



# IBM Cloud 用戶實作研習營

## IBM Cloud Virtual Private Cloud (VPC) 使用教學

2019/8/7



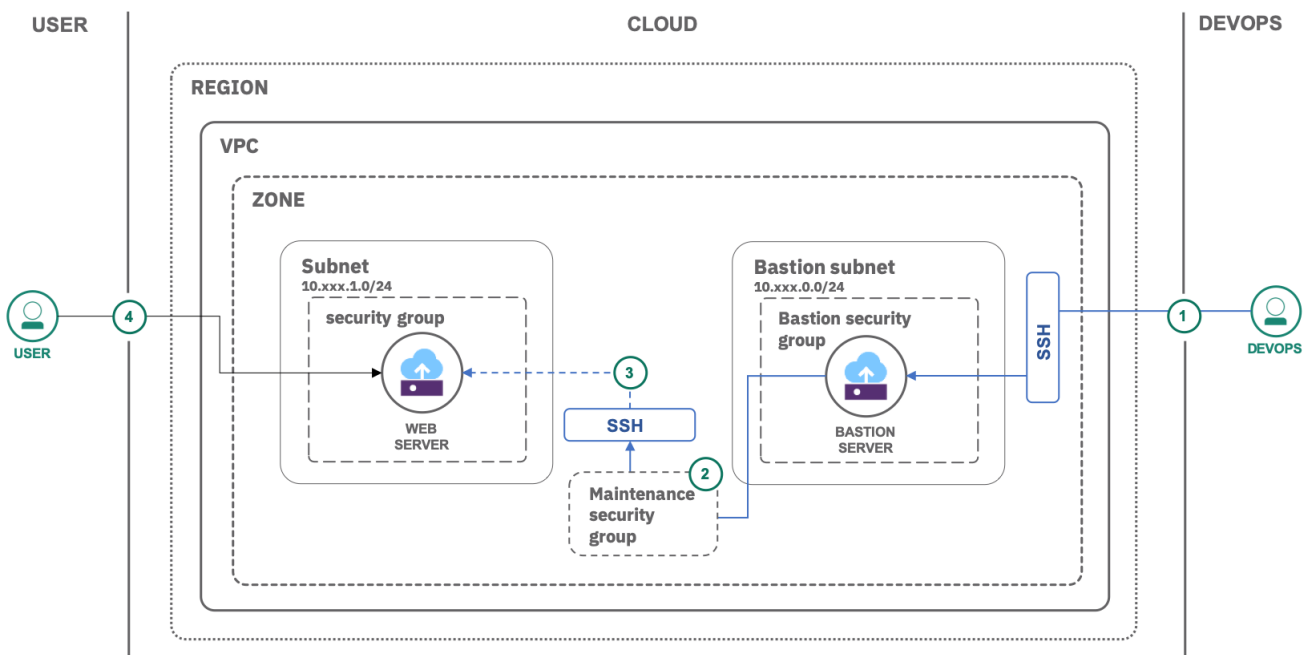
# Securely access remote instances with a bastion host

- 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:
  - o Enter `wk1000vpc-pubpriv` as name for your VPC.
  - o Select a **Resource group**.
  - o 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**:
  - o As a unique name enter `wk1000vpc-secure-bastion-subnet`.
  - o Select a location.
  - o 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**.



IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage

1955198 - IBM PoC ...

All virtual private clouds

New virtual private cloud

Name

vpc-pubpriv

Resource group

Default

Tags

Examples: envdev, 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

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

☐ 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

IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage

1955198 - IBM PoC ...

VPC on Classic

Virtual private cloud

REGIONS

Dallas

| Status    | Name        | Resource group | Subnets | Default ACL  | Default Security Group                  |
|-----------|-------------|----------------|---------|--|---|
| Available | vpc-pubpriv | Default        | 1       | allow-all-network-acl-584cd078-59bf-4725-b99b-644ef6595677 | agorizing-edge-ipv4glass-elastic-colony |

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**.

IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage

1955198 - IBM PoC ...

VPC on Classic

Subnets for VPC

REGIONS

Dallas

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

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 **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.

The screenshot shows the 'Security groups for VPC' page in the IBM Cloud console. The left sidebar contains a navigation menu with 'Security groups' highlighted. The main content area shows a table of existing security groups. A 'New security group' button is located in the top right corner of the table area.

The screenshot shows the 'New security group for VPC' form. The 'Name' field is 'vpc-secure-bastion-sg', 'Virtual private cloud' is 'vpc-pubpriv', and 'Resource group' is 'Default'. The 'Inbound rules' section shows two rules: ICMP (Type: 8, Code: Any) and TCP (Ports 22-22). The 'Add rule' button is highlighted in the top right corner of the rules section.

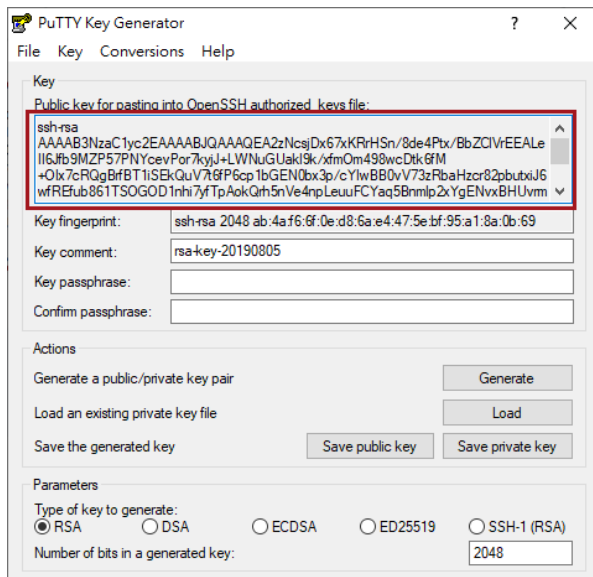
## Create a bastion instance

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**
  - o Enter **wk1000vpc-ssh-key** as key name.
  - o Leave the **Region** as is.
  - o Copy the contents of your existing local SSH key and paste it under **Public key**.
  - o 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
  - o Make sure that **wk1000vpc-secure-bastion-subnet** is selected as the subnet.
  - o Uncheck the default security group and mark **wk1000vpc-secure-bastion-sg**.
  - o Click **Save**.
9. Click **Create virtual server instance**.



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

IBM Cloud

Search resources and offerings...

Catalog

Docs

Support

Manage

1955198 - IBM PoC ...

Overview

Monitoring

All instances for VPC

vpc-secure-bastion-vsi

Powered On

View docs

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

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-...

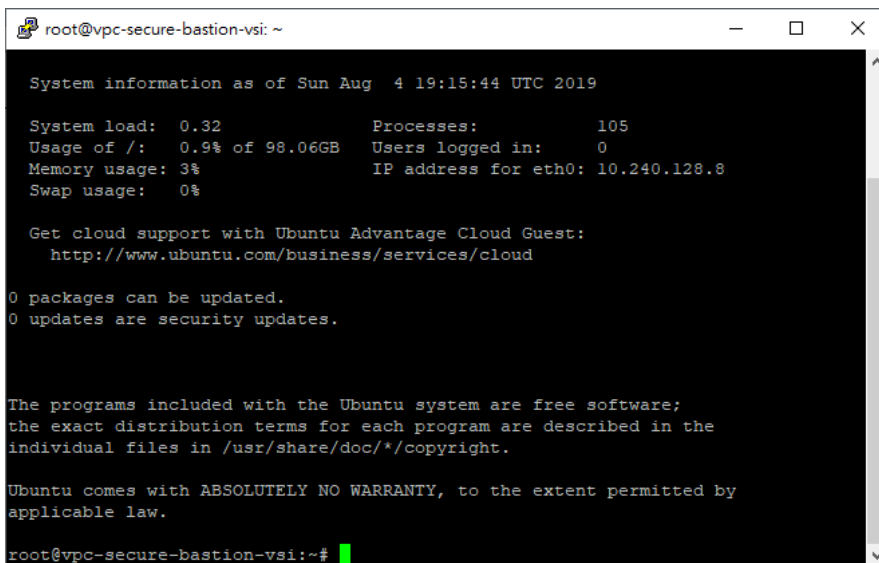
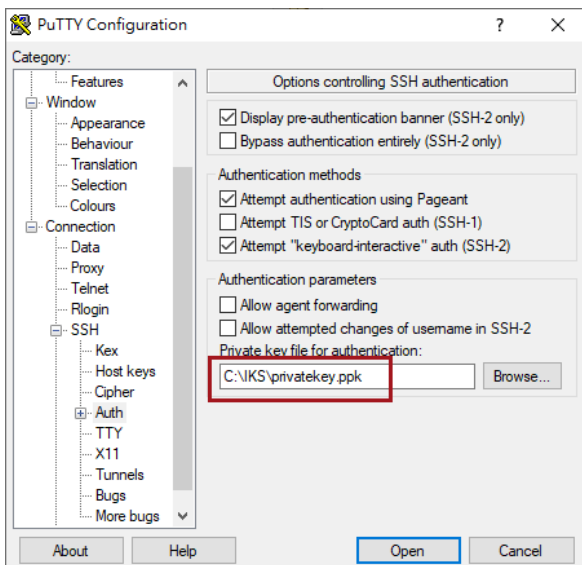
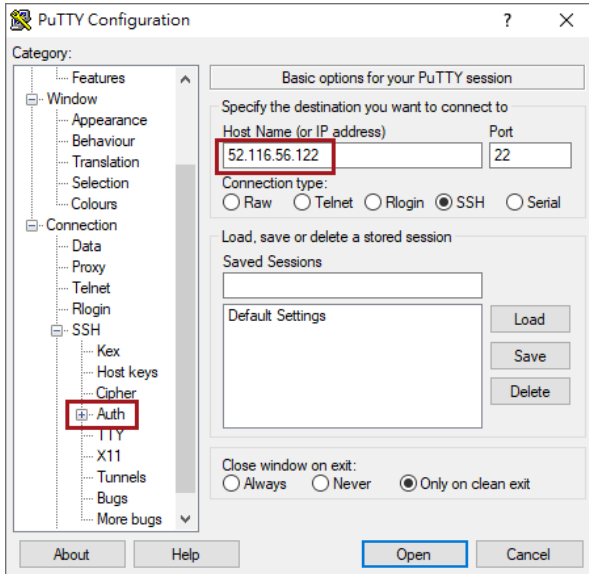
10.240.128.8

52.116.56.122

vpc-secure-bastion-ig

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







## 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.

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

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

#### Outbound rules

| 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. 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 |



Rules

Attached interfaces

All security groups for VPC

**vpc-secure-bastion-sg**  
Id: 2d3564f0a-e879-42c3-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   | <a href="#">vpc-secure-maintenance-sg</a> | 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,

- 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.
- Select **VPC default** for your subnet access control list (ACL). You can configure the inbound and outbound rules later.
- Switch the **Public gateway** to **Attached**.
- Click **Create subnet** to provision it.



VPC on Classic

Getting started

Overview

Compute

Virtual server instances

SSH keys

Custom images

Network

VPCs

Subnets

Floating IPs

Public gateways

Access control lists

Security groups

VPNs

Load balancers

Subnets for VPC

REGIONS

Dallas

New subnet

| Status    | Subnets                                   | Virtual private cloud       | Location | IP Range        | Public Gateway |
|-----------|---|-----------------------------|----------|-----------------|----------------|
| Available | <a href="#">vpc-secure-bastion-subnet</a> | <a href="#">vpc-pubpriv</a> | Dallas 3 | 10.240.128.0/24 | —              |

Items per page: 10 | 1-1 items

Data updated 23 seconds ago

What do you want to do next?

Since you've already created a subnet, you can add other services.

All subnets for VPC

New subnet for VPC

Name

vpc-secure-private-subnet

Virtual private cloud

vpc-pubpriv

Location

Dallas

IP range

10.240.129.0/24

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

VPC Default(allow-all-network-acl-584cd078-5f81-4225-8b9b-644ef6595677)

Public gateway

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

Detached

Attached

Order summary

United States

Subnet

provided

Estimated monthly

\$0.00

Create subnet

View docs

Get sample API call

Terms

[Virtual Server](#)
[Virtual Private Cloud](#)
[Block Storage](#)

## 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**.

VPC on Classic

Getting started

Overview

Compute

Virtual server instances

SSH keys

Custom images

Network

VPCs

Subnets

Floating IPs

Public gateways

Access control lists

Security groups

VPNs

Load balancers

Security groups for VPC

REGIONS

Dallas

New security group

| Name   | Default | Resource Group | Virtual private cloud       | Rules | Attached Interfaces |
|--|---------|----------------|-----------------------------|-------|---------------------|
| <a href="#">agonizing-edge-spyglass-elastic-colony</a> | ✓       | —              | <a href="#">vpc-pubpriv</a> | 2     | 0                   |
| <a href="#">vpc-secure-bastion-sg</a>                  | —       | —              | <a href="#">vpc-pubpriv</a> | 3     | 1                   |
| <a href="#">vpc-secure-maintenance-sg</a>              | —       | —              | <a href="#">vpc-pubpriv</a> | 5     | 0                   |

Data updated 8 seconds ago



All security groups for VPC

## New security group for VPC

Name  Virtual private cloud  Resource group

Rules

### Inbound rules

| Protocol | Source type | Source | Value |
|----------|-------------|--------|-------|
|----------|-------------|--------|-------|

The inbound rules list is empty. All inbound traffic will be blocked. To create inbound rules, click [Add rule](#)

### Outbound rules

| Protocol | Destination type | Destination | Value |
|----------|------------------|-------------|-------|
|----------|------------------|-------------|-------|

The outbound rules list is empty. All outbound traffic will be blocked. To create outbound rules, click [Add rule](#)

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](#)

## 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 you 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
  - o Select **wk1000vpc-secure-private-subnet** as the subnet.
  - o Uncheck the default security and group and activate **wk1000vpc-secure-private-sg**.
  - o Click **Save**.
9. Click **Create virtual server instance**.

VPC on Classic

Getting started

Overview

Compute

Virtual server instances

SSH keys

Custom images

Network

VPCs

Subnets

Floating IPs

Public gateways

Access control lists

Security groups

VPNs

Subnets for VPC

REGIONS

Dallas

New subnet

| Status    | Subnets                                   | Virtual private cloud | Location | IP Range        | Public Gateway |
|-----------|---|-----------------------|----------|-----------------|----------------|
| Available | <a href="#">vpc-secure-bastion-subnet</a> | vpc-pubpriv           | Dallas 3 | 10.240.128.0/24 | —              |
| Available | <a href="#">vpc-secure-private-subnet</a> | vpc-pubpriv           | Dallas 3 | 10.240.129.0/24 | \$2.116.56.22  |

Items per page: 10 | 1-2 items

Data updated 22 seconds ago

What do you want to do next?

Since you've already created a subnet, you can add other services.





# 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.

Security groups for VPC

| Name                                   | Default                             | Resource Group | Virtual private cloud | Rules | Attached Interfaces |
|--|-------------------------------------|----------------|-----------------------|-------|---------------------|
| agonizing-edge-spyglass-elastic-colony | <input checked="" type="checkbox"/> | Default        | vpc-publicly          | 2     | 0                   |
| vpc-secure-bastion-sg                  | <input type="checkbox"/>            | Default        | vpc-publicly          | 3     | 1                   |
| <b>vpc-secure-maintenance-sg</b>       | <input type="checkbox"/>            | Default        | vpc-publicly          | 5     | 0                   |
| vpc-secure-private-sg                  | <input type="checkbox"/>            | Default        | vpc-publicly          | 0     | 0                   |

Data updated 26 seconds ago

Rules

Attached interfaces

All security groups for VPC

**vpc-secure-maintenance-sg**  
Id: 2d364f0e-e870-42c3-a554-000001845488

View docs

Attached interfaces

| Instance name | Interfaces | Subnet | Attached security groups |
|---------------|------------|--------|--------------------------|
|---------------|------------|--------|--------------------------|

The Attached interfaces list is empty. To attach interfaces, click [Edit interfaces](#).

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

Rules

Attached interfaces

All security groups for VPC

**vpc-secure-maintenance-sg**  
Id: 2d364f0e-e870-42c3-a554-000001845488

View docs

Attached interfaces

Editing items

| Instance name  | Interfaces                               | Subnet                    | Attached security groups |
|--|--|---------------------------|--------------------------|
| <input checked="" type="checkbox"/> vpc-secure-bastion-vs1 | <input checked="" type="checkbox"/> eth0 | vpc-secure-bastion-subnet | vpc-secure-bastion-sg    |
| <input checked="" type="checkbox"/> vpc-secure-private-vs1 | <input checked="" type="checkbox"/> eth0 | vpc-secure-private-subnet | vpc-secure-private-sg    |

Cancel Save

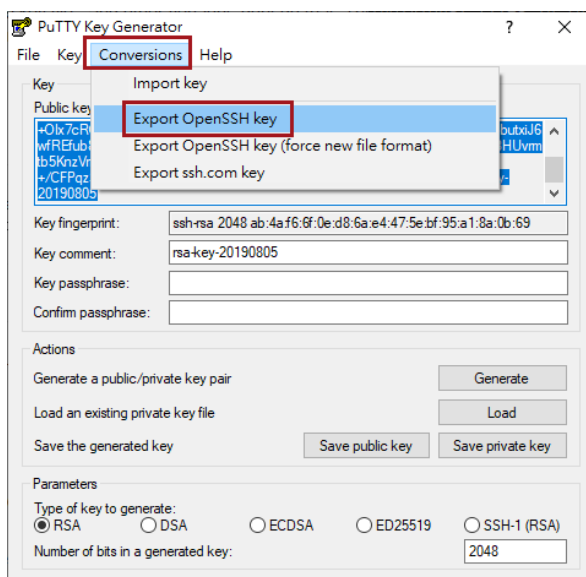


- Click **Save** for the changes to be applied.

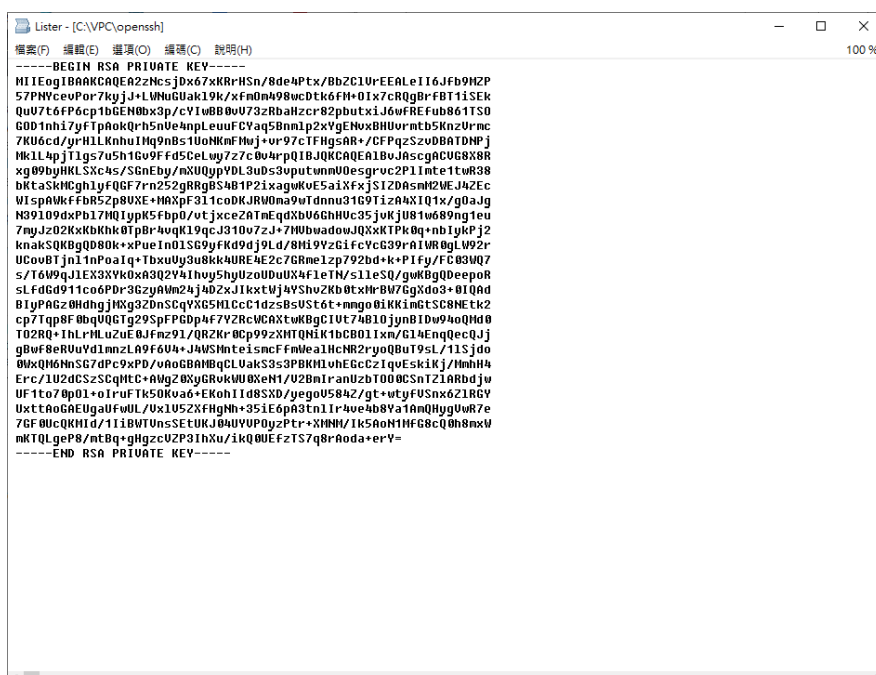
## Connect to the instance

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


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



- Copy the key content and create private key file on the bastion host





 root@vpc-secure-bastion-vsi: ~

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

```

root@vpc-secure-bastion-vsi: ~
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEa2zNcsjDx67xKRrHsn/8de4Ptx/BbZClVrEEALeII6Jfb9MZP
57PNVceyPor7kyjJ+LWNuGuakl9k/xfmOm498wcdtk6fM+OIx7cRQgBrfBT1iSEK
QuV76tfP6cp1bGEN0bX3p/cYIwBB0vV73zRbaHzer82pbuxiJ6vfrREfub861TSO
GODlnhi7yftPakQrh5nVe4npLuuFCYaq5Bnm1p2xYgENvxBHUVrmtb5KznZVrnc
7KU6cd/yrHlKnhuIMq9nBslUoNkMfMw+vr97cTFHgsAR+/CFPqzSzvDBATDNPj
Mkl14qyPTlgs7u5hlgV9Ffd5CeLwy7z7c0v4rpQIBJQKCAQEALbVasJAcgACVG8X8R
xg09byHKL5Xc4s/SGnEby/mXUQyupYDL3uDs3vputwmmVoesgrvc2P1TmteltwR38
bKtaSkMcghlyfQGF7rn252gRRgBS4B1P2ixagKvE5aiXfxjSIZDasm2WEJ4ZEc
WIsapAwkfrB5Zp8VXE+MAXpF31lcoDKJRWoma9wDnnu3lG9T1z44XlQ1x/gOaJg
N3919ldxpd1b7MQIypK5fbp0/vtjxceZATmEqdB6vGhHVC35jvKbU8lhw689ng1eu
7myJz02KxbKhk0tpBr4vgKl9qcJ3l0v7zJ+7MvBowadogJQXxKtPK0q+nbyIkWp2
kna3Q08KqD80k+xPueInOlSG9yfkGd9d9ld/8M49YzG1fcYcG39rAIWR80J9g9r
UCovBTjnl1nPoaIq+TbxuVy3u8kk4URE4E2c7GRmelzpj792bd4k+PiFy/FC03WQ7
s/T6w9qclEX3XyXoA3Q2Y4IInvy5hyUzoUDuUX4f1eTN/s1leSQ/gwKBgQDeepoR
sLfEdgd91lco6PDR3GzyAWm24j4DZxJIkxtWj4YShvZKb0ctMrBW7GqXdo3+0IOAD
BiYPAGzOHdhgjMXg3ZDnSCqYXG5M1CcClDzsBsVSt6t+mmgo01KKimGtSC8NEk2
cpT7qp8F0hgVQGTg29SpFPgDp4f7YZrCWCAxtwKBgCIvT74Bl0JxmBiDw94oQmD0
TO2Ro+IHlRmLuZuE0fjmfz9l/QRZKr0Cp99zXMTQmIKlBcB0lIxm/Gl4EnqQcQJj
qBwBf8erVuYdlmnzLA9f6V4+J4WSMnteismcFmFweAlHcNR2ryoQ0BtT9sL/1lSjd4
0WxQM6NnSG7dPc9xPD/vaAGBAMBqCLVakS3s3PBfM1vwEGGcZzqvEskiKj/MmhH0
Urc/1U24CSzSCqMtC+AWgZ0XyGRvKwUOXeN1/V2EmIraNuzbTOOOCsNtZlARbdjw
Uflto70pOl+oIruFTk50Kva6+EKohIId8SKD/yegoV584Z/gt+wtYfVsnx6Z1RGY
UxttAoAGeUgaUfUUL/Vx1V5ZxfHgNh+35iE6Pa3tnlIr4ve4b8YalAmQHygVwR7e
7GFOUqQKMid/1i1BWTvnsSEtUKJ04UYVPOyzPtr+XNMN/Ik5AoANlMfG8cQ0h8mxW
MTQlGep8rmtBq+BqGgzCVZP3ThXu/ikQOUefzTS7q8rAoda+erY=
-----END RSA PRIVATE KEY-----

```

```
ssh root@private_IP -I privatekey
```

 root@vpc-secure-bastion-vsi: ~

```
root@vpc-secure-bastion-vsi:~# ssh root@10.240.129.9 -i privatekey
```



root@vpc-secure-bastion-vsi: ~

```
root@vpc-secure-bastion-vsi:~# ssh root@10.240.129.9 -i privatekey
Warning: Permanently added '10.240.129.9' (RSA) to the list of known hosts.
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 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 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`**

```

root@ABC-BXTAGFE-AAT:~# systemctl status nginx
nginx.service
root@ABC-BXTAGFE-AAT:~# systemctl start nginx

```

## 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**.

VPC on Classic

Getting started

Overview

Compute

Virtual server instances

SSH keys

Custom images

Network

VPCs

Subnets

Floating IPs

Public gateways

Access control lists

Security groups

VPNs

Security groups for VPC

REGIONS

Dallas

New security group

| Name                                   | Default | Resource Group | Virtual private cloud | Rules | Attached Interfaces |
|--|---------|----------------|-----------------------|-------|---------------------|
| agonizing-edge-spyglass-elastic-colony |         | —              | vpc-pubpriv           | 2     | 0                   |
| vpc-secure-bastion-sg                  |         | —              | vpc-pubpriv           | 3     | 1                   |
| vpc-secure-maintenance-sg              |         | —              | vpc-pubpriv           | 5     | 2                   |
| vpc-secure-private-sg                  |         | —              | vpc-pubpriv           | 0     | 1                   |

All security groups for VPC

New security group for VPC

Name

Virtual private cloud

Resource group

vpc-pubpriv-frontend-sg

vpc-pubpriv

Default

Rules

Inbound rules

| Protocol | Source type | Source    | Value       |
|----------|-------------|-----------|-------------|
| TCP      | Any         | 0.0.0.0/0 | Ports 80-80 |

Outbound rules

| Protocol | Destination type | Destination | Value |
|----------|------------------|-------------|-------|
|----------|------------------|-------------|-------|

Edit interfaces

| Instance name  | Interfaces                               | Subnet                    | Attached security groups |
|--|--|---------------------------|--------------------------|
| > vpc-secure-bastion-vsi                                   | 0/1                                      | —                         | —                        |
| <input checked="" type="checkbox"/> vpc-secure-private-vsi | 1/1                                      | —                         | —                        |
|  | <input checked="" type="checkbox"/> eth0 | vpc-secure-private-subnet | 2                        |

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

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



VPC on Classic

Getting started

Overview

Compute

Virtual server instances

SSH keys

Custom images

Network

VPCs

Subnets

Floating IPs

Public gateways

Access control lists

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 | 52.116.56.122 | ... |
| Powered On | vpc-secure-private-vsi | vpc-pubpriv           | 10.240.129.9 | -             | ... |

Items per page: 10 | 1-2 items

Data updated 4 seconds ago

What do you want to do next?

Since you've already created a virtual server instance, you can add other services.

Overview

Monitoring

All instances for VPC

vpc-secure-private-vsi

Powered On

Dallas 3

Data updated 2 seconds ago

Instance details

Name

vpc-secure-private-vsi

Virtual private cloud

vpc-pubpriv

Resource group

Default

ID

34d5a4bf-86ad-47b4-9e8d-0e9e2a98fbbd

Created

August 5, 2019 8:52:39 PM

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-private-vsi-boot | 100  | 3000     | 46.88 | Provider managed | Enabled     |

Attach volume

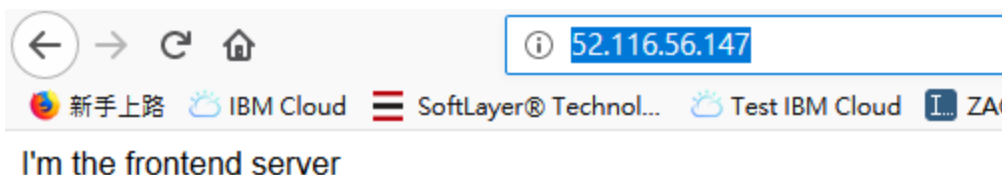
Data volumes

There are no volumes attached to this instance.

Network interfaces

| Interface | Subnet Name          | Private IP   | Floating IP | Security Groups                                    |
|-----------|----------------------|--------------|-------------|--|
| eth0      | vpc-secure-private-- | 10.240.129.9 | Reserve     | vpc-secure-private-sg<br>vpc-secure-maintenance-sg |

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.



Rules

Attached interfaces

All security groups for VPC

vpc-secure-maintenance-sg

Id: 2d364f0a-s870-42c3-s564-000001845488

View docs

...

Attached interfaces

Editing items

Cancel

Save

| Instance name                                  | Interfaces  | Subnet  | Attached security groups  |
|--|---|---|---------------------------|
| <div>▼</div> <div>vpc-secure-bastion-vsi</div> | <div>0/1</div> <div><input type="checkbox"/> eth0</div> | <div>–</div> <div>vpc-secure-bastion-subnet</div> | <div>–</div> <div>2</div> |
| <div>▼</div> <div>vpc-secure-private-vsi</div> | <div>0/1</div> <div><input type="checkbox"/> eth0</div> | <div>–</div> <div>vpc-secure-private-subnet</div> | <div>–</div> <div>2</div> |

## Remove resources

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



### Cannot delete vpc-pubpriv-frontend-sg

Before you can delete this security group, make sure that all network interfaces are detached, the security group isn't the default for any VPC, and the security group isn't referred to by any other security group rules.

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.

#### Floating IPs for VPC

REGIONS

Dallas

Reserve floating IP

| Status       | Address       | Location | Associated Device             |
|--------------|---------------|----------|-------------------------------|
| ● Associated | 52.116.56.147 | Dallas 3 | vpc-secure-private-vsi - eth0 |
| ● Associated | 52.116.56.122 | Dallas 3 | vpc-secure-bastion-vsi - eth0 |
| ● Associated | 52.116.56.22  | Dallas 3 | Public gateway on vpc-pubpriv |

Unassociate

Release

Copy UUID

Items per page: 10 | 1-3 items

Data updated 24 seconds ago

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.



## Virtual server instances for VPC

REGIONS  
Dallas

New instance +

| Status     | Name                                   | Virtual private cloud       | Private IP   | Floating IP   |     |
|------------|--|-----------------------------|--------------|---------------|-----|
| Powered On | <a href="#">vpc-secure-bastion-vsi</a> | <a href="#">vpc-pubpriv</a> | 10.240.128.8 | 52.116.56.122 | ... |
| Powered On | <a href="#">vpc-secure-private-vsi</a> | <a href="#">vpc-pubpriv</a> | 10.240.129.9 | —             | ... |

Items per page: 10 | 1-2 items

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

- Stop
- Reboot
- Delete

- 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.
- 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.