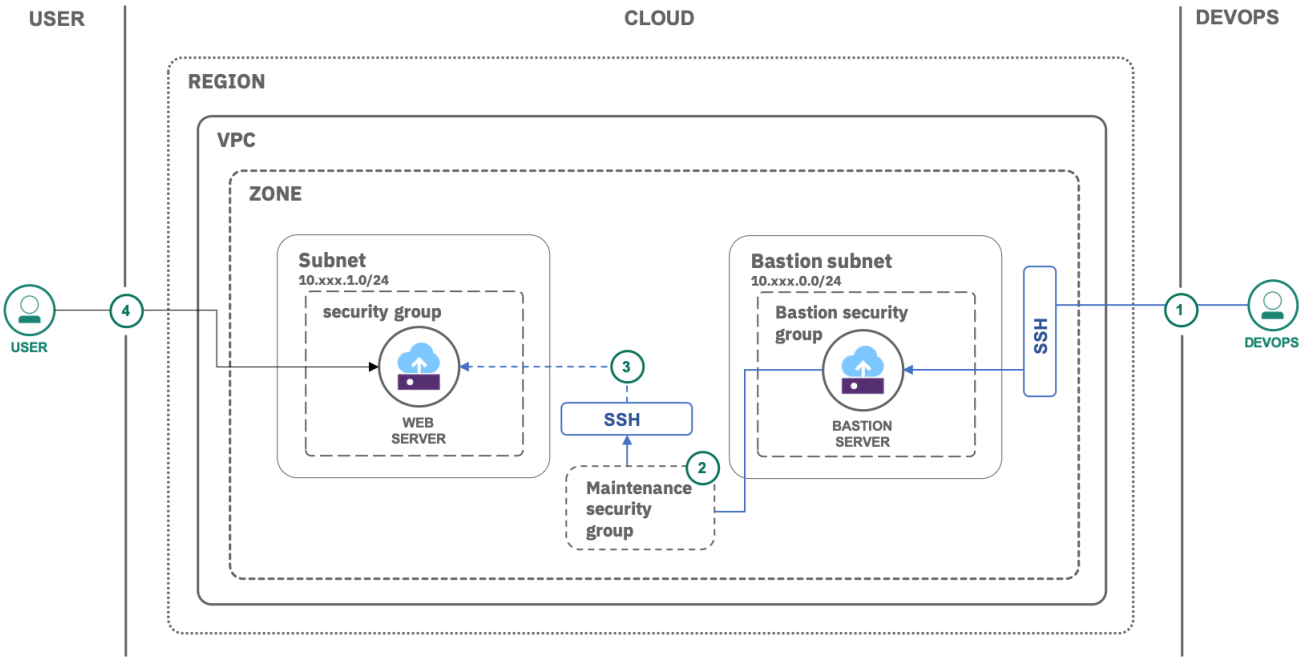
Securely access remote instances with a bastion host

- This tutorial walks you through the deployment of a bastion host to securely access remote instances within a virtual private cloud. Bastion host is an instance that is provisioned in a public subnet and can be accessed via SSH. Once set up, the bastion host acts as a **jump** server allowing secure connection to instances provisioned in a private subnet.
- To reduce exposure of servers within the VPC you will create and use a bastion host. Administrative tasks on the individual servers are going to be performed using SSH, proxied through the bastion. Access to the servers and regular internet access from the servers, e.g., for software installation, will only be allowed with a special maintenance security group attached to those servers

Objectives

- Learn how to set up a bastion host and security groups with rules
- Securely manage servers via the bastion host

Architecture



- After setting up the required infrastructure (subnets, security groups with rules, VSIs) on the cloud, the admin (DevOps) connects (SSH) to the bastion host using the private SSH key.
- The admin assigns a maintenance security group with proper outbound rules.
- The admin connects (SSH) securely to the instance's private IP address via the bastion host to install or update any required software e.g., a web server
- The internet user makes an HTTP/HTTPS request to the web server.

Create a Virtual Private Cloud

In this section, you will create your own IBM Cloud account, and then get access to a IBM Cloud Lab account which contains pre-provisioned clusters. Each lab attendee will be granted access to one cluster.

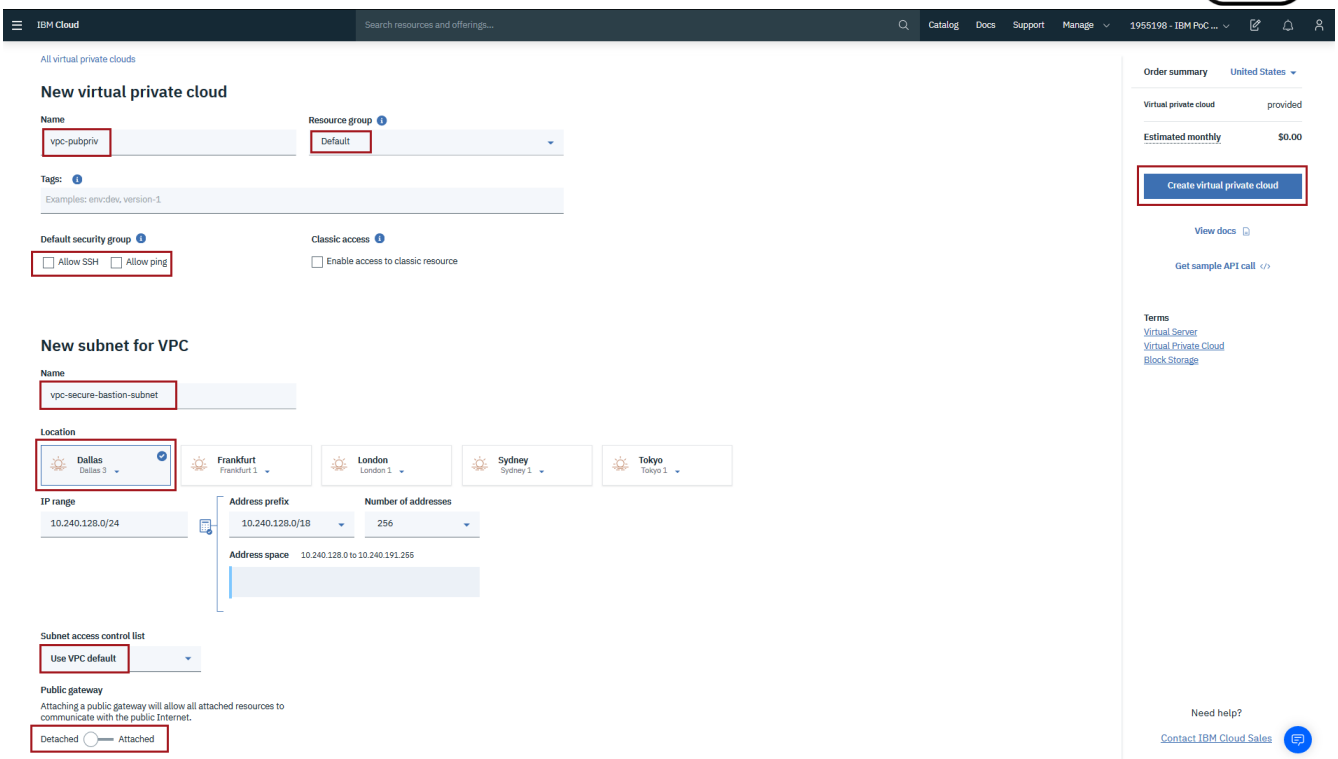
Login to IBM Cloud

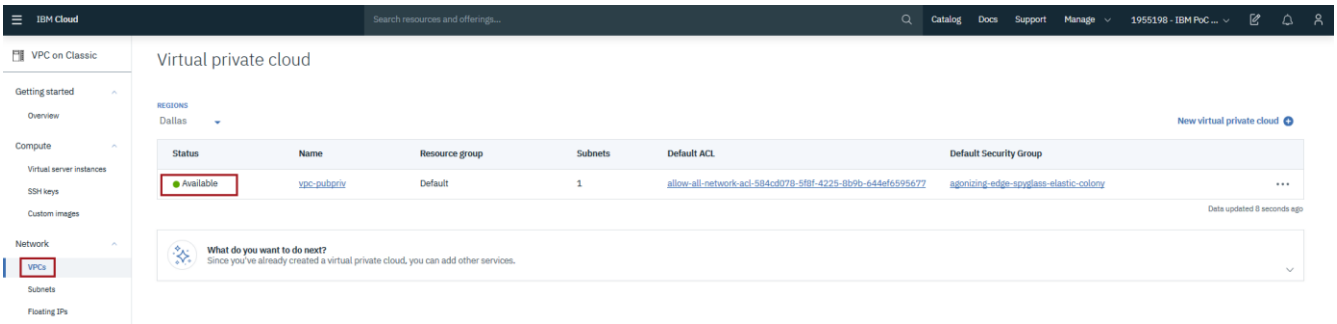
1. Create your own IBM Cloud account. Ex: wk1201908000@dayrep.com
2. After the email verification, confirm by logging in to https://cloud.ibm.com

Create a Virtual Private Cloud

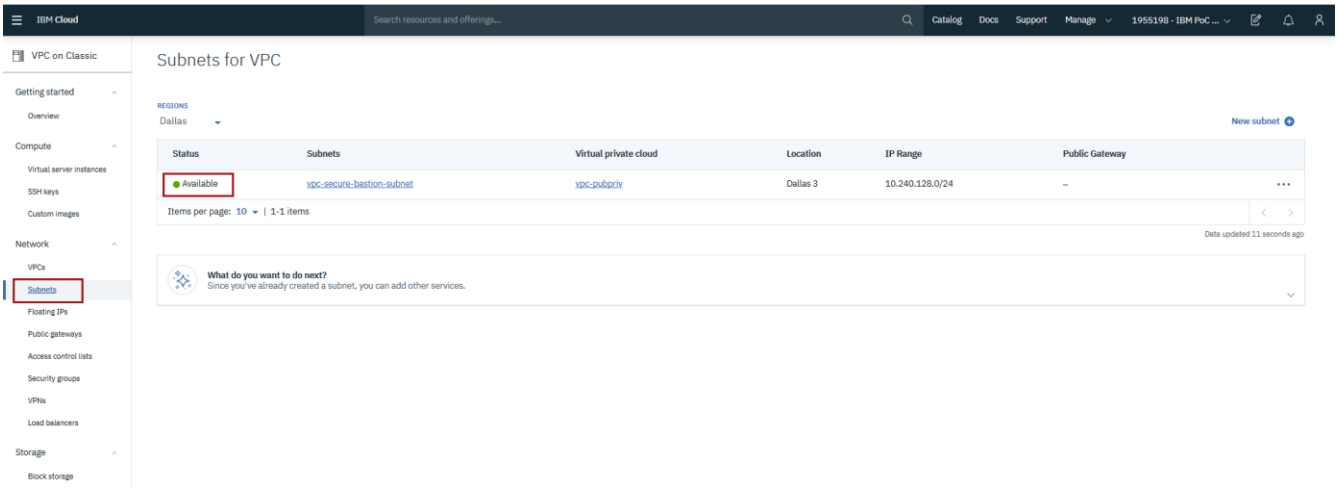
In this section, you will create the VPC and the bastion host.

1. Navigate to the VPC overview page and click on **Create a VPC**.
2. Under **New virtual private cloud** section:
   - Enter **wk1000vpc-pubpriv** as name for your VPC.
   - Select a **Resource group**.
   - Optionally, add **Tags** to organize your resources.
3. Select **Create new default (Allow all)** as your VPC default access control list (ACL).
4. Uncheck SSH and ping from the **Default security group**.
5. Under **New subnet for VPC**:
   - As a unique name enter **wk1000vpc-secure-bastion-subnet**.
   - Select a location.
   - Enter the IP range for the subnet in CIDR notation, i.e., **10.xxx.0.0/24**. Leave the **Address prefix** as it is and select the **Number of addresses** as 256.
6. Select **Use VPC default** for your subnet access control list (ACL).
7. Leave the **Public gateway** to **Detached**. Enabling the public gateway would enable public Internet access to all virtual server instances in the VPC. In this tutorial, the servers do not require such connectivity.
8. Click **Create virtual private cloud**.





To confirm the creation of the subnet, go to the **Subnets** page and wait until the status changes to **Available**.



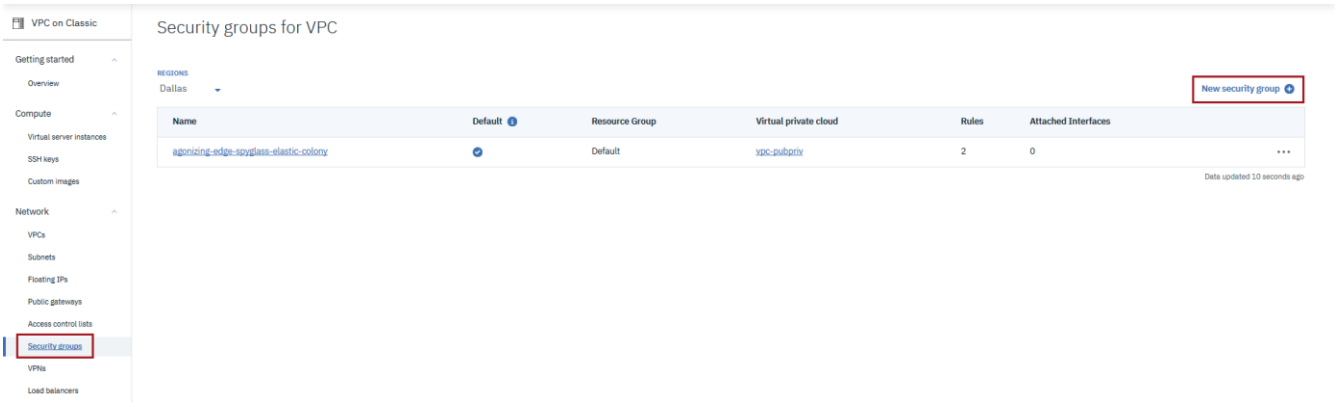
Create and configure bastion security group

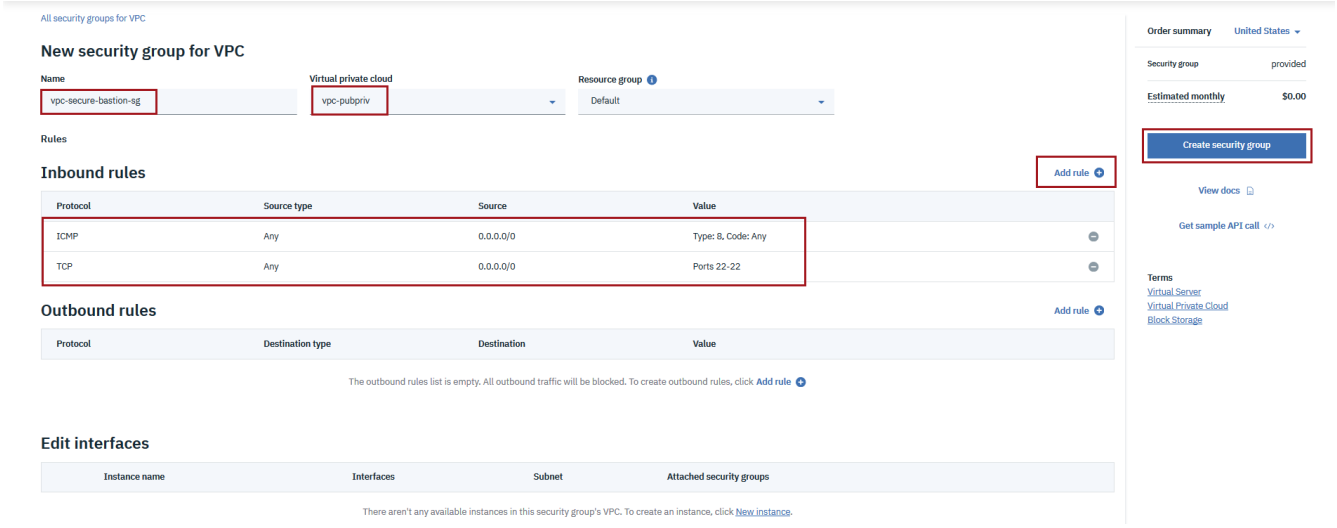
Let's create a security group and configure inbound rules to your bastion VSI.

1. Navigate to **Security groups** and click **New security group**. Enter **wk1000vpc-secure-bastion-sg** as name and select your VPC.
2. Now, create the following inbound rules by clicking **Add rule** in the inbound section. They allow SSH access and Ping (ICMP). **Inbound rule:**

Protocol	Source type	Source	Value
TCP	Any	0.0.0.0/0	Ports 22-22
ICMP	Any	0.0.0.0/0	Type: **8**,Code: **Leave empty**

3. Click **Create security group** to create it.



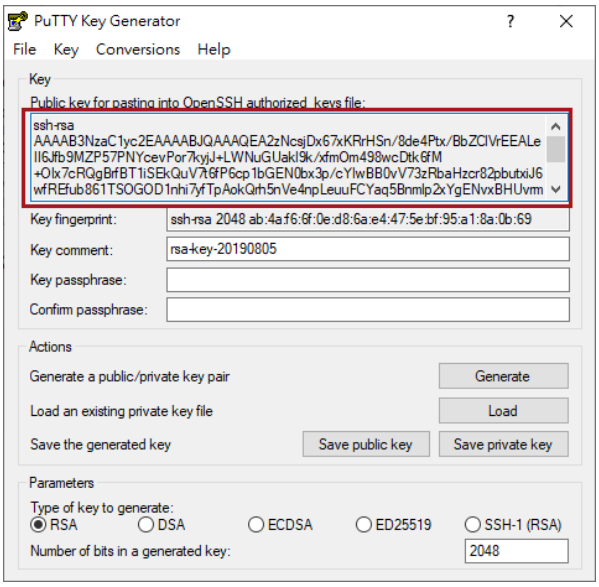


Create a bastion instance

With the subnet and security group already in place, next, create the bastion virtual server instance.

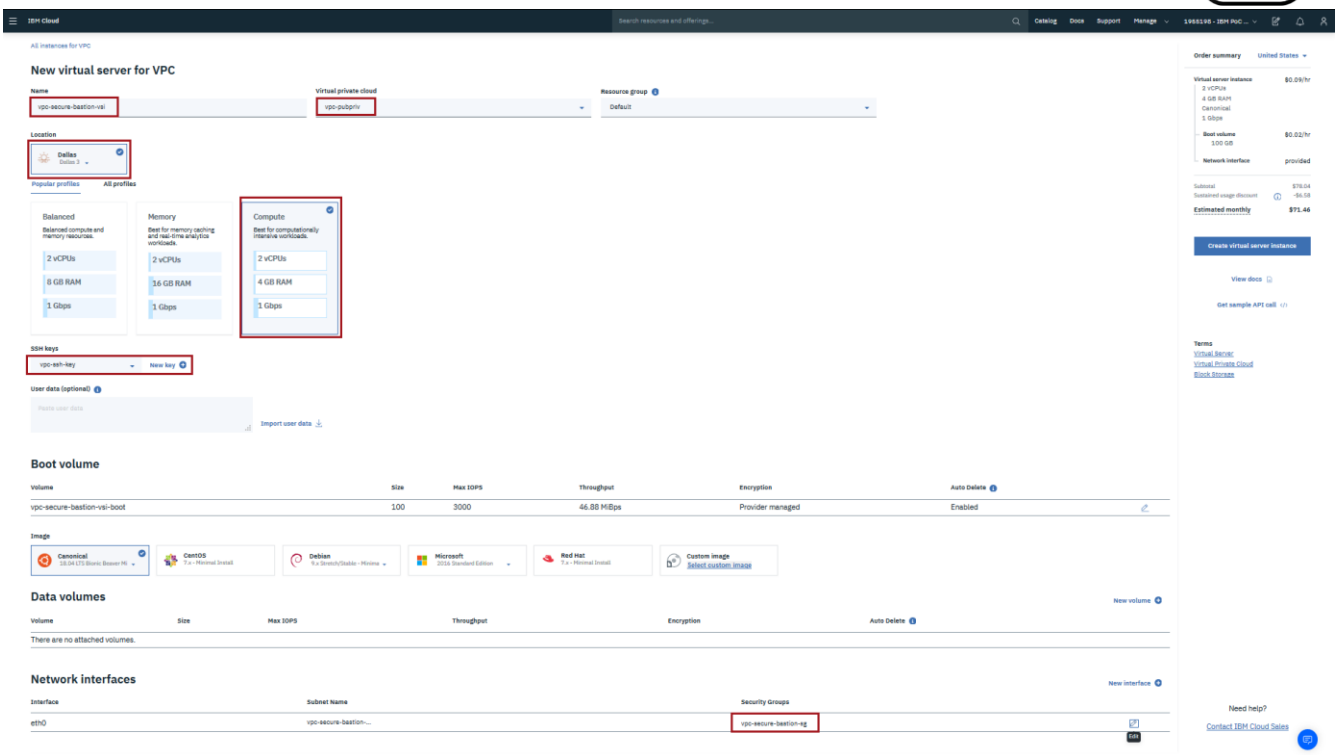
1. Under **Subnets** on the left pane, select **wk1000vpc-secure-bastion-subnet**.

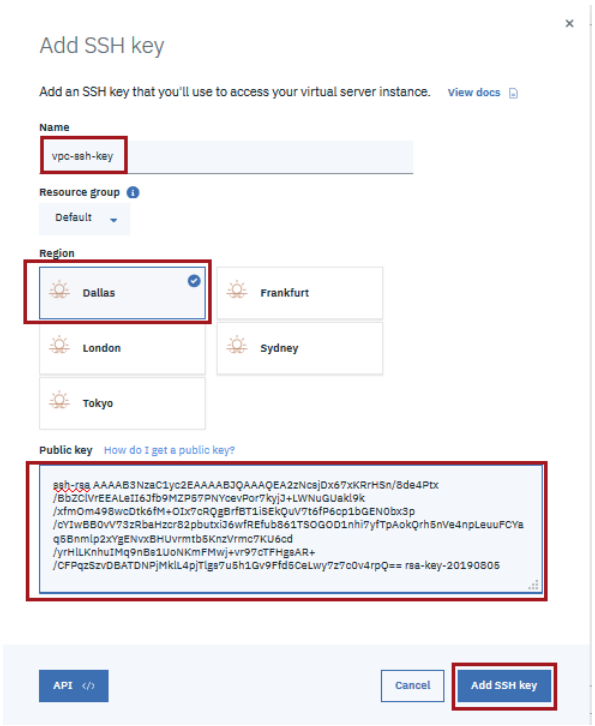
2. Click on **Attached resources** and provision a **New instance** called **wk1000vpc-secure-bastion-vsi** under your own VPC and resource group.
3. Select a **Location** and make sure to later use the same location again.
4. Select **Compute** (2 vCPUs and 4 GB RAM) as your profile.
5. Use Putty Key Generator to create public key and private key, then copy public key content for VSI provision.

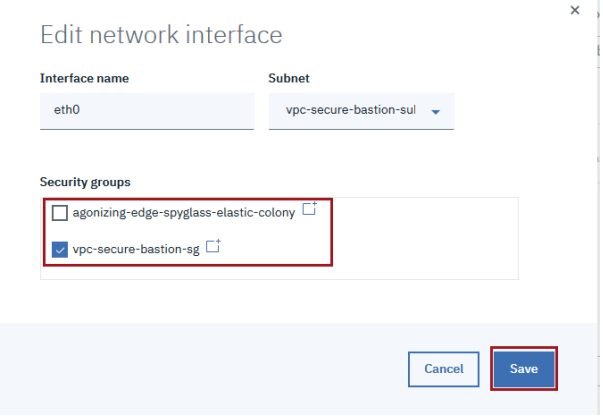


6. To create a new **SSH key**, click **New key**
   - Enter **wk1000vpc-ssh-key** as key name.
   - Leave the **Region** as is.
   - Copy the contents of your existing local SSH key and paste it under **Public key**.
   - Click **Add SSH key**.
7. Select **Ubuntu Linux** as your image. You can pick any version of the image.
8. Under **Network interfaces**, click on the **Edit** icon next to the Security Groups
   - Make sure that **wk1000vpc-secure-bastion-subnet** is selected as the subnet.
   - Uncheck the default security group and mark **wk1000vpc-secure-bastion-sg**.
   - Click **Save**.
9. Click **Create virtual server instance**.

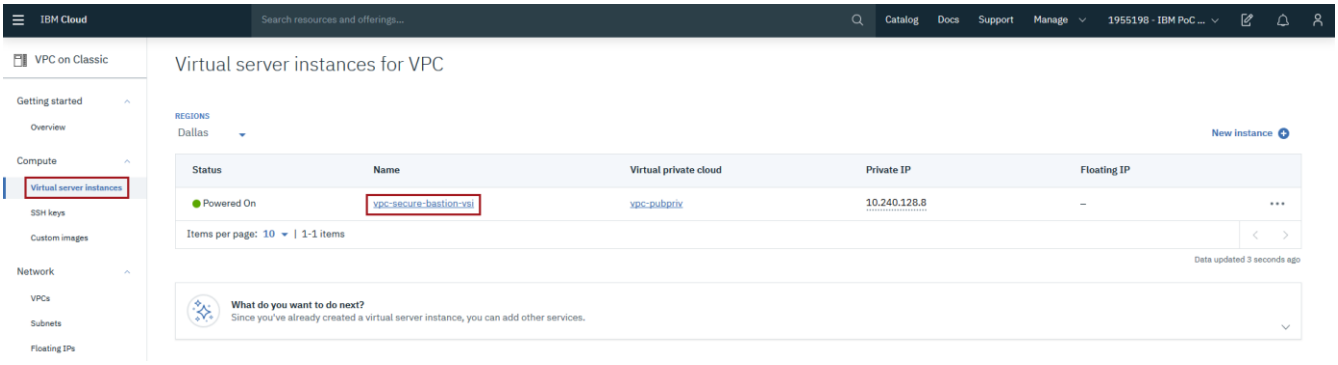
IBM **Cloud**

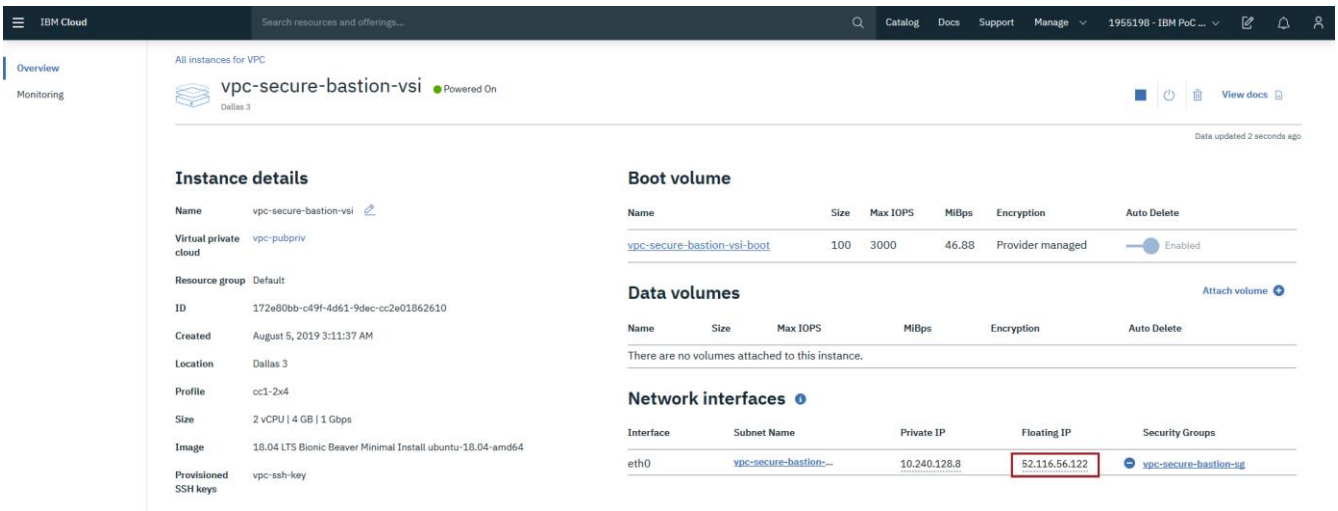

New virtual server for VPC
Boot volume
Data volumes
Network interfaces


Add SSH key
Add an SSH key that you'll use to access your virtual server instance.
View docs
Name
vpc-ssh-key
Resource group
Default
Region
Dallas
Frankfurt
London
Sydney
Tokyo
Public key
How do I get a public key?
API
Cancel
Add SSH key



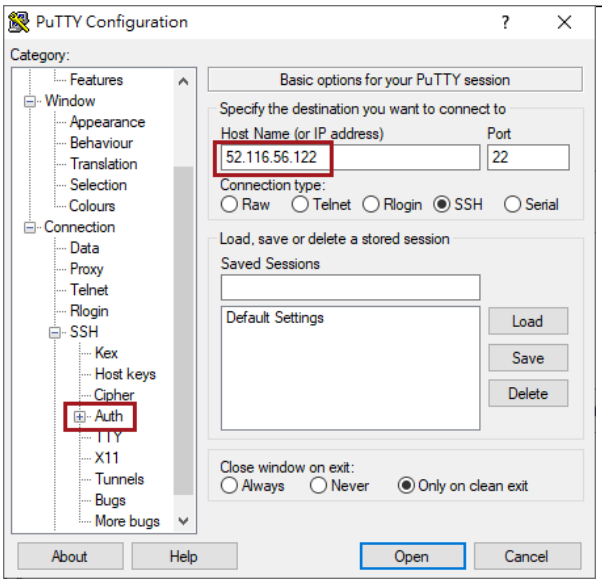
10. Once the instance is created, click on **wk1000vpc-secure-bastion-vsi** and **reserve** a floating IP.

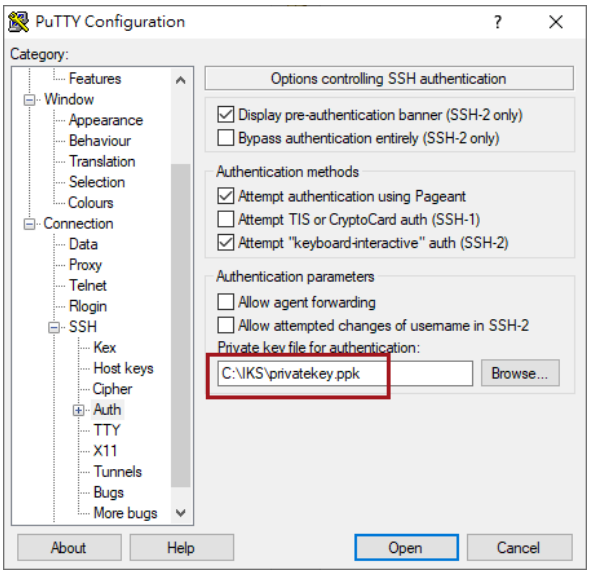


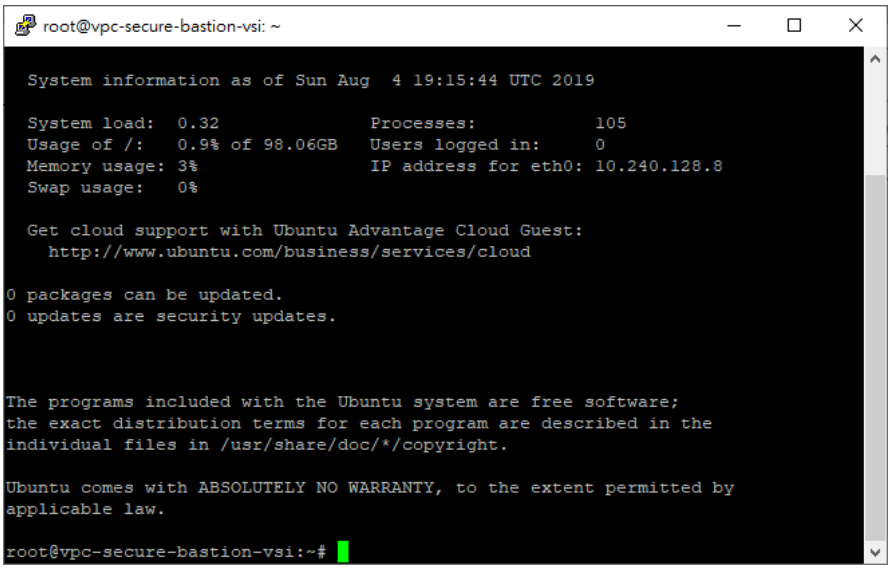


Test your bastion

Once your bastion's floating IP address is active, try connecting to it using ssh client with private key. (ex: Putty)


PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
52.116.56.122
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel


PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
C:\IKS\privatekey.ppk
Browse...
About
Help
Open
Cancel


root@vpc-secure-bastion-vsi: ~
System information as of Sun Aug 4 19:15:44 UTC 2019
System load: 0.32
Processes: 105
Usage of /: 0.9% of 98.06GB
Users logged in: 0
Memory usage: 3%
IP address for eth0: 10.240.128.8
Swap usage: 0%
Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud
0 packages can be updated.
0 updates are security updates.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
root@vpc-secure-bastion-vsi:~#

Configure a security group with maintenance access rules

With access to the bastion working, continue and create the security group for maintenance tasks like installing and updating the software.

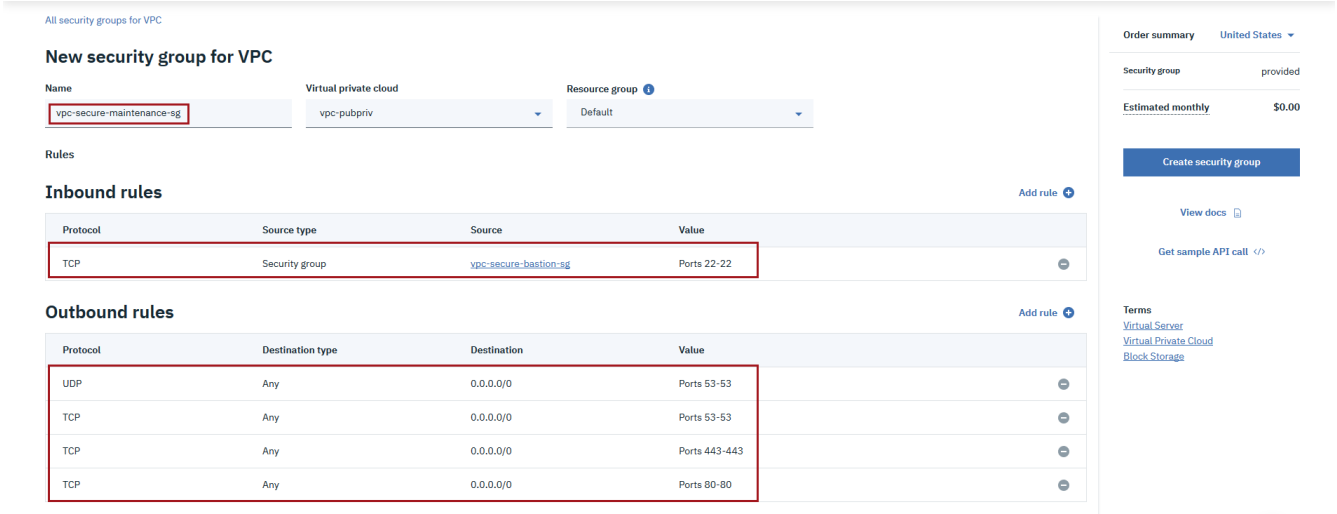
1. Navigate to **Security groups** and provision a new security group called **wk1000vpc-secure-maintenance-sg** with the below **outbound** rules

Protocol	Destination type	Destination	Value
TCP	Any	0.0.0.0/0	Ports 80-80
TCP	Any	0.0.0.0/0	Ports 443-443
TCP	Any	0.0.0.0/0	Ports 53-53
UDP	Any	0.0.0.0/0	Ports 53-53

2. DNS server requests are addressed on port 53. DNS uses TCP for Zone transfer and UDP for name queries either regular (primary) or reverse. HTTP requests are on port 80 and 443.
3. Next, add this **inbound** rule which allows SSH access from the bastion host.

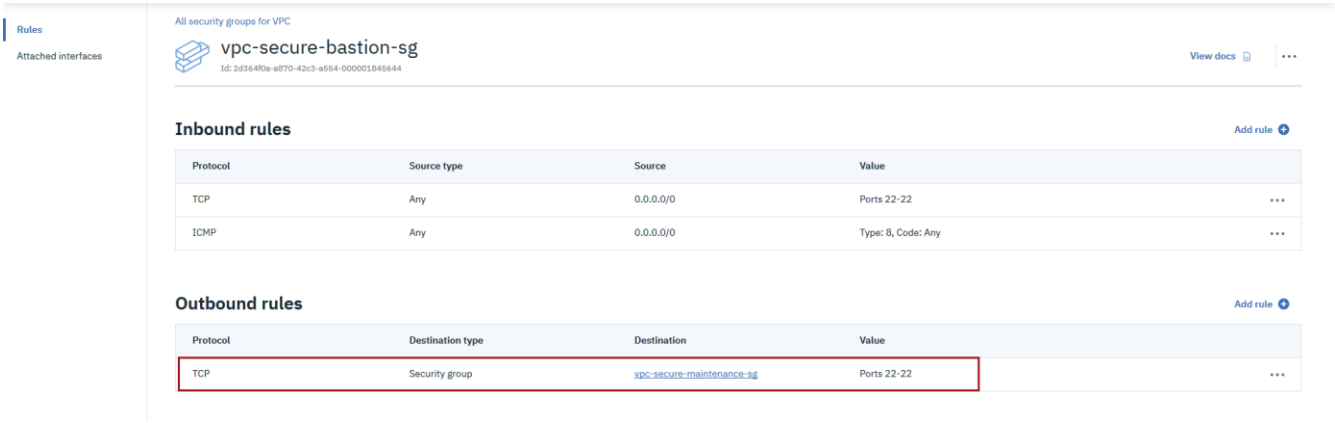
Protocol	Source type	Source	Value
TCP	Security group	wk1000vpc-secure-bastion-sg	Ports 22-22

4. Create the security group.



5. Navigate to **All Security Groups for VPC**, then select **wk1000vpc-secure-bastion-sg**.
6. Finally, edit the security group and add the following **outbound** rule.

Protocol	Destination type	Destination	Value
TCP	Security group	vpc-secure-maintenance-sg	Ports 22-22



Use the bastion host to access other instances in the VPC

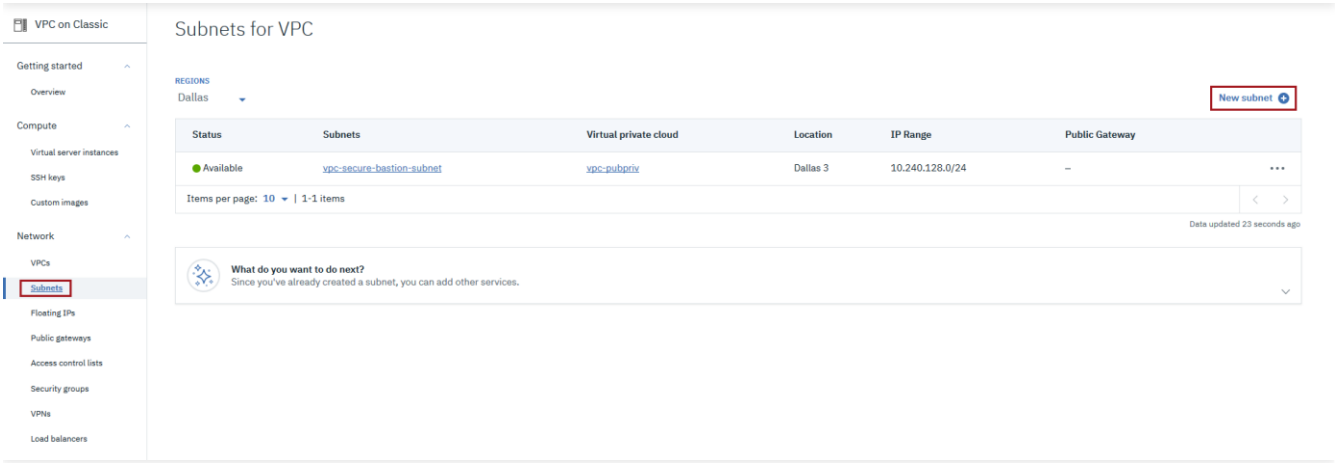
In this section, you will create a private subnet with virtual server instance and a security group. By default, any subnet created in a VPC is private.

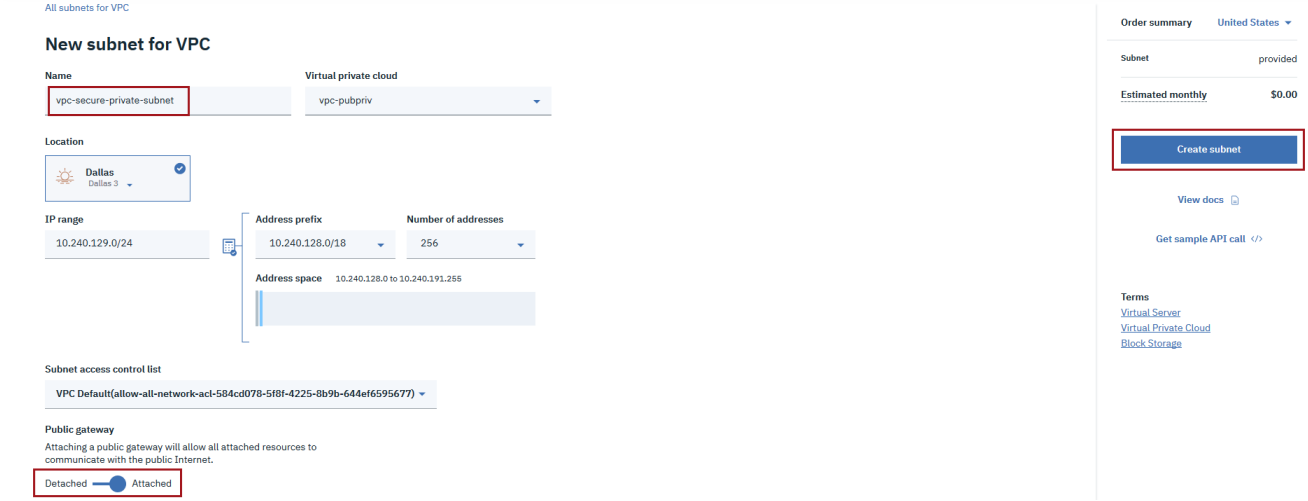
If you already have virtual server instances in your VPC that you want to connect to, you can skip the next three sections and start adding your virtual server instances to the maintenance security group.

Create a subnet

To create a new subnet,

1. Click **Subnets** under **Network** on the left pane, then **New subnet**.
    - Enter **wk1000vpc-secure-private-subnet** as name, then select the VPC you created.
    - Select a location.
    - Enter the IP range for the subnet in CIDR notation, i.e., **10.xxx.1.0/24**. Leave the **Address prefix** as it is and select the **Number of addresses** as 256.
2. Select **VPC default** for your subnet access control list (ACL). You can configure the inbound and outbound rules later.
3. Switch the **Public gateway** to **Attached**.
4. Click **Create subnet** to provision it.

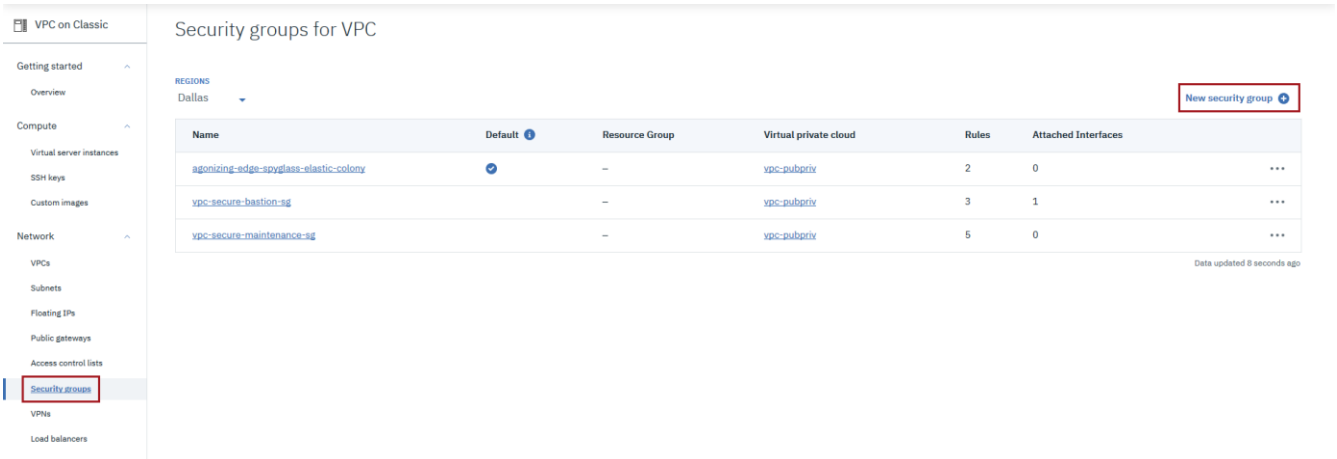


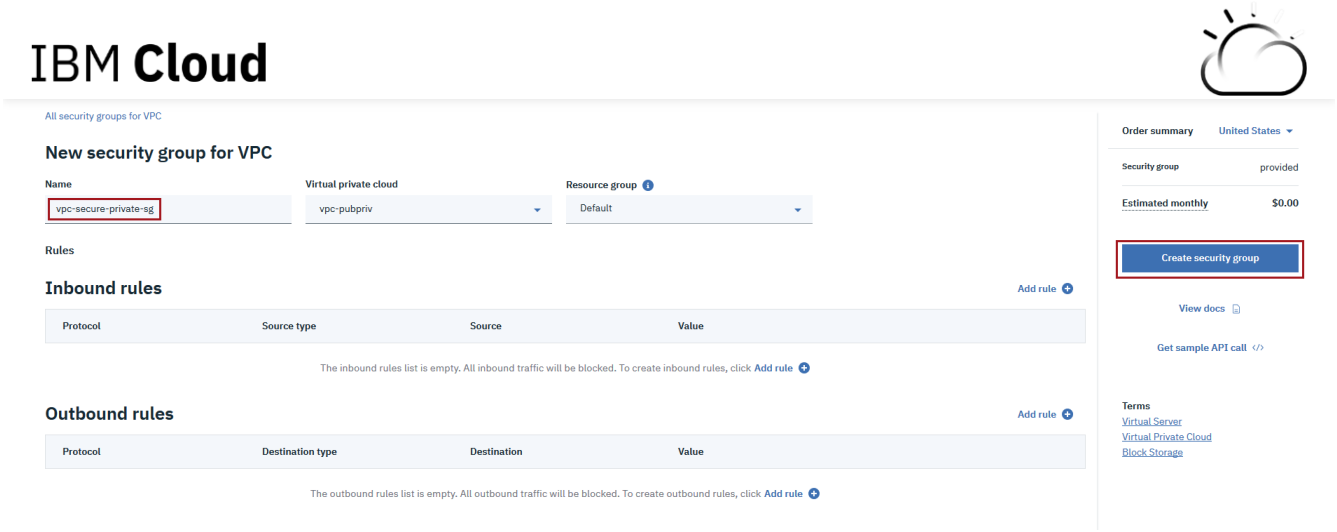


Create a security group

To create a new security group:

1. Click **Security groups** under Network, then **New security group**.
2. Enter **wk1000vpc-secure-private-sg** as name and select the VPC you created earlier.
3. Click **Create security group**.

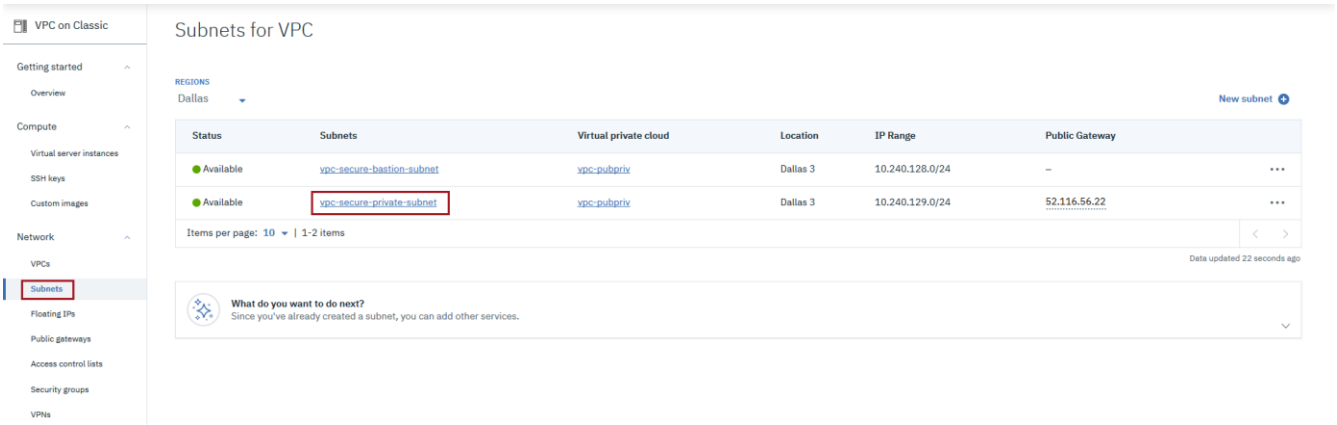


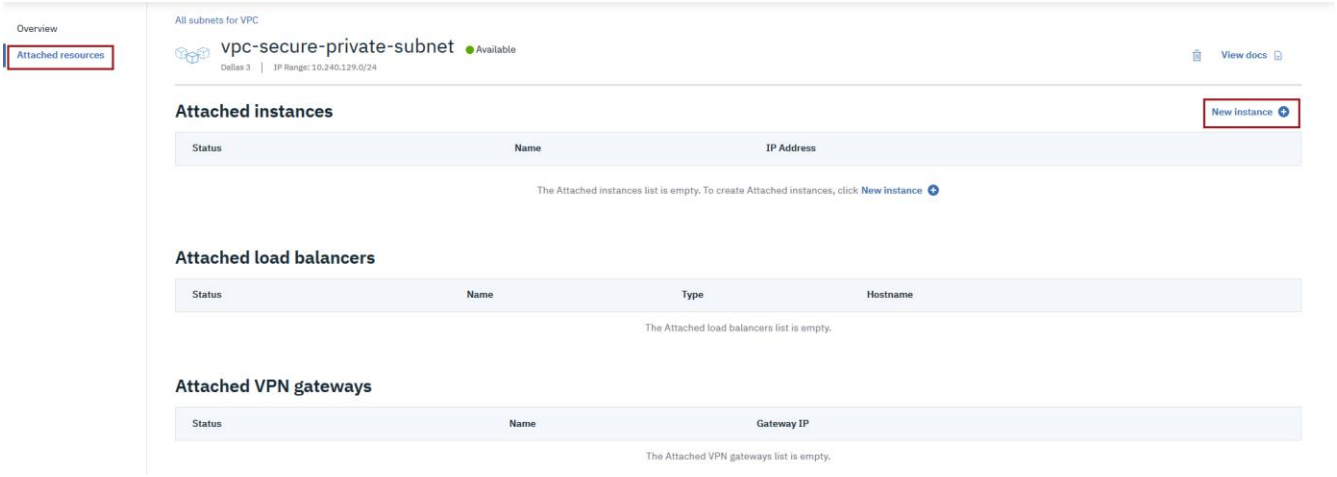


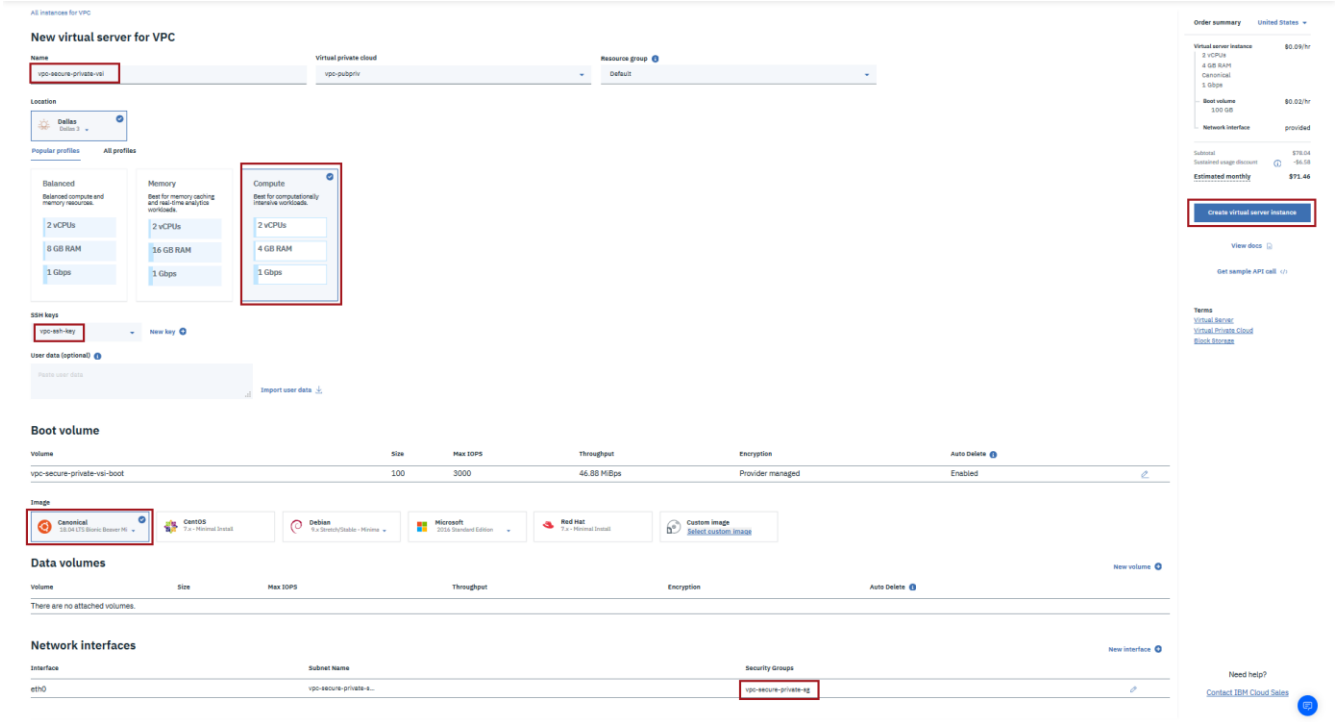
Create a virtual server instance

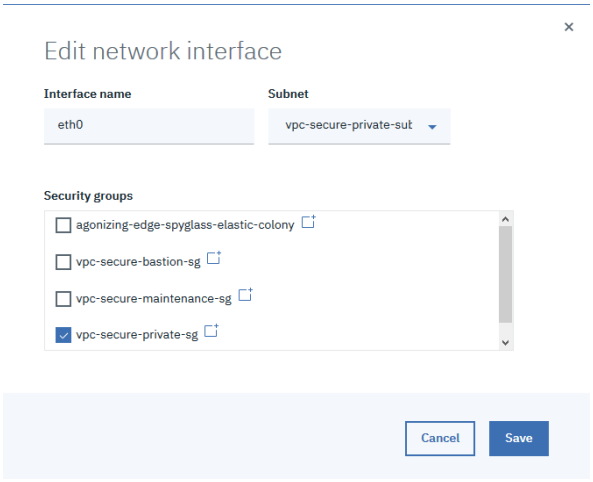
To create a virtual server instance in the newly created subnet: Click on **Attached resources** and provision a **New instance** called **wk1000vpc-secure-private-vsi** under your own VPC and resource group.

1. Click on the private subnet under **Subnets**.
2. Click **Attached resources**, then **New instance**.
3. Enter a unique name, **wk1000vpc-secure-private-vsi**, select the VPC your created and resource group as earlier.
4. Select a **Location** and make sure to later use the same location again.
5. Select **Compute** (2 vCPUs and 4 GB RAM) as your profile. To check other available profiles, click **All profiles**
6. For **SSH keys** pick the SSH key you created earlier for the bastion.
7. Select **Ubuntu Linux** as your image. You can pick any version of the image.
8. Under **Network interfaces**, click on the **Edit** icon next to the Security Groups
    - Select **wk1000vpc-secure-private-subnet** as the subnet.
    - Uncheck the default security and group and activate **wk1000vpc-secure-private-sg**.
    - Click **Save**.
9. Click **Create virtual server instance**.




Overview
Attached resources
All subnets for VPC
vpc-secure-private-subnet
Available
Dallas 3 | IP Range: 10.240.129.0/24
View docs
Attached instances
New instance
Status
Name
IP Address
The Attached instances list is empty. To create Attached instances, click New instance
Attached load balancers
Status
Name
Type
Hostname
The Attached load balancers list is empty.
Attached VPN gateways
Status
Name
Gateway IP
The Attached VPN gateways list is empty.


New virtual server for VPC
Name
Virtual private cloud
Resource group
Location
Dallas
Popular profiles
All profiles
Balanced
Memory
Compute
2 vCPUs
8 GB RAM
16 GB RAM
4 GB RAM
1 Gbps
SSH keys
New key
User data (optional)
Import user data
Boot volume
Volume
Size
Max IOPS
Throughput
Encryption
Auto Delete
vpc-secure-private-vsi-boot
100
3000
46.88 MiBps
Provider managed
Enabled
Image
Canonical
CentOS
Debian
Microsoft
Red Hat
Custom image
Select custom image
Data volumes
New volume
There are no attached volumes.
Network interfaces
New interface
Interface
Subnet Name
Security Groups
eth0
Order summary
Create virtual server instance
View docs
Get sample API call
Terms
Need help?
Contact IBM Cloud Sales

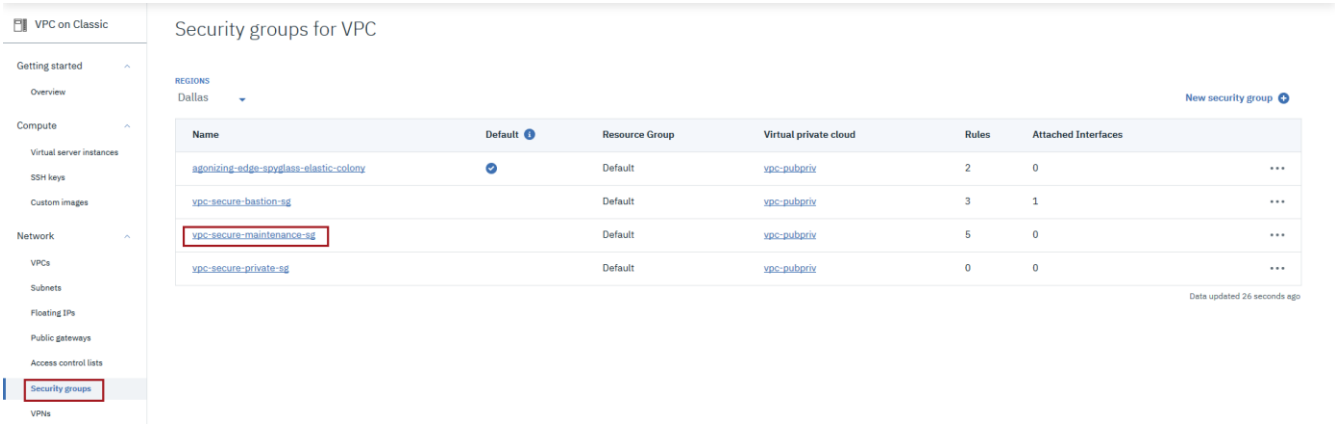

Edit network interface
Interface name
eth0
Subnet
vpc-secure-private-sut
Security groups
agonizing-edge-spyglass-elastic-colony
vpc-secure-bastion-sg
vpc-secure-maintenance-sg
vpc-secure-private-sg
Cancel
Save

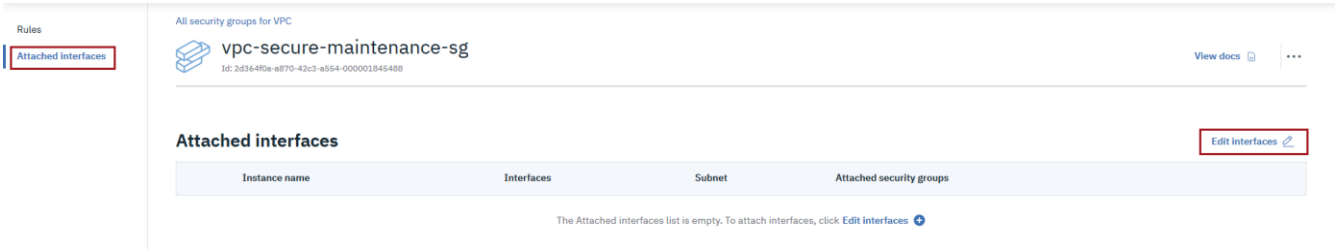
Add virtual servers to the maintenance security group

For administrative work on the servers, you have to associate the specific virtual servers with the maintenance security group. In the following, you will enable maintenance, log into the private server, update the software package information, then disassociate the security group again.

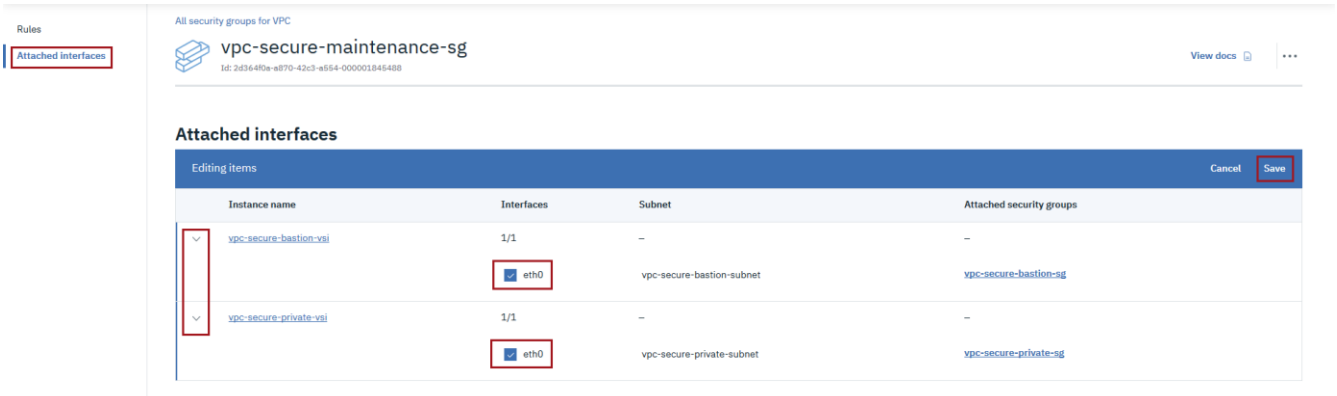
Let's enable the maintenance security group for the server.

1. Navigate to **Security groups** and select **wk1000vpc-secure-maintenance-sg** security group.





2. Click **Attached interfaces**, then **Edit interfaces**.
3. Expand the virtual server instances and activate the selection next to **primary** in the **Interfaces** column.

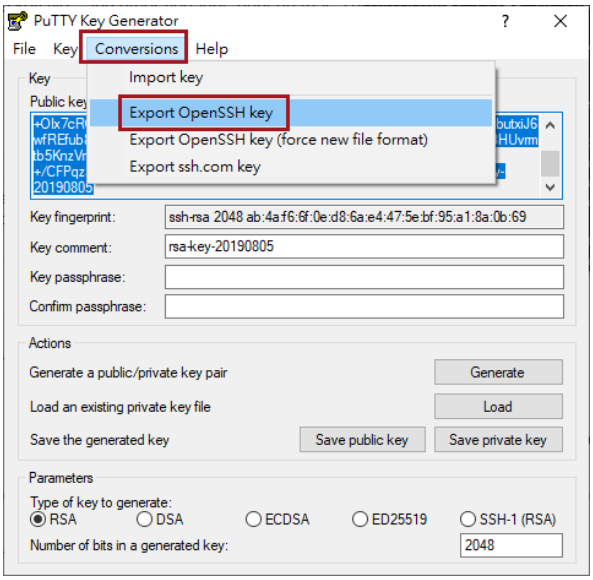


4. Click **Save** for the changes to be applied.

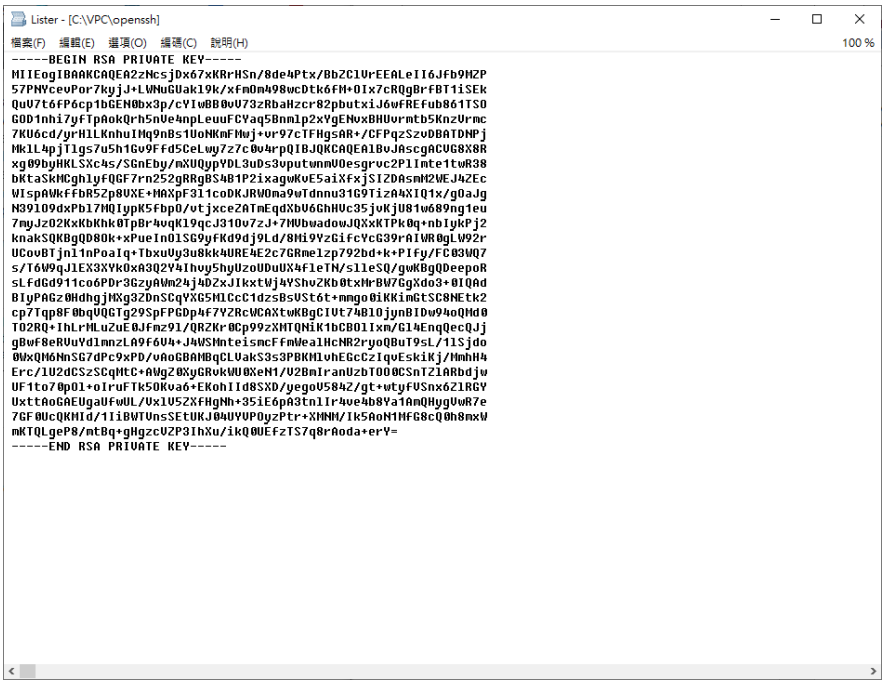
Connect to the instance

To SSH into an instance using its **private IP**, you will use the bastion host as your **jump host**.

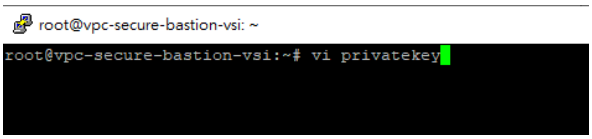
1. Obtain the private IP address of a virtual server instance under **Virtual server instances**.
2. Use Putty to connect the bastion **floating IP** address you used earlier
3. Use PuTTY Key Generator to export OpenSSH key file

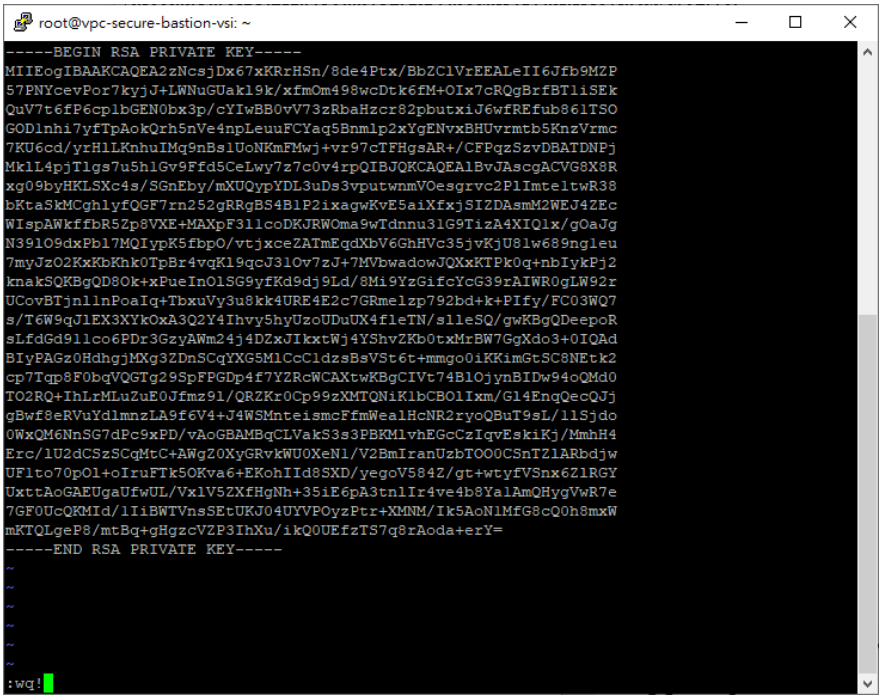


4. Copy the key content and create private key file on the bastion host

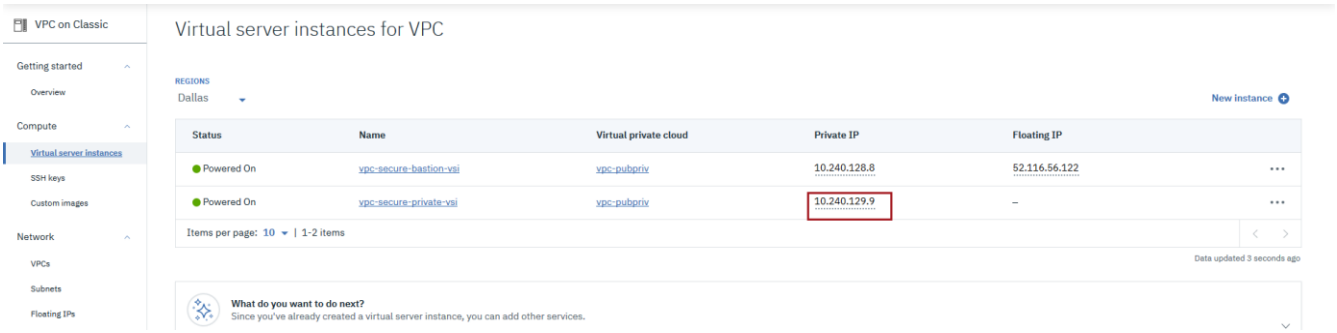


vi privatekey

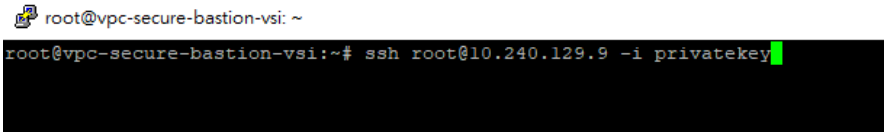




5. Copy the private host IP and use below command to connect private host.



ssh root@private_IP -I privatekey



6. If you get the bad permissions msg.. You can use below command to change the private key file privilege.

root@vpc-secure-bastion-vsi: ~

```
root@vpc-secure-bastion-vsi:~# ssh root@10.240.129.9 -i privatekey
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'privatekey' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "privatekey": bad permissions
root@10.240.129.9: Permission denied (publickey).
root@vpc-secure-bastion-vsi:~#
```

chmod 700 privatekey

root@vpc-secure-bastion-vsi: ~

```
root@vpc-secure-bastion-vsi:~# chmod 700 privatekey
```

```
root@vpc-secure-bastion-vsi:~# ssh root@10.240.129.9 -i privatekey
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Aug  5 15:19:31 UTC 2019

  System load:  0.0               Processes:           98
  Usage of /:   0.9% of 98.06GB   Users logged in:     0
  Memory usage: 3%                IP address for eth0: 10.240.129.9
  Swap usage:   0%


  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.


Last login: Mon Aug  5 15:09:21 2019 from 10.240.128.8
root@vpc-secure-private-vsi:~#
```

Install software and perform maintenance tasks

Once connected, you can install software on the virtual server in the private subnet or perform maintenance tasks.

1. Use below command to update the software package information:

apt-get update

```
root@vpc-secure-private-vsi:~# apt-get update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic InRelease [242 kB]
Get:3 http://security.ubuntu.com/ubuntu bionic-security/multiverse Sources [2744 B]
Get:4 http://security.ubuntu.com/ubuntu bionic-security/universe Sources [151 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:6 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/restricted Sources [1504 B]
Get:8 http://archive.ubuntu.com/ubuntu bionic/universe Sources [9051 kB]
Get:9 http://security.ubuntu.com/ubuntu bionic-security/main Sources [117 kB]
Get:10 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [464 kB]
Get:11 http://security.ubuntu.com/ubuntu bionic-security/main Translation-en [160 kB]
Get:12 http://security.ubuntu.com/ubuntu bionic-security/restricted amd64 Packages [4296
B]
Get:13 http://security.ubuntu.com/ubuntu bionic-security/restricted Translation-en [2192
B]
Get:14 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [576 kB]
Get:15 http://archive.ubuntu.com/ubuntu bionic/multiverse Sources [181 kB]
Get:16 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en [189 kB]
Get:17 http://archive.ubuntu.com/ubuntu bionic/restricted Sources [5324 B]
Get:18 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [4008
B]
Get:19 http://archive.ubuntu.com/ubuntu bionic/main Sources [829 kB]
Get:20 http://security.ubuntu.com/ubuntu bionic-security/multiverse Translation-en [2060
B]
Get:21 http://archive.ubuntu.com/ubuntu bionic/main amd64 Packages [1019 kB]
Get:22 http://archive.ubuntu.com/ubuntu bionic/main Translation-en [516 kB]
Get:23 http://archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages [9184 B]
Get:24 http://archive.ubuntu.com/ubuntu bionic/restricted Translation-en [3584 B]
Get:25 http://archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]
Get:26 http://archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]
Get:27 http://archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Get:28 http://archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Get:29 http://archive.ubuntu.com/ubuntu bionic-updates/multiverse Sources [5452 B]
```

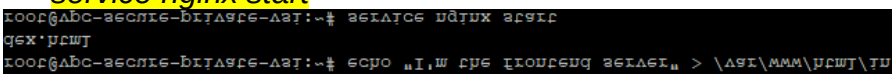
2. Install the desired software, e.g., Nginx.

apt-get install -y nginx

```
root@vpc-secure-private-vsi: ~
root@vpc-secure-private-vsi:~# apt-get install -y nginx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libjbig0
  libjpeg-turbo8 libjpeg8 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
  libnginx-mod-mail libnginx-mod-stream libtiff5 libwebp6 libxpm4 nginx-common
  nginx-core
Suggested packages:
  libgd-tools fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libjbig0
  libjpeg-turbo8 libjpeg8 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
  libnginx-mod-mail libnginx-mod-stream libtiff5 libwebp6 libxpm4 nginx
  nginx-common nginx-core
0 upgraded, 18 newly installed, 0 to remove and 229 not upgraded.
Need to get 2461 kB of archives.
After this operation, 8202 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libjpeg-turbo8
amd64 1.5.2-0ubuntu5.18.04.1 [110 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic/main amd64 fonts-dejavu-core all 2
.37-1 [1041 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic/main amd64 fontconfig-config all 2
.12.6-0ubuntu2 [55.8 kB]
```

3. Create index.html and Install the desired software, e.g., Nginx.

echo "I'm the frontend server" > /var/www/html/index.html
service nginx start



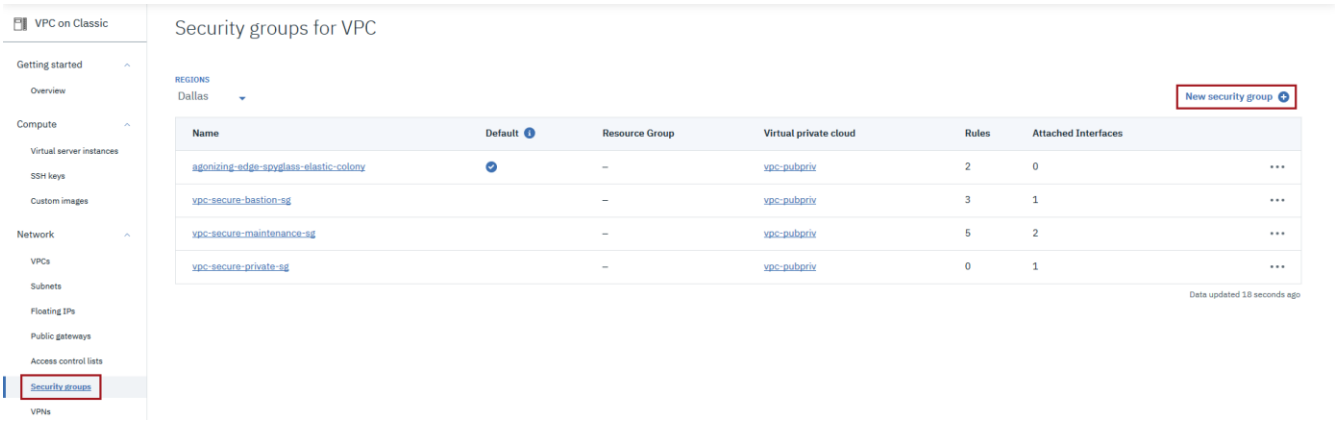
Create a frontend security group

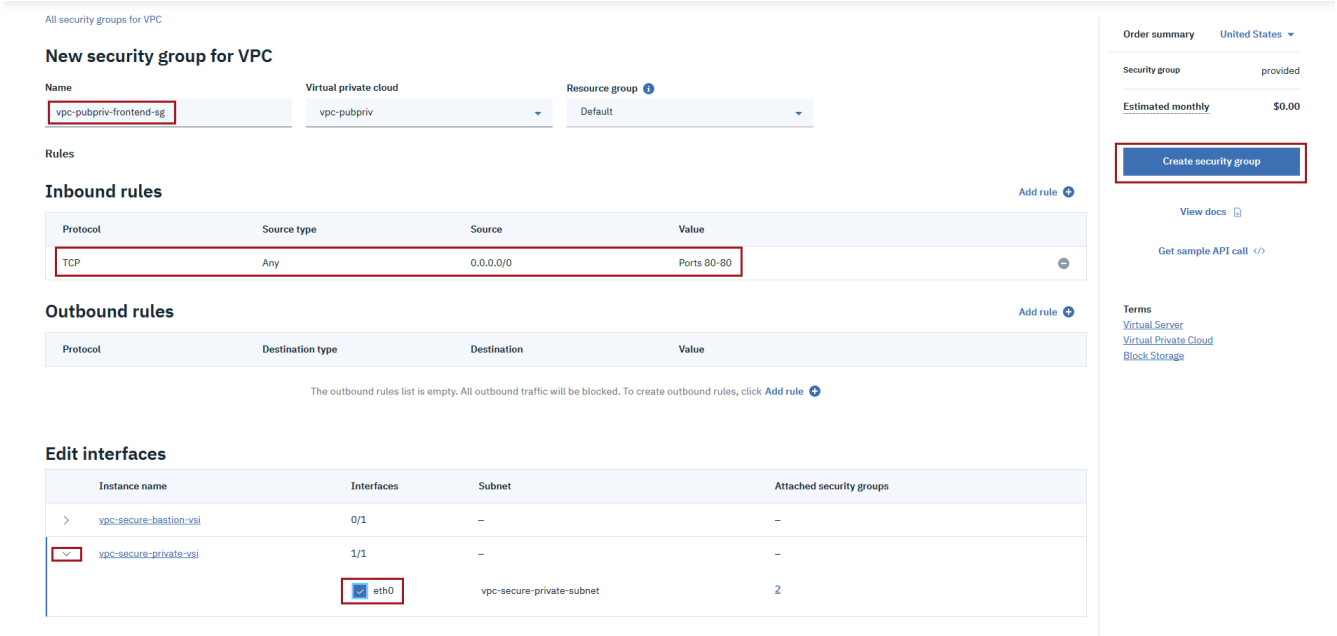
To create a new security group for the frontend:

1. Click **Security groups** under Network, then **New security group**.
2. Enter **wk1000vpc-pubpriv-frontend-sg** as name and select the VPC you created earlier.
3. Add the following **inbound** rule using Add rule.

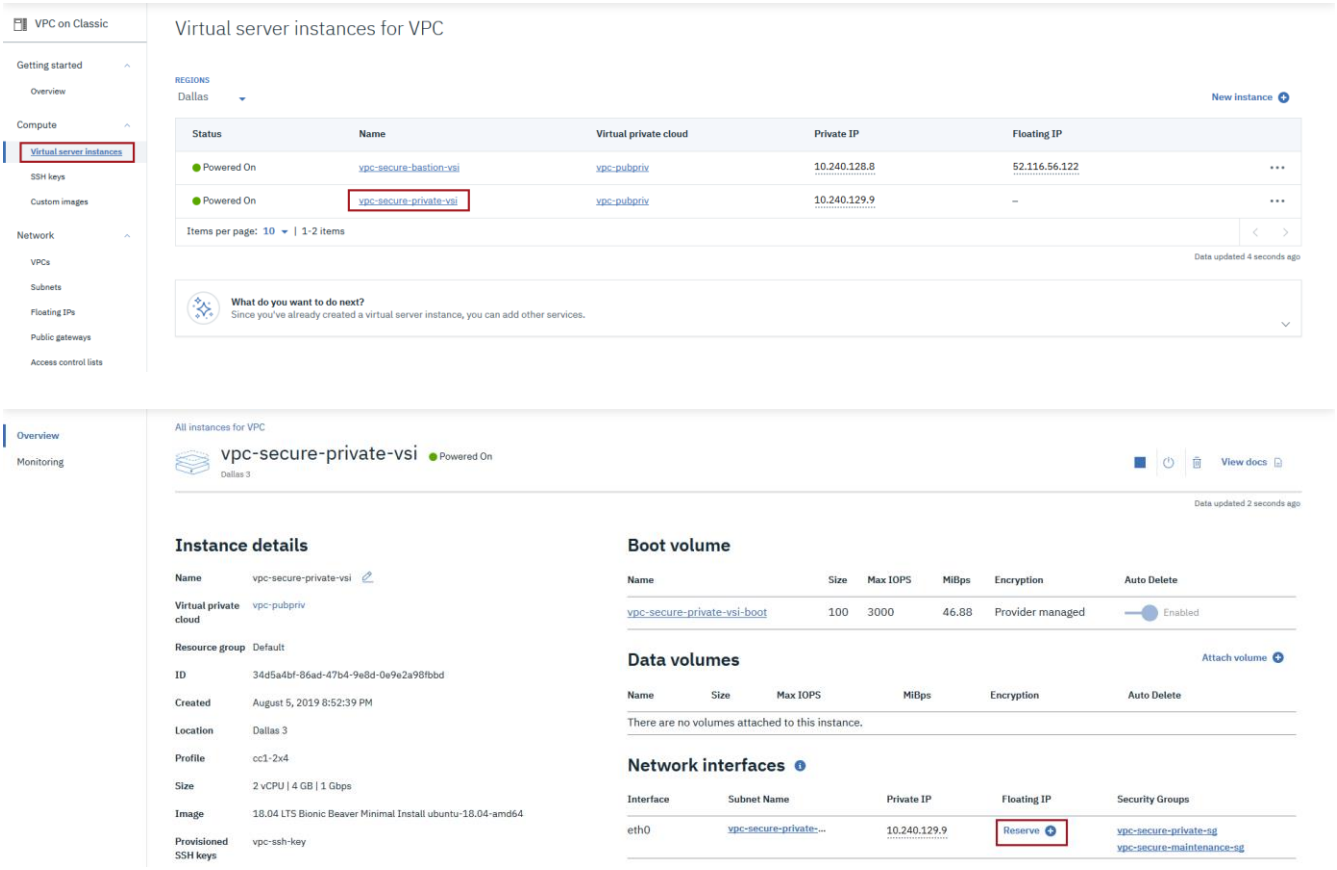
Protocol	Source type	Source	Value	Description
TCP	Any	0.0.0.0/0	Ports 80-80	This rule allows incoming connections on port 80 to the frontend server.

4. Edit interface and expand the private virtual server instance and activate the selection next to **primary** in the **Interfaces** column
5. Click **Create security group**.

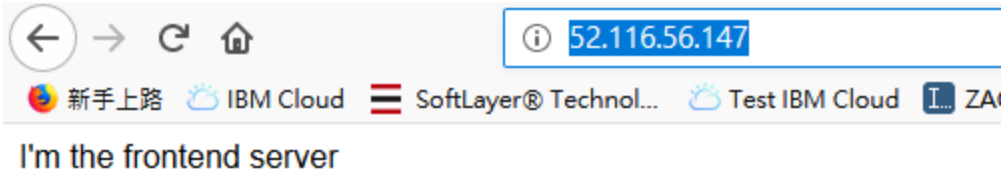




6. Once the instance is created, click on **wk1000vpc-secure-private-vsi** and **reserve** a floating IP.



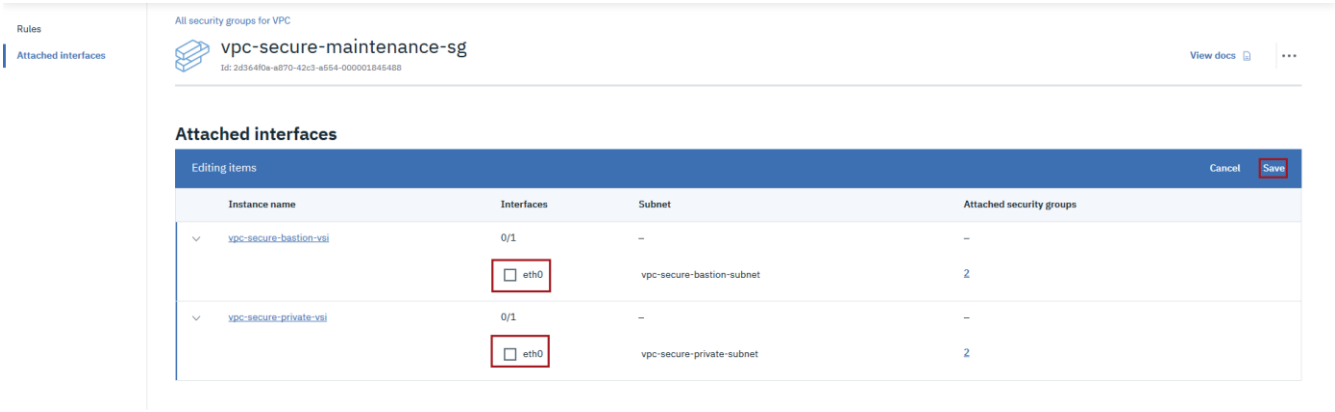
7. Use browser to navigate the private host floating IP to see the index.html you created.



Disable the maintenance security group

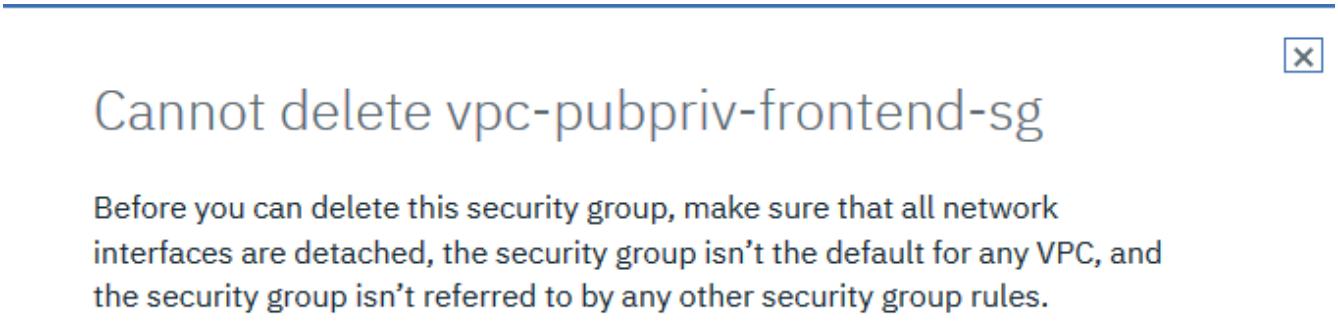
Once you're done installing software or performing maintenance, you should remove the virtual servers from the maintenance security group to keep them isolated.

1. Navigate to **Security groups** and select **wk1000vpc-secure-maintenance-sg** security group.
2. Click **Attached interfaces**, then **Edit interfaces**.
3. Expand the virtual server instances and uncheck the selection next to **primary** in the **Interfaces** column.
4. Click **Save** for the changes to be applied.

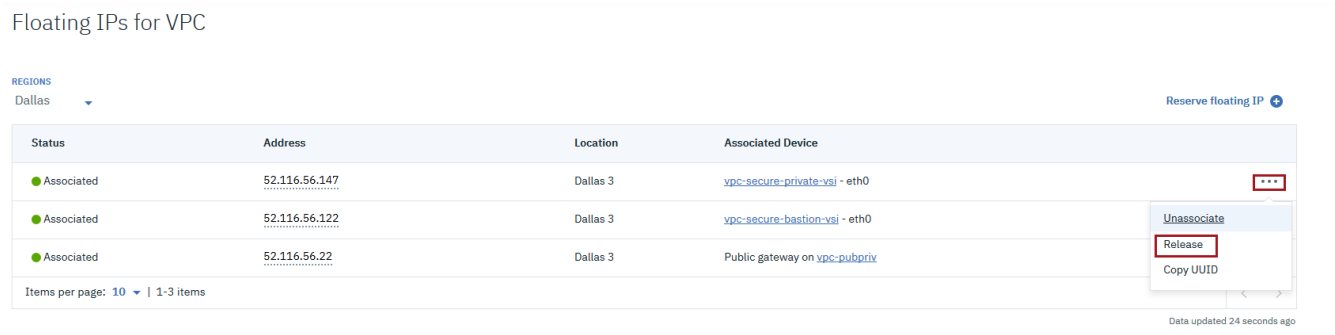


Remove resources

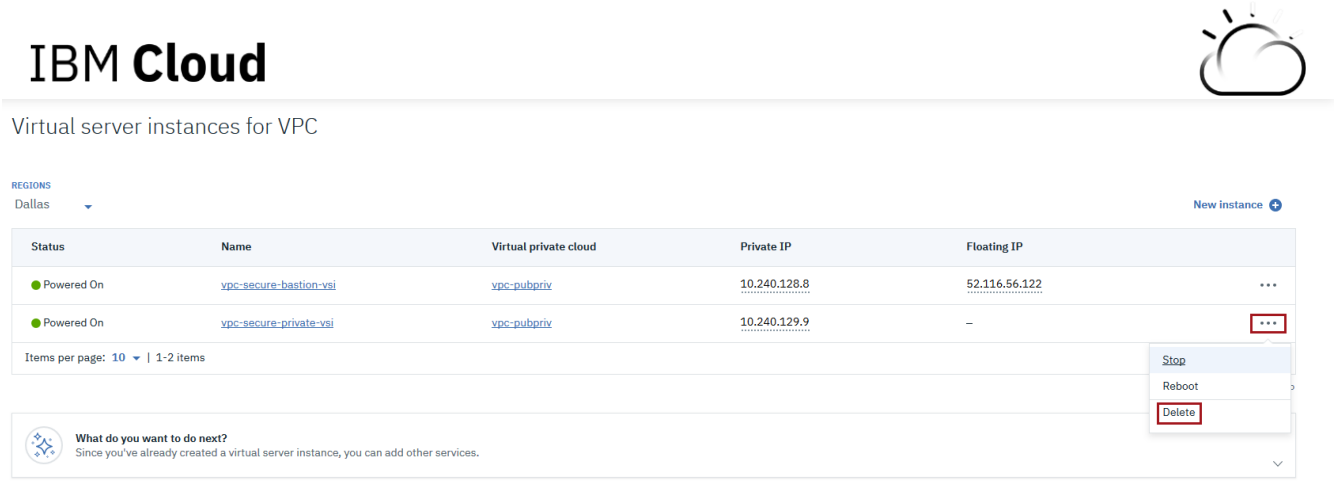
1. You can delete the security group directly and you would get the warning.



2. In the VPC management console, click on **Floating IPs**, then on the IP address for your VSIs, then in the action menu select **Release**. Confirm that you want to release the IP address.



3. Next, switch to **Virtual server instances** and **Delete** your instances. The instances will be deleted and their status will remain in **Deleting** for a while. Make sure to refresh the browser from time to time.



4. Once the VSIs are gone, switch to **Subnets**. If the subnet has an attached public gateway, then click on the subnet name. In the subnet details, detach the public gateway. Subnets without public gateway can be deleted from the overview page. Delete your subnets.
5. After the subnets have been deleted, switch to **VPC** tab and delete your VPC.

When using the console, you may need to refresh your browser to see updated status information after deleting a resource.