IBM Cloud 用戶實作研習營

IBM Cloud Virtual Private Cloud (VPC) 使用教學

2019/8/7

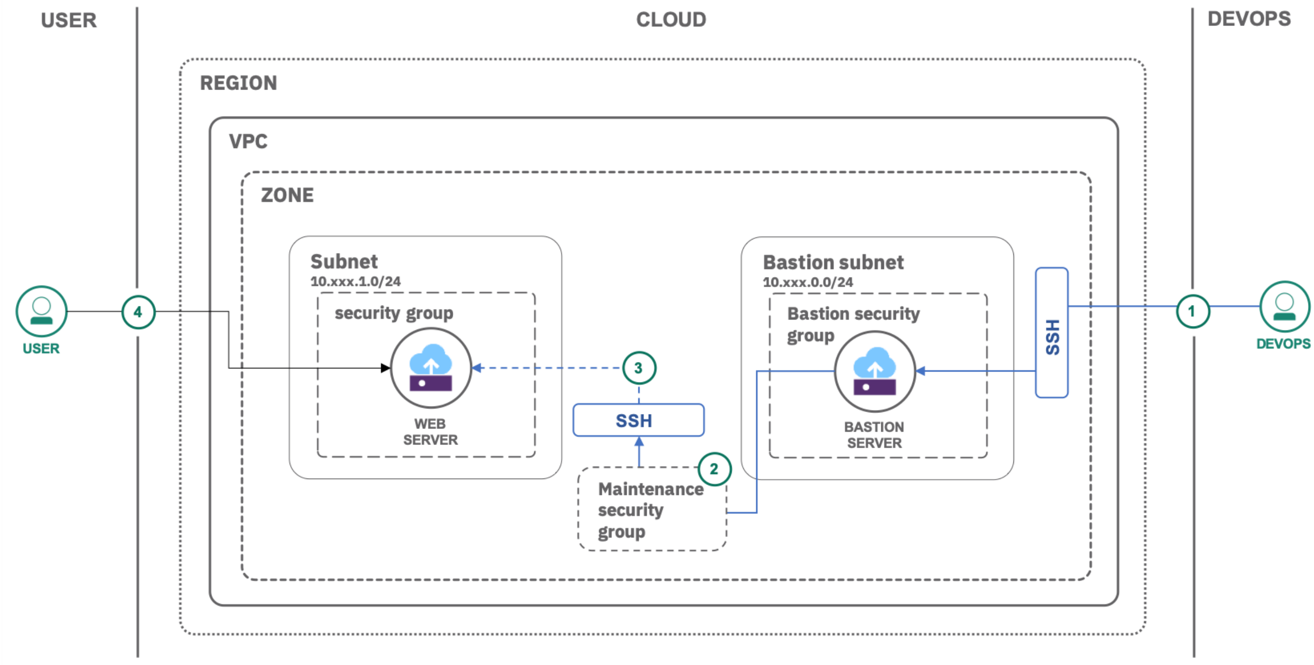
Securely access remote instances with a bastion host

- 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 bastion host

In this section, you will create and configure a bastion host along with a security group in a separate subnet.

Create a subnet

1. Click **Subnets** under **Network** on the left pane, then **New subnet**.
    - Enter **vpc-secure-bastion-subnet** as name, then select the VPC you created.
    - Select a location and zone.
    - 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.
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 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 **vpc-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. To enhance security further, the inbound traffic could be restricted to the company network or a typical home network. You could run `curl ipecho.net/plain ; echo` to obtain your network's external IP address and use that instead.
4. 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 **vpc-secure-bastion-subnet**.
2. Click on **Attached resources** and provision a **New instance** called **vpc-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. To create a new **SSH key**, click **New key**
    - Enter **vpc-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**.

6. Select **Ubuntu Linux** as your image. You can pick any version of the image.
7. Under **Network interfaces**, click on the **Edit** icon next to the Security Groups
    - Make sure that **vpc-secure-bastion-subnet** is selected as the subnet.
    - Uncheck the default security group and mark **vpc-secure-bastion-sg**.
    - Click **Save**.
8. Click **Create virtual server instance**.
9. Once the instance is created, click on **vpc-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:

```
ssh -i ~/.ssh/<PRIVATE_KEY> root@<BASTION_FLOATING_IP_ADDRESS>
```

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 vpc-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	vpc-secure-bastion-sg	Ports 22-22

4. Create the security group.
5. Navigate to **All Security Groups for VPC**, then select **vpc-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 **vpc-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 **vpc-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 vpc-secure-bastion-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, **vpc-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 **vpc-secure-private-subnet** as the subnet.
   - Uncheck the default security and group and activate **vpc-secure-private-sg**.
   - Click **Save**.
9. Click **Create virtual server instance**.

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 **vpc-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 the ssh command with `-J` to log into the server with the bastion floating IP address you used earlier and the server Private IP address shown under Network interfaces.
3. `ssh -J root@<BASTION_FLOATING_IP_ADDRESS> root@<PRIVATE_IP_ADDRESS>`

`-J` flag is supported in OpenSSH version 7.3+. In older versions `-J` is not available. In this case the safest and most straightforward way is to use ssh's stdio forwarding (`-W`) mode to "bounce" the connection through a bastion host. e.g., `ssh -o ProxyCommand="ssh -W %h:%p root@<BASTION_FLOATING_IP_ADDRESS" root@<PRIVATE_IP_ADDRESS>`

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. First, update the software package information:
2.
3.

```
1. apt-get update
```

2.
3. Install the desired software, e.g., Nginx or MySQL or IBM Db2.

When done, disconnect from the server with `exit` command.

To allow HTTP/HTTPS requests from the internet user, assign a floating IP to the VSI in the private subnet and open required ports (80 - HTTP and 443 - HTTPS) via the inbound rules in the security group of private VSI.

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 **vpc-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. 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.
2. Once the VSIs are gone, switch to **Subnets** and delete your subnets.
3. After the subnets have been deleted, switch to the **Virtual private clouds** 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.

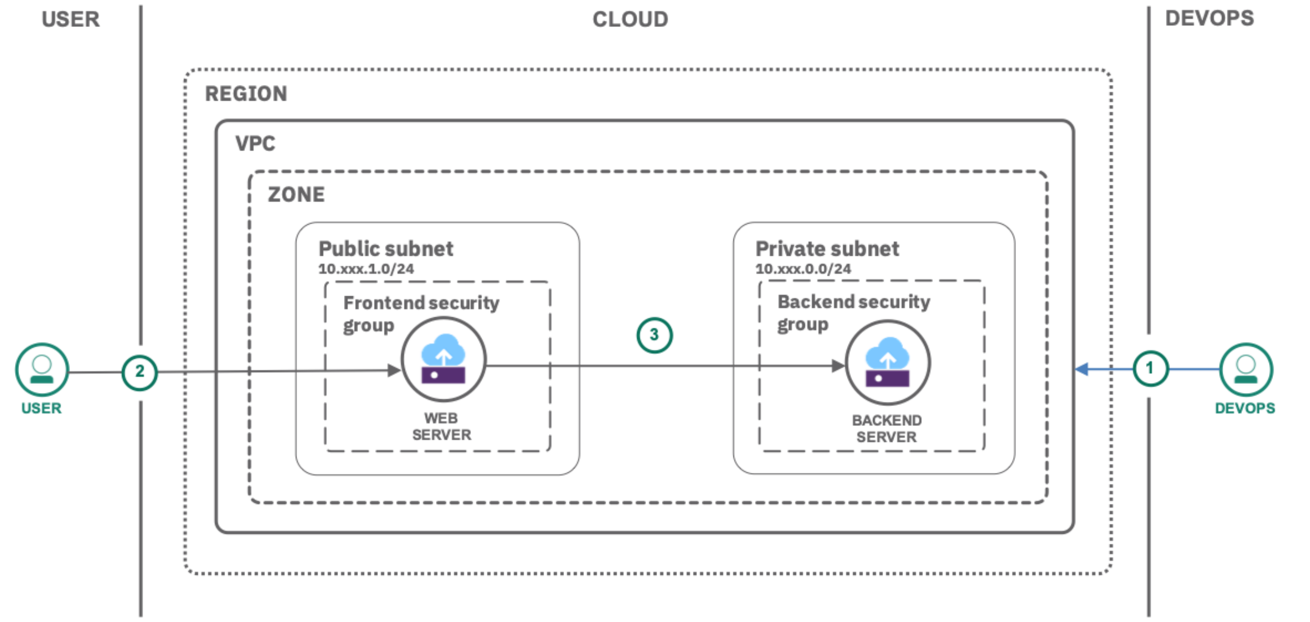
Private and public subnets in a Virtual Private Cloud

- This tutorial walks you through creating your own IBM® Cloud Virtual Private Cloud (VPC) with a public and a private subnet and a virtual server instance (VSI) in each subnet. A VPC is your own, private cloud on shared cloud infrastructure with logical isolation from other virtual networks.

Objectives

- Understand the infrastructure objects available for virtual private clouds
- Learn how to create a virtual private cloud, subnets and server instances
- Know how to apply security groups to secure access to the servers

Architecture



- The admin (DevOps) sets up the required infrastructure (VPC, subnets, security groups with rules, VSIs) on the cloud.
- The internet user makes an HTTP/HTTPS request to the web server on the frontend.
- The frontend requests private resources from the secured backend and serves results to the user.

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.

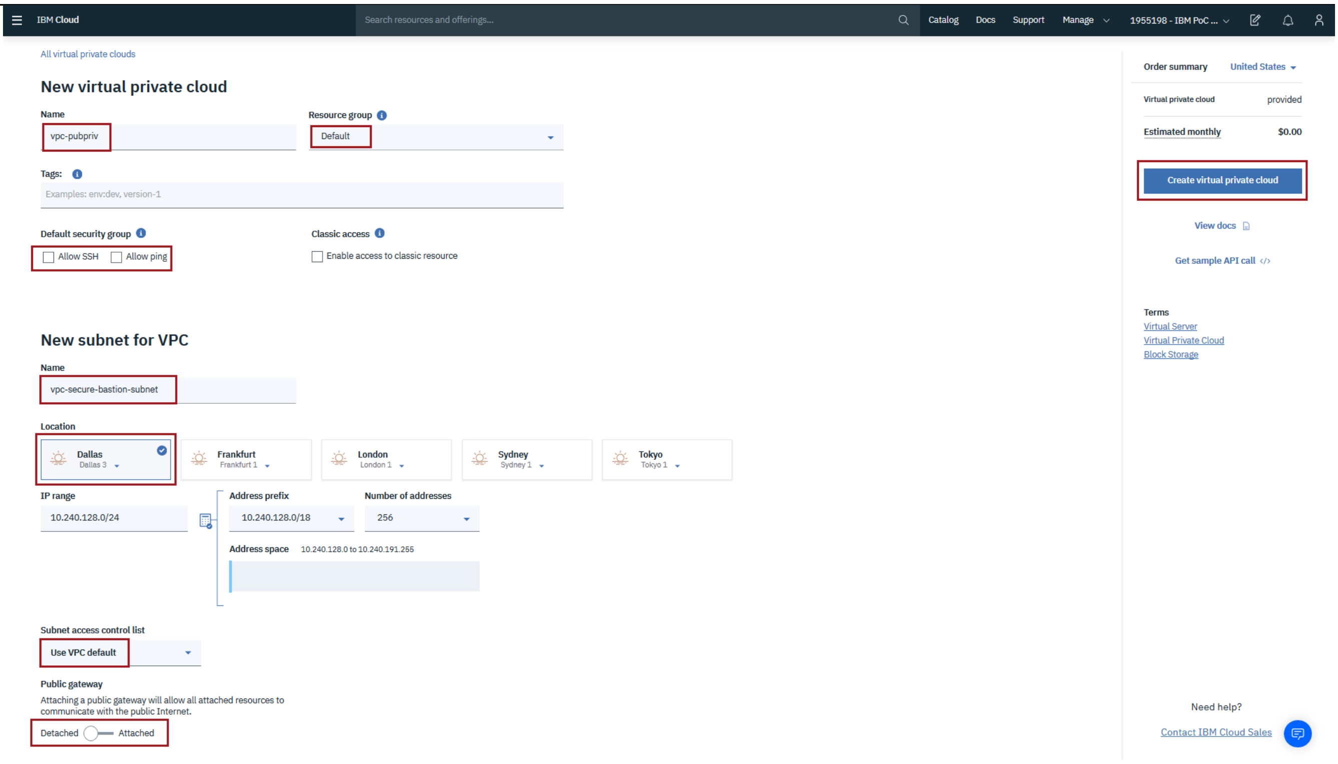
Login to IBM Cloud

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

Get a Kubernetes cluster

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 **vpc-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 **vpc-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**.



All virtual private clouds

New virtual private cloud

Name: vpc-pubpriv

Resource group: Default

Tags: Examples: env:dev, version-1

Default security group: □ Allow SSH □ Allow ping

Classic access: □ Enable access to classic resource

New subnet for VPC

Name: vpc-secure-bastion-subnet

Location: Dallas (Dallas 3) ✓ | Frankfurt (Frankfurt 1) | London (London 1) | Sydney (Sydney 1) | Tokyo (Tokyo 1)

IP range: 10.240.128.0/24

Address prefix: 10.240.128.0/18

Number of addresses: 256

Address space: 10.240.128.0 to 10.240.191.255

Subnet access control list: Use VPC default

Public gateway: Attaching a public gateway will allow all attached resources to communicate with the public Internet.

Detached ○ Attached

Order summary: United States

Virtual private cloud: provided

Estimated monthly: $0.00

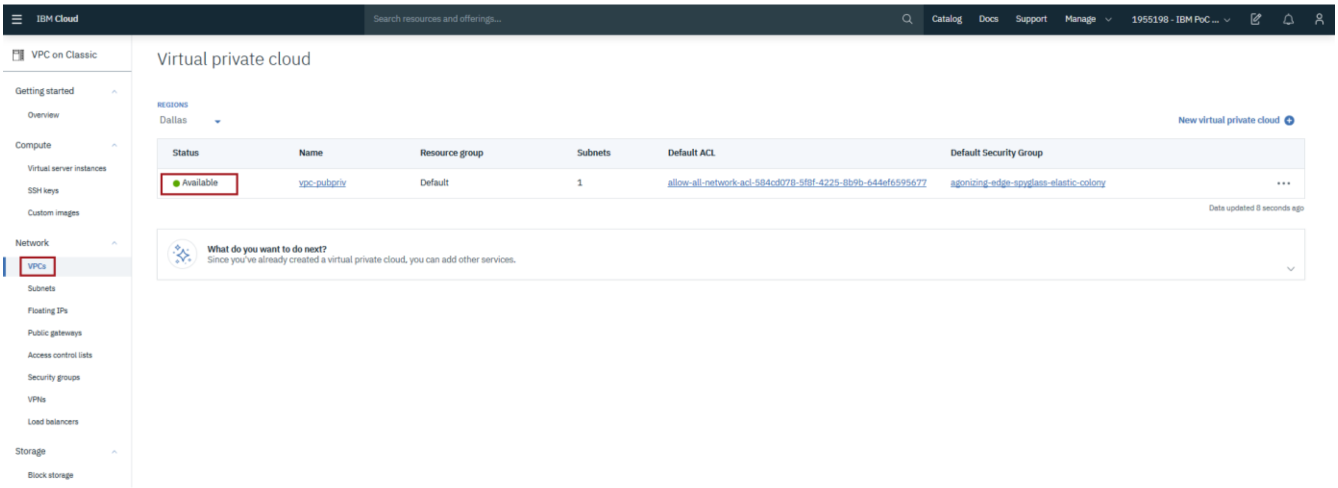
Create virtual private cloud

View docs

Get sample API call

Terms
Virtual Server
Virtual Private Cloud
Block Storage

Need help?
Contact IBM Cloud Sales



Virtual private cloud

REGIONS: Dallas

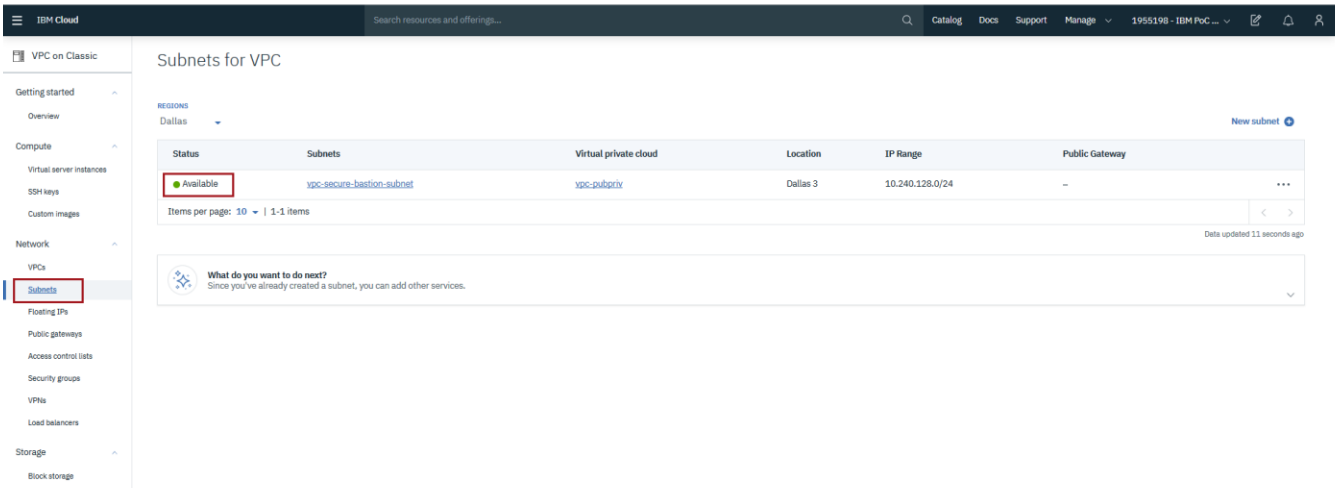
New virtual private cloud

Status	Name	Resource group	Subnets	Default ACL	Default Security Group
● Available	vpc-pubpriv	Default	1	allow-all-network-acl-584cd078-5f8f-4225-8b9b-644ef6595677	agonizing-edge-spyglass-elastic-colony

Data updated 8 seconds ago

What do you want to do next?
Since you've already created a virtual private cloud, you can add other services.

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



Subnets for VPC

Status	Subnets	Virtual private cloud	Location	IP Range	Public Gateway
● Available	vpc-secure-bastion-subnet	vpc-pubpriv	Dallas 3	10.240.128.0/24	–

Items per page: 10 | 1-1 items

Data updated 11 seconds ago

What do you want to do next?
Since you've already created a subnet, you can add other services.

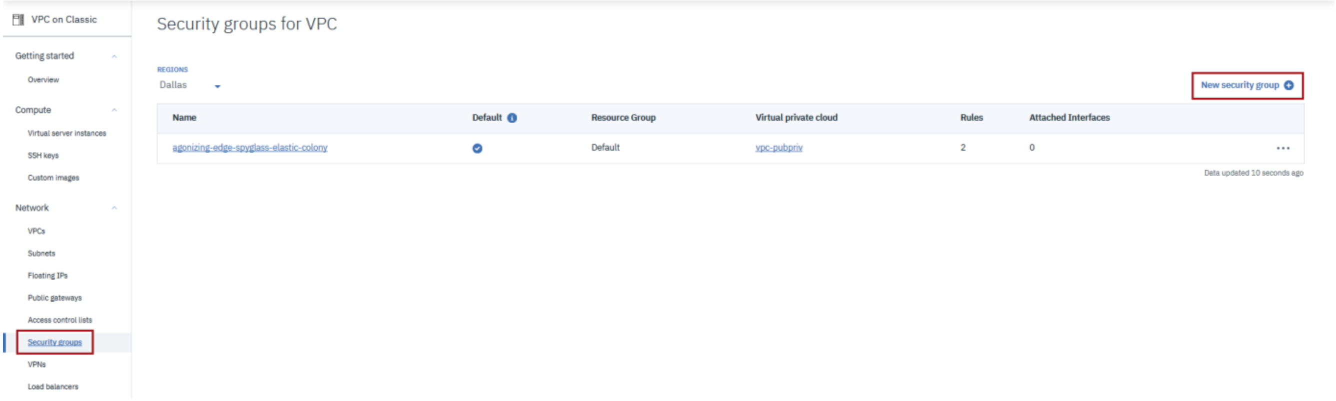
Create and configure bastion security group

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 **vpc-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**

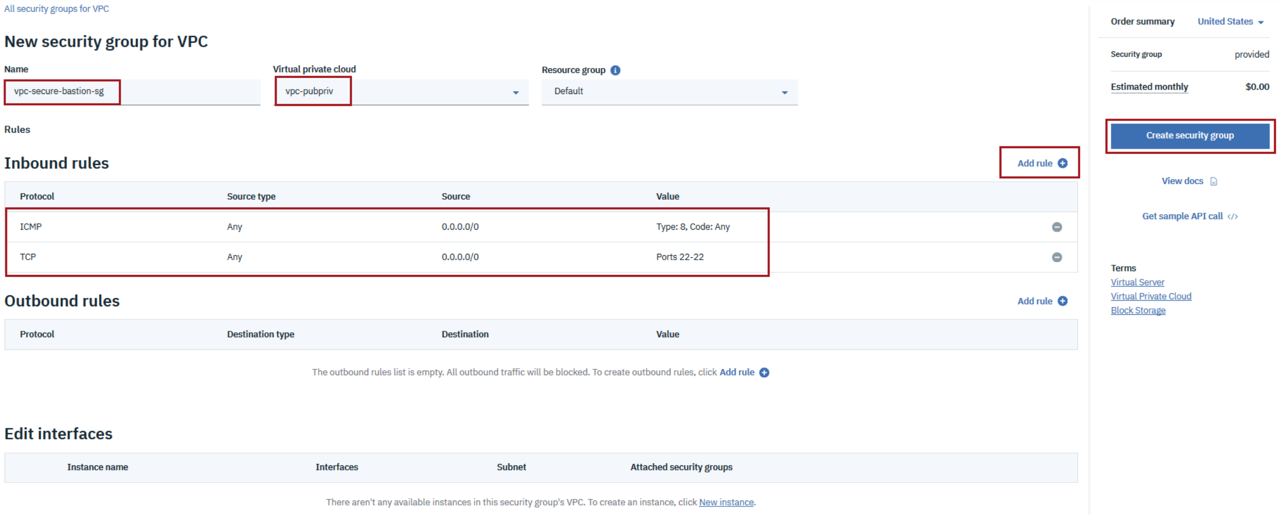
3. To enhance security further, the inbound traffic could be restricted to the company network or a typical home network. You could run `curl ipecho.net/plain ; echo` to obtain your network's external IP address and use that instead.
4. Click **Create security group** to create it.



Security groups for VPC

Name	Default	Resource Group	Virtual private cloud	Rules	Attached Interfaces
agonizing-edge-spyglass-elastic-colony	✓	Default	vpc-pubpriv	2	0

Data updated 10 seconds ago



All security groups for VPC

New security group for VPC

Name: vpc-secure-bastion-sg

Virtual private cloud: vpc-pubpriv

Resource group: Default

Rules

Inbound rules

Add rule

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

Outbound rules

Add rule

Protocol	Destination type	Destination	Value

The outbound rules list is empty. All outbound traffic will be blocked. To create outbound rules, click Add rule

Edit interfaces

Instance name	Interfaces	Subnet	Attached security groups

There aren't any available instances in this security group's VPC. To create an instance, click New instance.

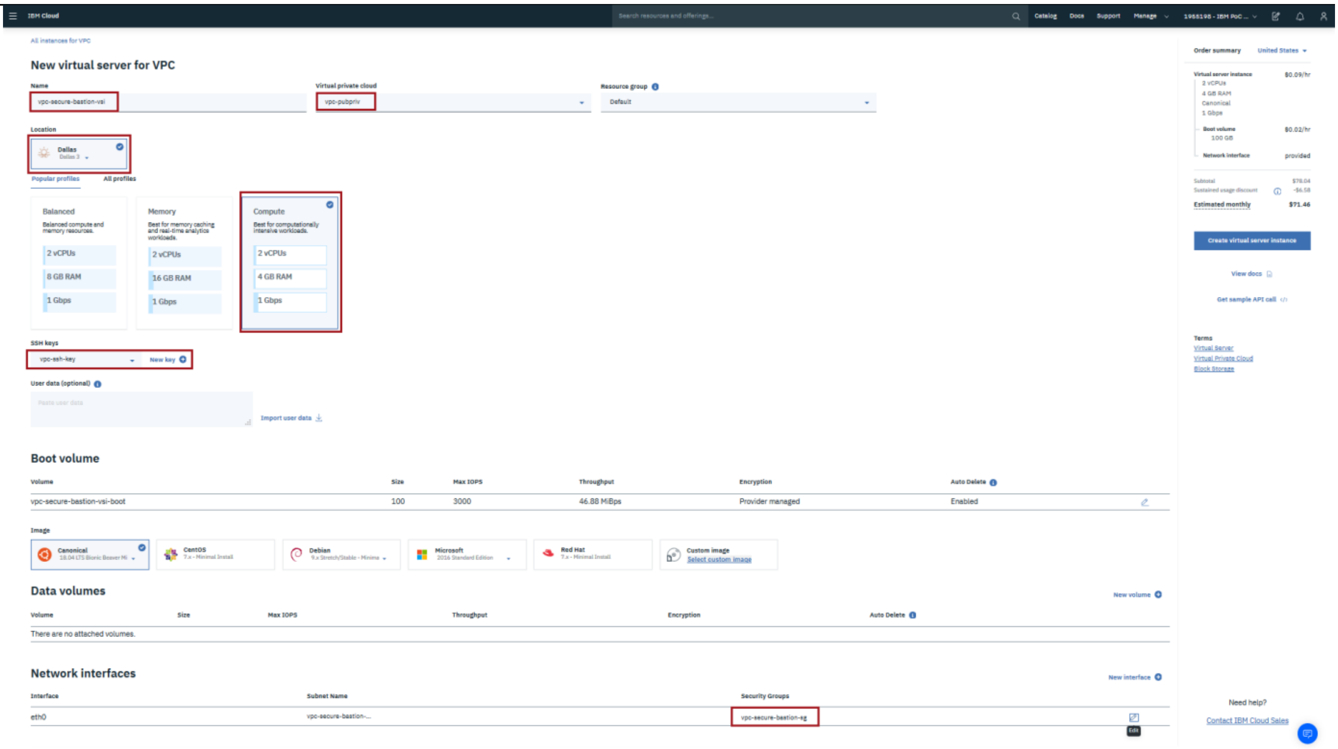
Order summary United States

Security group	provided
Estimated monthly	$0.00

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 **vpc-secure-bastion-subnet**.
2. Click on **Attached resources** and provision a **New instance** called **vpc-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. To create a new **SSH key**, click **New key**
   - Enter **vpc-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**.
6. Select **Ubuntu Linux** as your image. You can pick any version of the image.
7. Under **Network interfaces**, click on the **Edit** icon next to the Security Groups
   - Make sure that **vpc-secure-bastion-subnet** is selected as the subnet.
   - Uncheck the default security group and mark **vpc-secure-bastion-sg**.
   - Click **Save**.
8. Click **Create virtual server instance**.
9. Once the instance is created, click on **vpc-secure-bastion-vsi** and **reserve** a floating IP.



New virtual server for VPC

Name: vpc-secure-bastion-vsi

Virtual private cloud: vpc-pubpriv

Resource group: Default

Location: Dallas
Dallas 3

Balanced	Memory	Compute
Balanced compute and memory resources.	Best for memory caching and real-time analytics workloads.	Best for computationally intensive workloads.
2 vCPUs	2 vCPUs	2 vCPUs
8 GB RAM	16 GB RAM	4 GB RAM
1 Gbps	1 Gbps	1 Gbps

SSH keys: vpc-ssh-key

User data (optional): Paste user data

Boot volume

Volume	Size	Max IOPS	Throughput	Encryption	Auto Delete
vpc-secure-bastion-vsi-boot	100	3000	46.88 MiBps	Provider managed	Enabled

Image
- Canonical 18.04 LTS Bionic Beaver Mi
- CentOS 7.x - Minimal Install
- Debian 9.x Stretch/Stable - Minima
- Microsoft 2016 Standard Edition
- Red Hat 7.x - Minimal Install
- Custom image Select custom image

Data volumes

Volume	Size	Max IOPS	Throughput	Encryption	Auto Delete
There are no attached volumes.					

Network interfaces

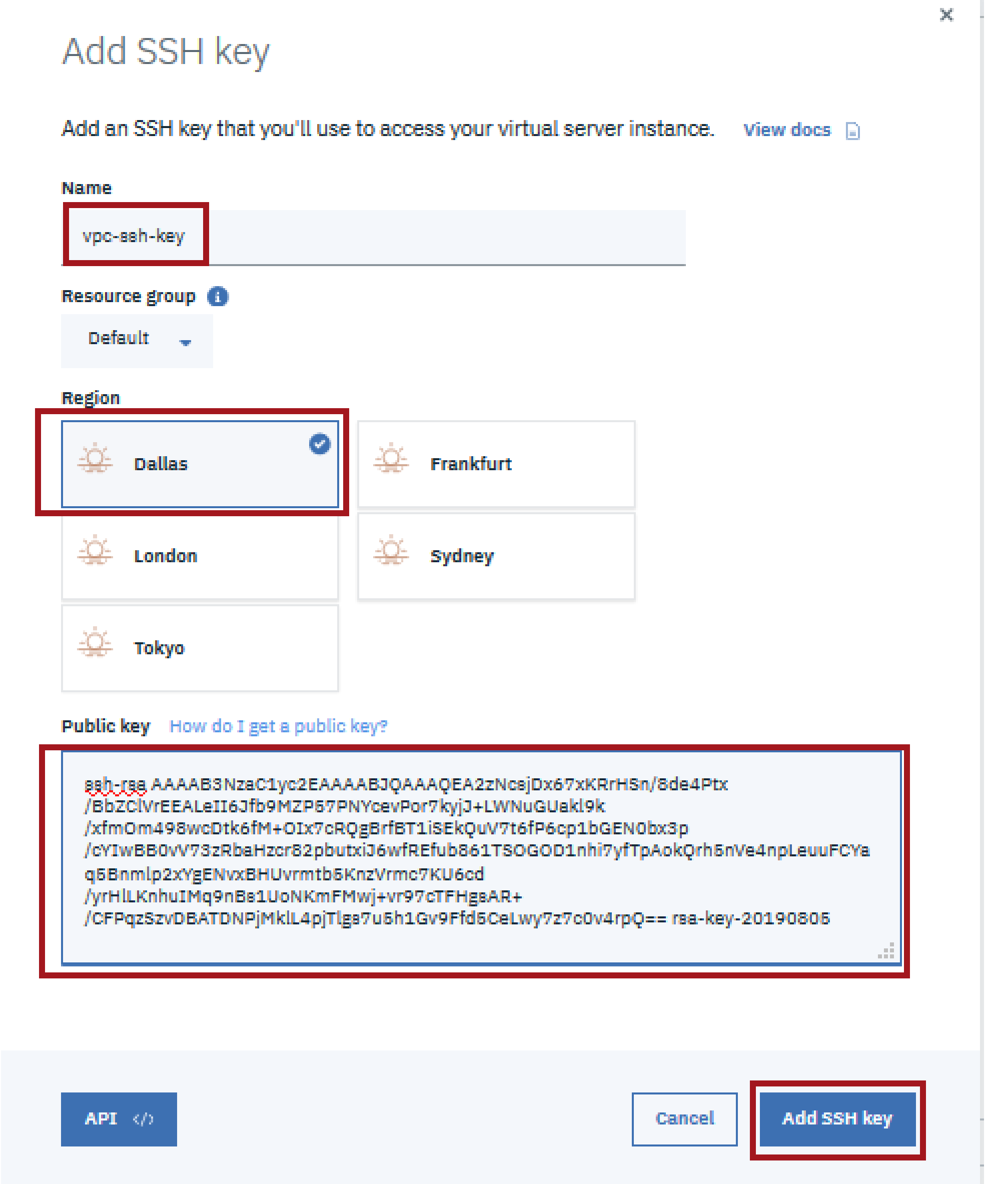
Interface	Subnet Name	Security Groups
eth0	vpc-secure-bastion-...	vpc-secure-bastion-sg

Order summary United States

Virtual server instance	$0.09/hr
2 vCPUs	
4 GB RAM	
Canonical	
1 Gbps	
Boot volume	$0.02/hr
100 GB	
Network interface	provided
Subtotal	$78.04
Sustained usage discount	-$6.58
Estimated monthly	$71.46

Terms
Virtual Server
Virtual Private Cloud
Block Storage

Need help?
Contact IBM Cloud Sales



Add SSH key

Add an SSH key that you'll use to access your virtual server instance.

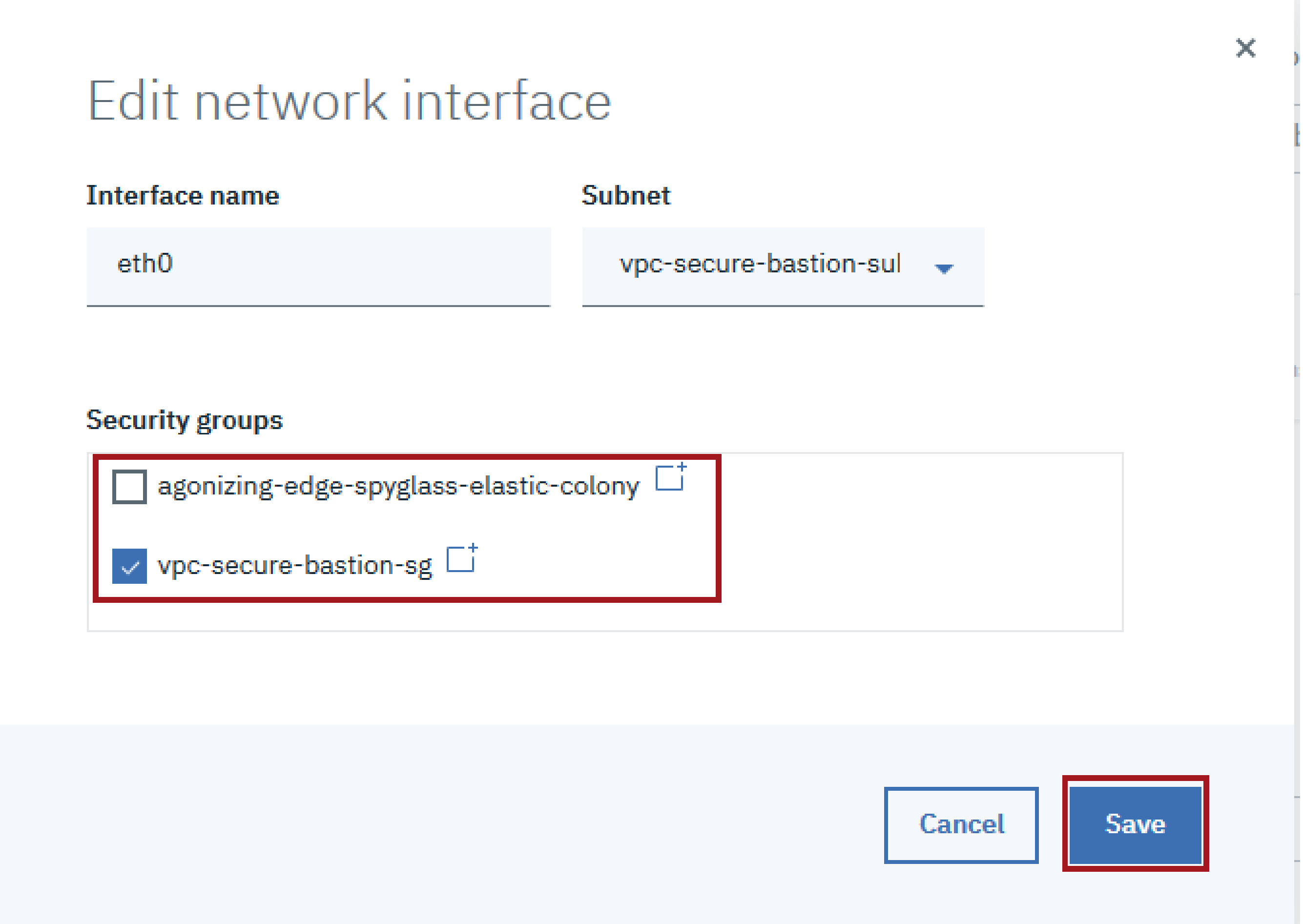
Name: vpc-ssh-key

Resource group: Default

Region: ☑ Dallas

Public key

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA2zNcsjDx67xKRrHSn/8de4Ptx
/BbZClVrEEALeII6Jfb9MZP57PNYcevPor7kyjJ+LWNuGUakl9k
/xfmOm498wcDtk6fM+OIx7cRQgBrfBT1iSEkQuV7t6fP6cp1bGEN0bx3p
/cYIwBB0vV73zRbaHzcr82pbutxiJ6wfREfub861TSOGOD1nhi7yfTpAokQrh5nVe4npLeuuFCYa
q5Bnmlp2xYgENvxBHUvrmtb5KnzVrmc7KU6cd
/yrHlLKnhuIMq9nBs1UoNKmFMwj+vr97cTFHgsAR+
/CFPqzSzvDBATDNPjMklL4pjTlgs7u5h1Gv9Ffd5CeLwy7z7c0v4rpQ== rsa-key-20190805
```



Edit network interface

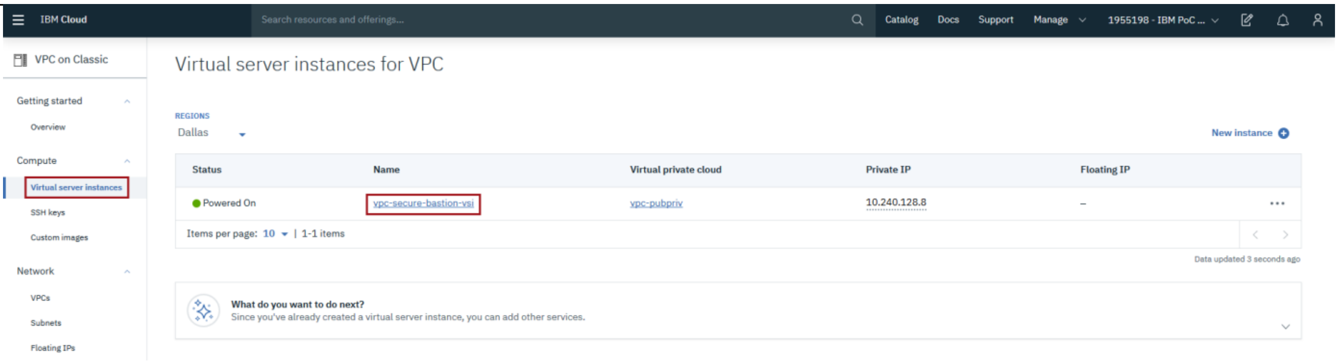
Interface name: eth0

Subnet: vpc-secure-bastion-sul

Security groups

☐ agonizing-edge-spyglass-elastic-colony

☑ vpc-secure-bastion-sg



Virtual server instances for VPC

REGIONS
Dallas

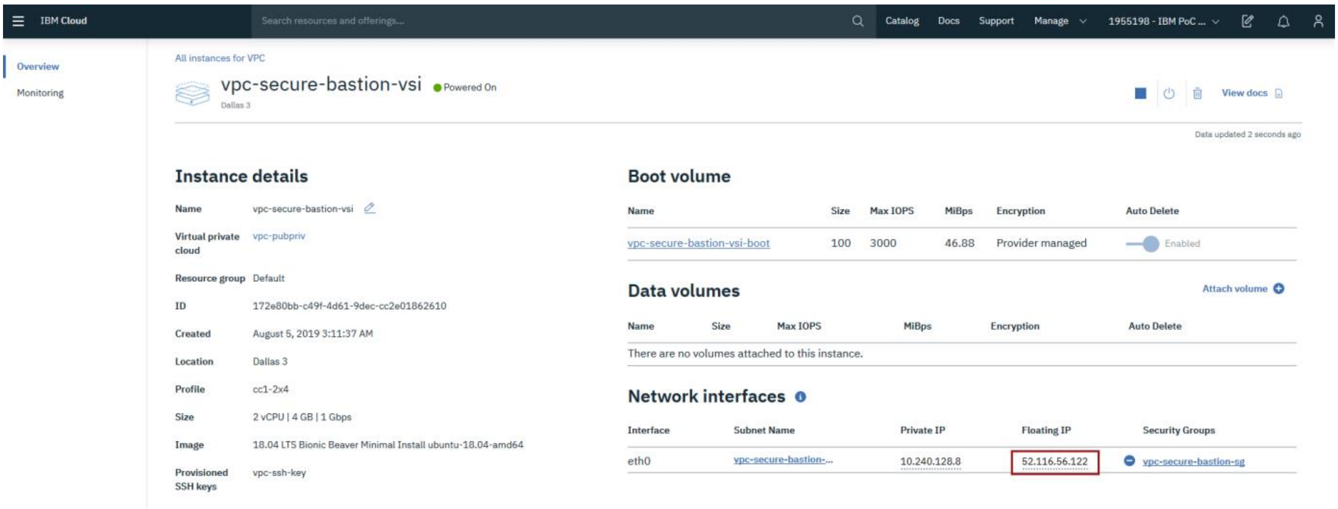
New instance

Status	Name	Virtual private cloud	Private IP	Floating IP
● Powered On	vpc-secure-bastion-vsi	vpc-pubpriv	10.240.128.8	–

Items per page: 10 | 1-1 items

Data updated 3 seconds ago

What do you want to do next?
Since you've already created a virtual server instance, you can add other services.



All instances for VPC

vpc-secure-bastion-vsi ● Powered On
Dallas 3

Data updated 2 seconds ago

Instance details

Name	vpc-secure-bastion-vsi
Virtual private cloud	vpc-pubpriv
Resource group	Default
ID	172e80bb-c49f-4d61-9dec-cc2e01862610
Created	August 5, 2019 3:11:37 AM
Location	Dallas 3
Profile	cc1-2x4
Size	2 vCPU | 4 GB | 1 Gbps
Image	18.04 LTS Bionic Beaver Minimal Install ubuntu-18.04-amd64
Provisioned SSH keys	vpc-ssh-key

Boot volume

Name	Size	Max IOPS	MiBps	Encryption	Auto Delete
vpc-secure-bastion-vsi-boot	100	3000	46.88	Provider managed	Enabled

Data volumes

Attach volume

Name	Size	Max IOPS	MiBps	Encryption	Auto Delete

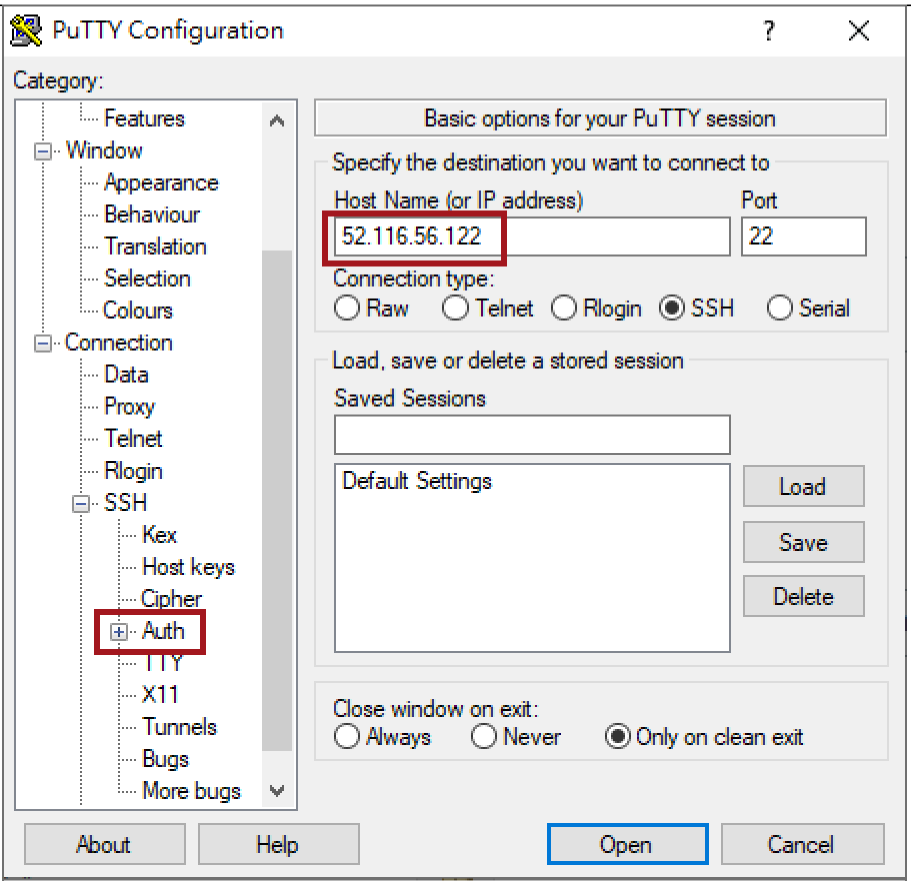
There are no volumes attached to this instance.

Network interfaces

Interface	Subnet Name	Private IP	Floating IP	Security Groups
eth0	vpc-secure-bastion-...	10.240.128.8	52.116.56.122	vpc-secure-bastion-sg

Test your bastion

Once your bastion's floating IP address is active, try connecting to it using ssh client



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 52.116.56.122

Port: 22

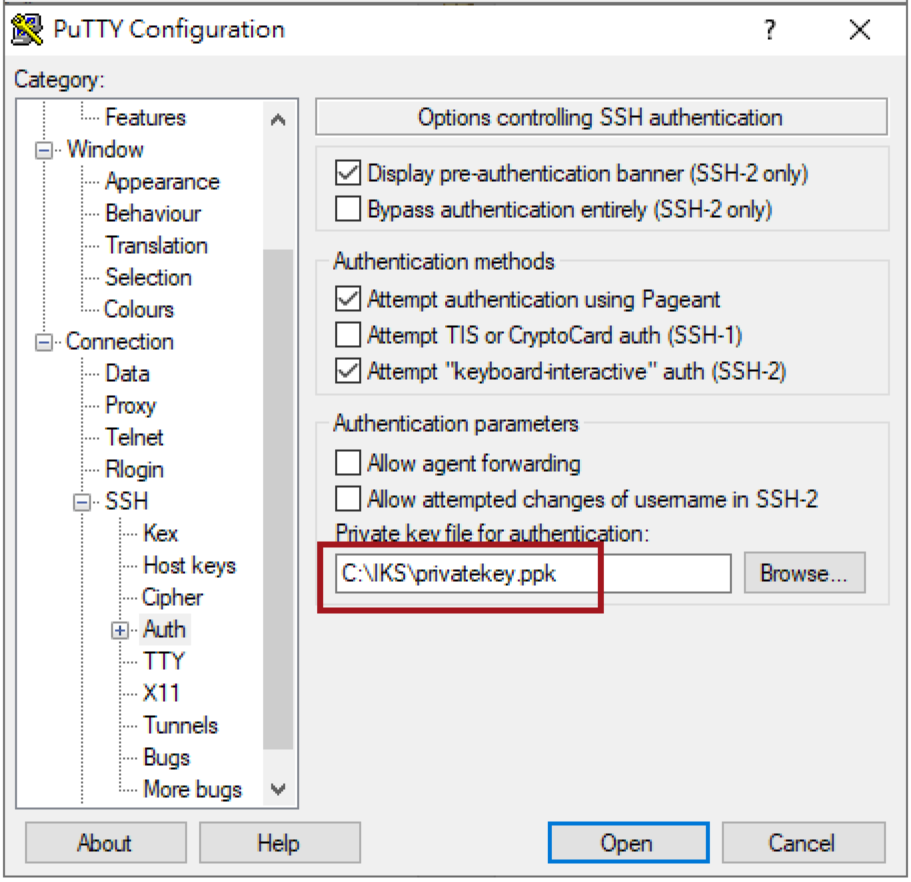
Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit



PuTTY Configuration

Category:

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
☐ Bypass authentication entirely (SSH-2 only)

Authentication methods

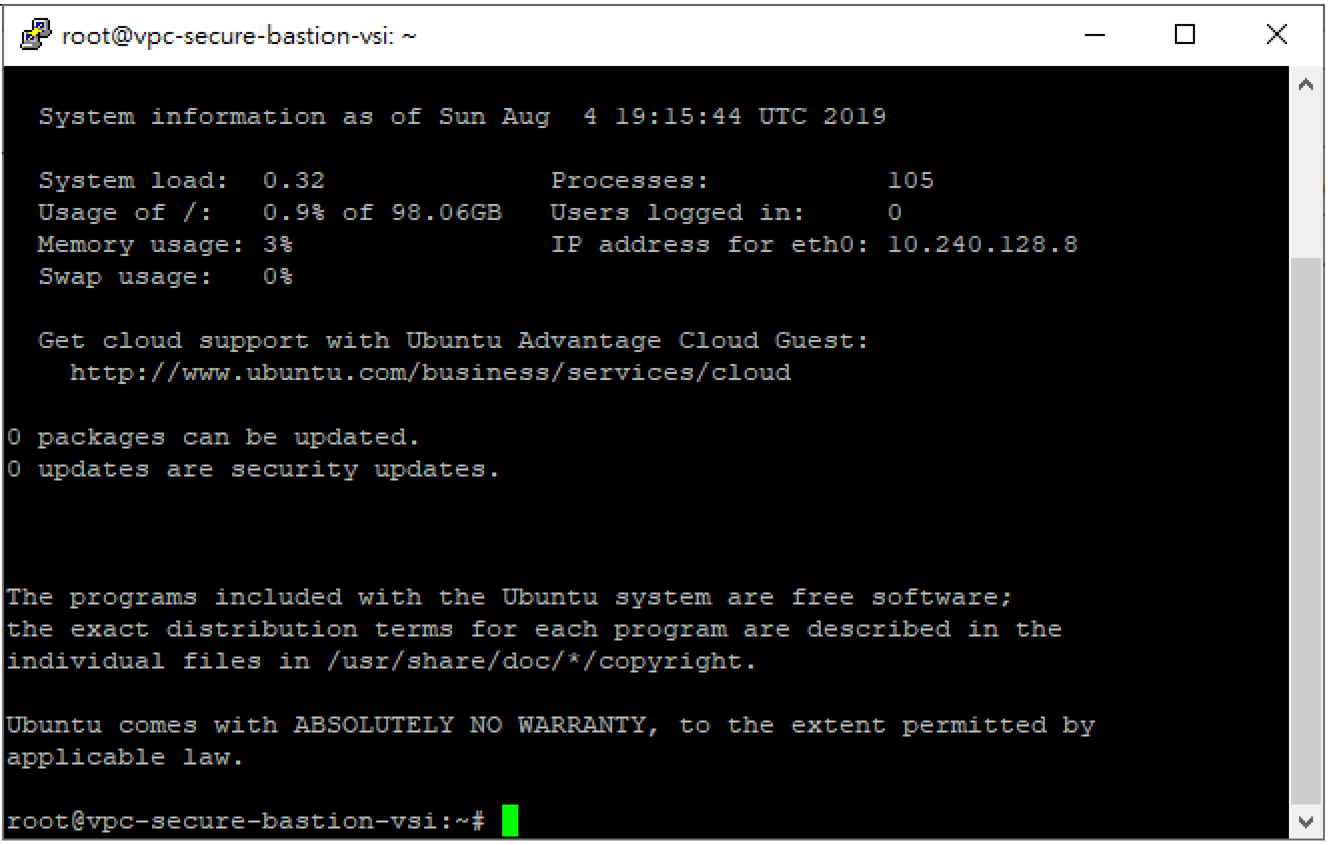
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

C:\IKS\privatekey.ppk



```
  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.

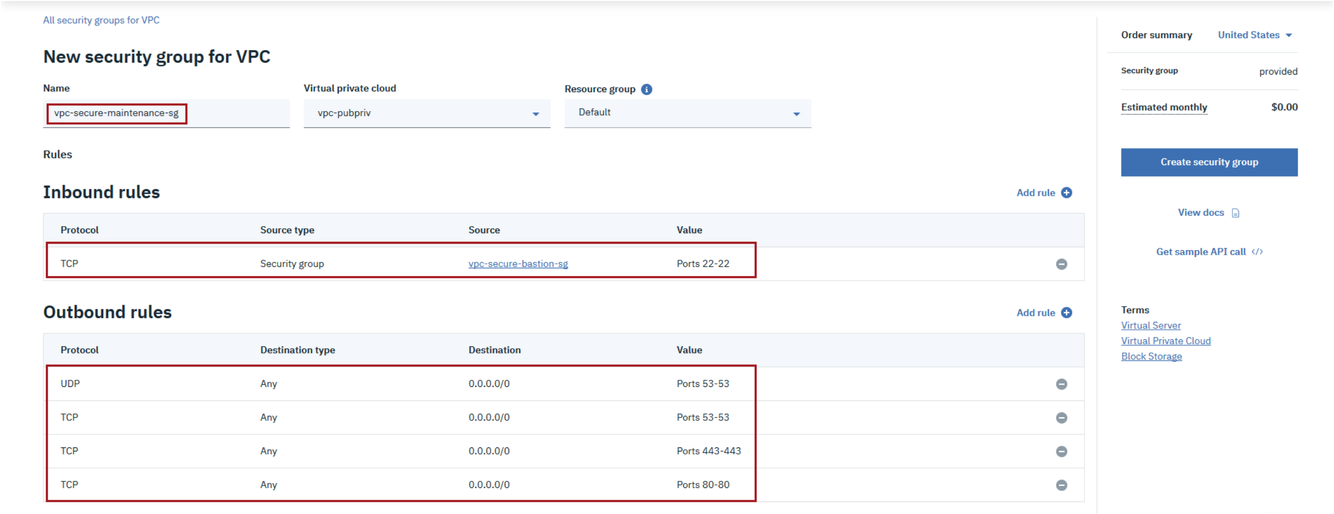
1. Navigate to **Security groups** and provision a new security group called **vpc-secure-maintenance-sg** with the below outbound rules

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	vpc-secure-bastion-sg	Ports 22-22

4. Create the security group.



All security groups for VPC

New security group for VPC

Name: vpc-secure-maintenance-sg

Virtual private cloud: vpc-pubpriv

Resource group: Default

Rules

Inbound rules

Add rule

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

Outbound rules

Add rule

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

Order summary United States

Security group provided

Estimated monthly $0.00

Create security group

View docs

Get sample API call

Terms

Virtual Server

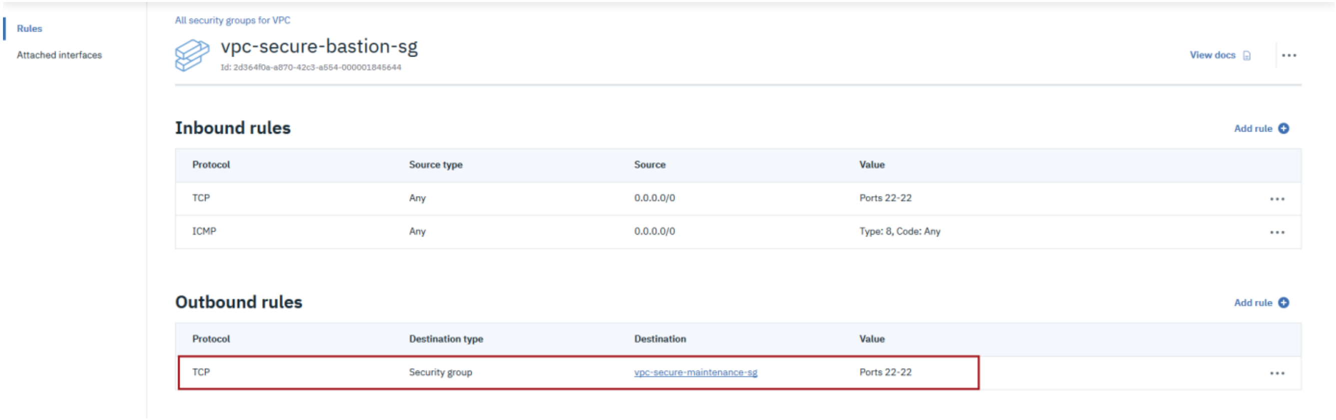
Virtual Private Cloud

Block Storage

5.
6. Navigate to **All Security Groups for VPC**, then select **vpc-secure-bastion-sg**.
7. 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

1.



Rules

Attached interfaces

All security groups for VPC

vpc-secure-bastion-sg

Id: 2d364f0a-a870-42c3-a554-000001845644

View docs

Inbound rules

Add 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: Any

Outbound rules

Add rule

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

2.

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 **vpc-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 **vpc-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 vpc-secure-bastion-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, **vpc-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 **vpc-secure-private-subnet** as the subnet.
   - Uncheck the default security and group and activate **vpc-secure-private-sg**.
   - Click **Save**.
9. Click **Create virtual server instance**.

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 **vpc-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 the ssh command with `-J` to log into the server with the bastion floating IP address you used earlier and the server Private IP address shown under Network interfaces.
3. `ssh -J root@<BASTION_FLOATING_IP_ADDRESS> root@<PRIVATE_IP_ADDRESS>`

`-J` flag is supported in OpenSSH version 7.3+. In older versions `-J` is not available. In this case the safest and most straightforward way is to use ssh's stdio forwarding (`-W`) mode to "bounce" the connection through a bastion host. e.g., `ssh -o ProxyCommand="ssh -W %h:%p root@<BASTION_FLOATING_IP_ADDRESS" root@<PRIVATE_IP_ADDRESS>`

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. First, update the software package information:
2.
3.
1. `apt-get update`
2.
3. Install the desired software, e.g., Nginx or MySQL or IBM Db2.

When done, disconnect from the server with `exit` command.

To allow HTTP/HTTPS requests from the internet user, assign a floating IP to the VSI in the private subnet and open required ports (80 - HTTP and 443 - HTTPS) via the inbound rules in the security group of private VSI.

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 **vpc-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. 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.
2. Once the VSIs are gone, switch to **Subnets** and delete your subnets.
3. After the subnets have been deleted, switch to the **Virtual private clouds** 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.

Create a backend subnet, security group and VSI

In this section, you will create a subnet, a security group and a virtual server instance for the backend.

Create a subnet for the backend

To create a new subnet for the backend,

1. Select **Subnets** under **Network** and click **New subnet**.
   - Enter **vpc-pubpriv-backend-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).
3. Click **Create subnet** to provision it.

Create a backend security group

The backend security group will allow to control the inbound and outbound connections for the backend servers.

To create a new security group for the backend:

1. Select **Security groups** under **Network**, then click **New security group**.
2. Enter **vpc-pubpriv-backend-sg** as name and select the VPC you created earlier.
3. Click **Create security group**.

You will later edit the security group to add the inbound and outbound rules.

Create a backend virtual server instance

To create a virtual server instance in the newly created subnet:

1. Click on the backend subnet under **Subnets**.

2. Click **Attached resources**, then **New instance**.
3. To configure the instance:
    1. Set the **name** to **vpc-pubpriv-backend-vsi**.
    2. Select the VPC you created and resource group as earlier.
    3. Select the same **Location** as before.
    4. Select **Compute** with 2vCPUs and 4 GB RAM as your profile.To check other available profiles, click **All profiles**
    5. Set **SSH keys** to the the SSH key you created earlier.
    6. Set **User data** to
    7.
    8.

3.

    6. `#!/bin/bash`
    7. `apt-get update`
    8. `apt-get install -y nginx`
    9. `echo "I'm the backend server" > /var/www/html/index.html`
    10. `service nginx start`
    11. This will install a simple web server into the instance.
    12. Set the **image** to **Ubuntu Linux**. You can pick any version of the image.
4. Under **Network interfaces**, click on the **Edit** icon next to the Security Groups

    - Select **vpc-pubpriv-backend-subnet** as the subnet.
    - Uncheck the default security group and check **vpc-pubpriv-backend-sg** and **vpc-secure-maintenance-sg**.
    - Click **Save**.
2. Click **Create virtual server instance**.

Create a frontend subnet, security group and VSI

Similar to the backend, you will create a frontend subnet with virtual server instance and a security group.

Create a subnet for the frontend

To create a new subnet for the frontend,

1. Select Subnets under **Network** and click **New subnet**.
    - Enter **vpc-pubpriv-frontend-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.2.0/24**. 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. Given all virtual server instances in the frontend subnet will have a floating IP attached, it is not required to enable a public gateway for the subnet. The virtual server instances will have Internet connectivity through their floating IP.
4. Click **Create subnet** to provision it.

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 **vpc-pubpriv-frontend-sg** as name and select the VPC you created earlier.
3. Click **Create security group**.

Create a frontend virtual server instance

To create a virtual server instance in the newly created subnet:

1. Click on the frontend subnet under **Subnets**.
2. Click **Attached resources**, then **New instance**.
3. To configure the instance:
    1. Set the **name** to **vpc-pubpriv-frontend-vsi**.
    2. Select the VPC you created and resource group as earlier.
    3. Select the same **Location** as before.
    4. Select **Compute** with 2vCPUs and 4 GB RAM as your profile. To check other available profiles, click **All profiles**
    5. Set **SSH keys** to the the SSH key you created earlier.
    6. Set **User data** to
    7.
    8.

3.

```
6. #!/bin/bash
7. apt-get update
8. apt-get install -y nginx
9. echo "I'm the frontend server" > /var/www/html/index.html
10.service nginx start
```

11. This will install a simple web server into the instance.
12. Set the **image** to **Ubuntu Linux**. You can pick any version of the image.

4. Under **Network interfaces**, click on the **Edit** icon next to the Security Groups
    - Select **vpc-pubpriv-frontend-subnet** as the subnet.
    - Uncheck the default security and group and activate **vpc-pubpriv-frontend-sg** and **vpc-secure-maintenance-sg**.
    - Click **Save**.
    - Click **Create virtual server instance**.

2. Select the frontend VSI **vpc-pubpriv-frontend-vsi**, scroll to **Network Interfaces** and click **Reserve** under **Floating IP** to associate a public IP address to your frontend VSI. Save the associated IP Address to a clipboard for future reference.

Set up connectivity between frontend and backend

With all servers running, in this section you will set up the connectivity to allow regular operations between the frontend and backend servers.

Configure the frontend security group

The frontend instance has its software installed but it can not yet be reached.

1. To confirm the web server can not yet be accessed, open a web browser pointing to `http://<floating-ip-address-of-the-frontend-vsi>` or use:
2.
3.
1. `curl -v -m 30 http://<floating-ip-address-of-the-frontend-vsi>`
2. The connection should time out eventually.
3. To enable inbound connection to the web server installed on the frontend instance, you need to open the port where the web server is listening on.
4. Navigate to **Security groups** in the **Network** section, then click on **vpc-pubpriv-frontend-sg**.
5. First, add the following **inbound** rules using **Add rule**. They allow incoming HTTP requests and Ping (ICMP).

Protocol	Source type	Source	Value	Description
TCP	Any	0.0.0.0/0	Ports 22-22	This rule allows connections from any IP address to the frontend web server.
ICMP	Any	0.0.0.0/0	Type: **8**,Code: **Leave empty**	This rule allows the frontend server to be pinged by any host.

6. Next, add this **outbound** rule.

Protocol	Destination type	Destination	Value	Description
TCP	Any	0.0.0.0/0	Ports 80-80	This rule allows the frontend server to communicate with the backend server.

7. The port of the backend depends on the software you are installing on the virtual server. This tutorial uses a web server listening on port 80.
8. Access the frontend instance again at `http://<floating-ip-address-of-the-frontend-vsi>` to view the welcome page of the web server.

Test the connectivity between the frontend and the backend

The backend server is running the same web server software than the frontend server. It could be considered as a microservice exposing an HTTP interface that the frontend would be calling. In this section, you will attempt to connect to the backend from the frontend server instance.

1. In the Virtual Server Instances list, retrieve the floating IP address of the bastion server host (**vpc-secure-bastion**) and the private IP addresses of the frontend (**vpc-pubpriv-frontend-vsi**) and backend (**vpc-pubpriv-backend-vsi**) server instances.
2. Use `ssh` to connect to the frontend virtual server:
3.

4.
2. `ssh -J root@<floating-ip-address-of-the-bastion-vsi> root@<private-ip-address-of-the-frontend-vsi>`
3.
4. Call the backend web server:
5. `curl -v -m 30 http://<private-ip-address-of-the-backend-vsi>`

   After 30 seconds, the call should timeout. Indeed, the security group for the backend server has not yet been configured and is not allowing any inbound connection.

Configure the backend security group

To allow inbound connections to the backend server, you need to configure the associated security group.

1. Navigate to **Security groups** in the **Network** section, then click on **vpc-pubpriv-backend-sg**.
2. Add the following **inbound** rule using **Add rule**.

Protocol	Source type	Source	Value	Description
TCP	Security group	vpc-pubpriv-frontend-sg	Ports 80-80	This rule allows incoming connections on port 80 from the frontend server to the backend server.

Confirm the connectivity

1. Call the backend web server from the frontend server again:
2. `curl -v -m 30 http://<private-ip-address-of-the-backend-vsi>`
3. The request returns quickly and outputs the message `I'm the backend server` from the backend web server. This completes the configuration of the connectivity between the servers.

Complete the maintenance

With the frontend and backend server software properly installed and working, the servers can be removed from the maintenance security group.

1. Navigate to **Security groups** in the **Network** section, then click on **vpc-secure-maintenance-sg**.
2. Select **Attached interfaces**.
3. **Edit interfaces** and uncheck the **vpc-pubpriv-frontend-vsi** and **vpc-pubpriv-backend-vsi** interfaces.
4. **Save** the configuration.
5. Access the frontend instance again at `http://<floating-ip-address-of-the-frontend-vsi>` to confirm it is still working as expected.

Once the servers are removed from the maintenance group, they can no longer be accessed with `ssh`. They will only allow traffic to their web servers.

In this tutorial, you deployed two tiers of an application, one frontend server visible from the public Internet and one backend server only accessible within the VPC by the frontend server. You configured security group rules to ensure traffic would be allowed only the specific ports required by the application.

Remove resources

1. 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.
2. 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.
3. 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.
4. 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.

Appendix

Setting up access to your Classic Infrastructure from VPC

Pre-requisites:

1. Your classic account must be linked to your IBM Cloud account. See Linking IBMid accounts for instructions on how to do this.
2. Your classic account must be enabled for VRF.
   - If you already have Direct Link on your account, you are ready.
   - If your account is not VRF-enabled, open a ticket to request "VRF Migration" for your account. See Converting to VRF to learn more about the conversion process.

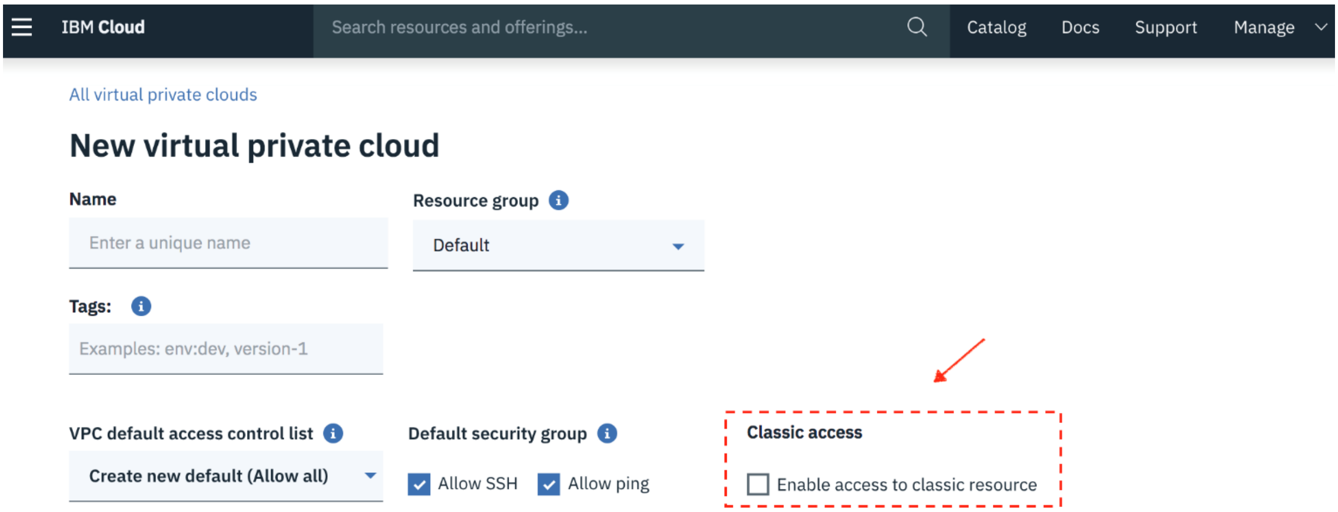
Create a Classic Access VPC

You can create a VPC with Classic Access capability by using the User Interface (UI), Command Line Interface (CLI), or Application Programming Interface (API).

A VPC must be set up for Classic Access when it's created: you cannot update a VPC to add or remove the Classic Access capability.

Create a Classic Access VPC from the User Interface

Create a Classic Access VPC from the **Create VPC** page, by clicking on the checkbox titled **Enable access to classic resource**, under the **Classic access** label.



All virtual private clouds

New virtual private cloud

Name: Enter a unique name

Resource group: Default

Tags: Examples: env:dev, version-1

VPC default access control list: Create new default (Allow all)

Default security group: ☑ Allow SSH ☑ Allow ping

Classic access: □ Enable access to classic resource

How to initiate VRF conversion

To request conversion of your account to VRF, follow these steps:

1. Open a support case through the IBM Cloud console.
2. Select "Technical" for the type of support needed and "VPC Network" for the category.
3. Enter "Convert account to VRF for VPC Classic Access" as the subject.
4. For the description, enter the following text: "We are requesting that account *your account number* is moved to its own VRF. We understand the risks and approve the change. Please reply with the scheduled window(s) of time where this change will be made so we can prepare for the migration."

Migration is completed by the IBM Cloud Network Engineering team. No other information is required from you, except an agreed-to schedule. Typically, packet loss might last 15 - 30 minutes, depending on the complexity of your account. It might be longer if your account has legacy Direct Link connections. The process is highly automated, requiring minimal interaction by the IBM team, and it should be transparent.