



GDCC

Government Data Center and Cloud Service

GDCC OPENSTACK

User Guide

National Telecom Public Company Limited

support@gdcc.onde.go.th

Contents

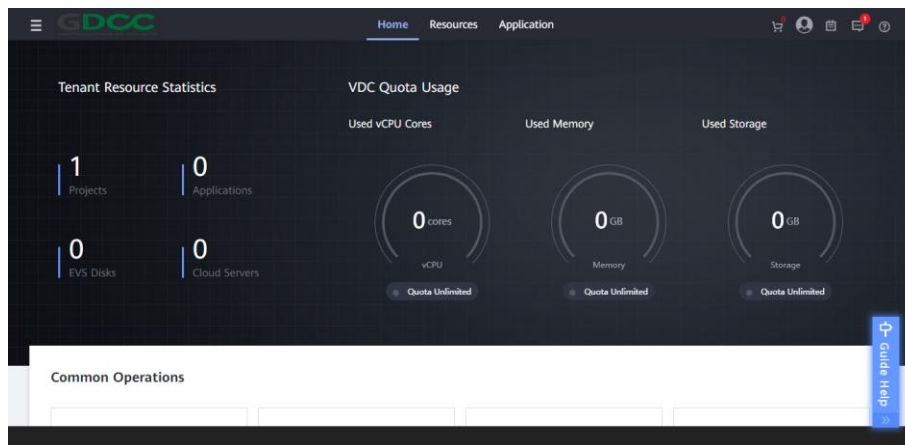
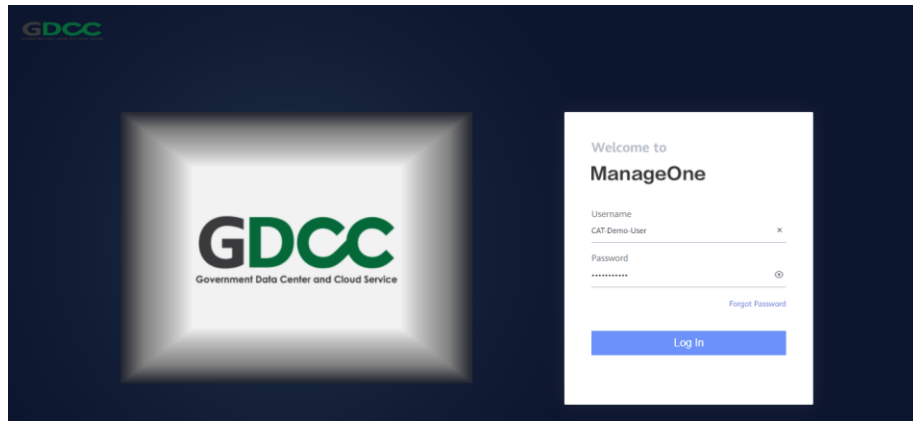
1. Getting started with the cloud tenant portal.....	2
2. Create Elastic Cloud Server (ECS)	3
3. Changing Password of Elastic Cloud Server	4
4. Create Keypair	4
5. Managing Elastic Volume Service (EVS).....	5
6. Managing Cloud Backup and Recovery	5
7. Managing Security Group	5
8. Create Virtual Private Cloud	6
9. Create Virtual Private Network	7
10. Managing NAT Gateway	7
11. Managing Elastic IP.....	8
12. Create VPC Peering.....	8

Tenant Portal Guide

1. Getting started with the cloud tenant portal

1.1 Open a web browser and go to the <https://console.mycloud.gdcc.onde.go.th/>

1.2 Enter your **Username, Password**, click **“Log In”** (system will force change password after first log in).

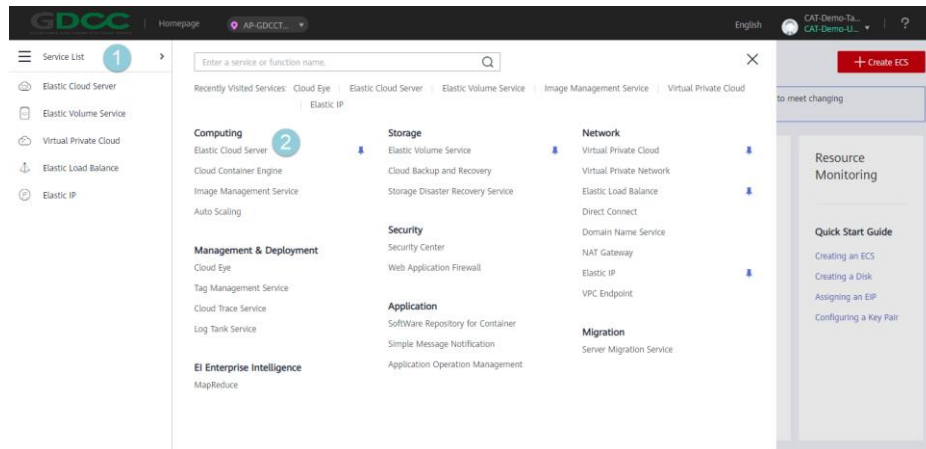


If you login success, you can see:

- My resources of user, such as Projects, Applications, EVS Disks, Cloud Servers, VDC Quota Usage (vCPU Cores, Memory, Storage).

2. Create Elastic Cloud Server (ECS)

2.1 On the cloud tenant portal click menu “**Service List**” and select **Computing > Elastic Cloud Server**.



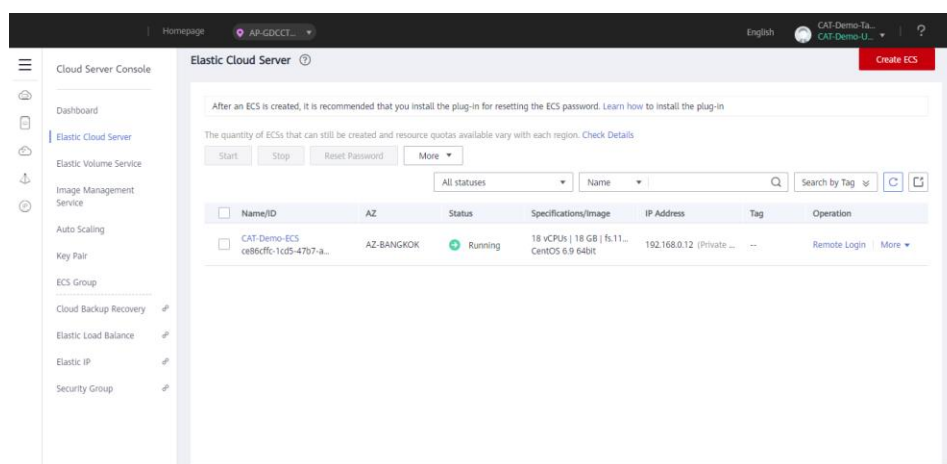
2.2 On the **Elastic Cloud Server** dashboard, click “**Create ECS**” and then click “**Apply Now**” on **Select Service** page.

2.3 Configure Basic Settings by select **AZ**, **Specification**, **Image**, **System Disk** and click “**Next: Configure Network**”.

2.4 Configure Network by select **Network (VPC)**, **Security Group**, **EIP** and click “**Next: Configure Advanced Settings**”.

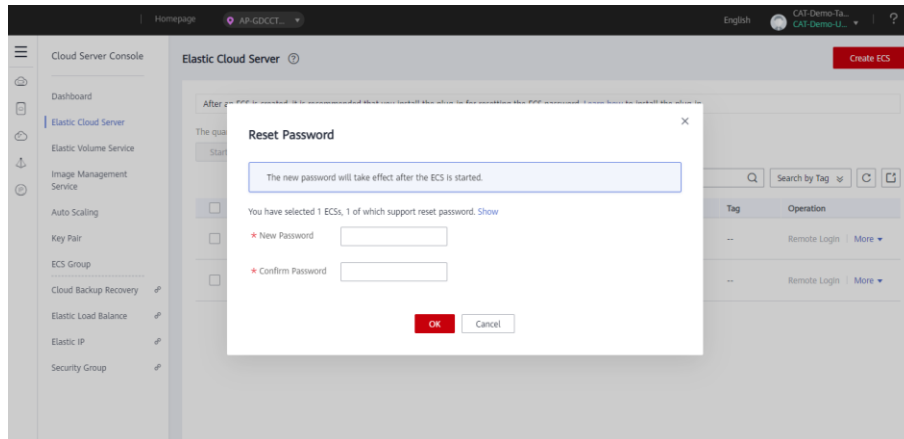
2.5 Configure Advanced Settings by type **ECS Name**, **Login Mode** (password or keypair) then click “**Next: Confirm**” and click “**Apply Now**”.

2.6 Wait system create ECS, If the system has proceeded successfully, it will show as below picture.



3. Changing Password of Elastic Cloud Server

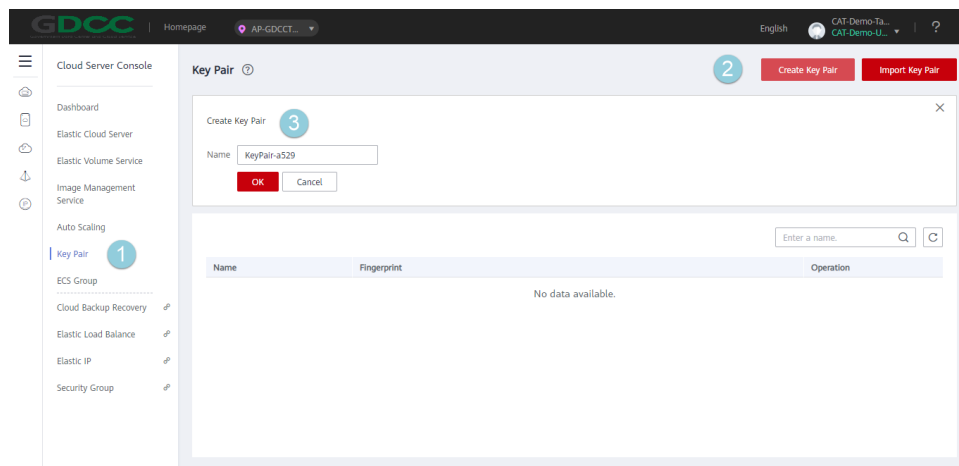
- 3.1 On the cloud tenant portal click menu “Service List” and click “Elastic Cloud Server”.
- 3.2 Choose ECS, select “Reset Password” and then system show a pop-up as follows (required power off ECS before reset password).



- 3.3 Enter **New Password** and **Confirm Password** and then click “OK”.
- 3.4 Power on ECS and password will be generated on the specify password text box.

4. Create Keypair

- 4.1 On the cloud tenant portal click menu “Service List” and select **Computing > Elastic Cloud Server > Key pair** then click “Create Key Pair” and enter **Name** of keypair and click “OK”.



5. Managing Elastic Volume Service (EVS)

- 5.1 On the cloud tenant portal click menu **“Service List”** and select **Storage > Elastic Volume Service**.
- 5.2 On the **Elastic Volume Service** dashboard, click **“Create Disk”** and then click **“Apply Now”**.
- 5.3 Select **AZ**, **Disk Size**, enter **Disk Name**, select **Quantity** of Elastic Volume Service and then click **“Next”** and **“Submit”**.
- 5.4 For Attach/Detach and Expand Capacity.
 - **Attach:** Click **“Attach”**, select **Name** of ECS to add Disk and click **“OK”**.
 - **Detach:** Click **“More”**, select **“Detach”** and click **“Yes”** (required power off ECS for detach system disk).
 - **Expand Capacity:** Click **“Expand Capacity”**, **Add Capacity (GB)**, click **“Next”** and then click **“Submit”** (required detach disk for expand capacity).
- 5.5 For Delete Elastic Volume, click **“More”**, select **“Delete”** and then click **“Yes”** (required detach disk for delete elastic volume).

6. Managing Cloud Backup and Recovery

On the cloud tenant portal click menu **“Service List”** and select **Storage > Cloud Backup and Recovery**.

Cloud Server Backup and Recovery

- a. Backup
 - **Automatic Backup:** Click tab **“Cloud Server Backup”**, click **“Create Server Backup Vault”** and click **“Next”**. Tab Associated Server select **“Configure”**, select **Server List** of ECS that you want to backup, enter **Capacity** of Vault, enter **Vault Name**, click **“Next”** and **“Submit”**.
 - **Manual Backup:** Click tab **“Cloud Server Backup”**, click check box **“Name/ID”** of Vault, click **“More”**, click **“Perform Backup”** and enter **Name** of backup and then click **“OK”**.
- b. Recovery
 - Click tab **“Cloud Server Backup”**, click tab **“Backups”**, click check box **“Backup Name”**, click **“Restore Server”**, and click **“Yes”**.

7. Managing Security Group

- 7.1 On the cloud tenant portal click menu **“Service List”** and select **Computing > Elastic Cloud Server > Security Group**.
- 7.2 It will open Security Groups in the new page and show Security Groups menu in the navigation pane on the left.

7.3 On the **Security Groups** page, click **“Create Security Group”** and set the parameters as prompted.

- a. **Template:** Specifies the security group template.
 - **Custom:** This template allows you to create security groups with custom security group rules.
 - **General-purpose web server:** This template includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389.
 - **All ports open:** This template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks. Exercise caution when using this template.
- b. **Name:** Enter security group name.
- c. Click **“OK”**.

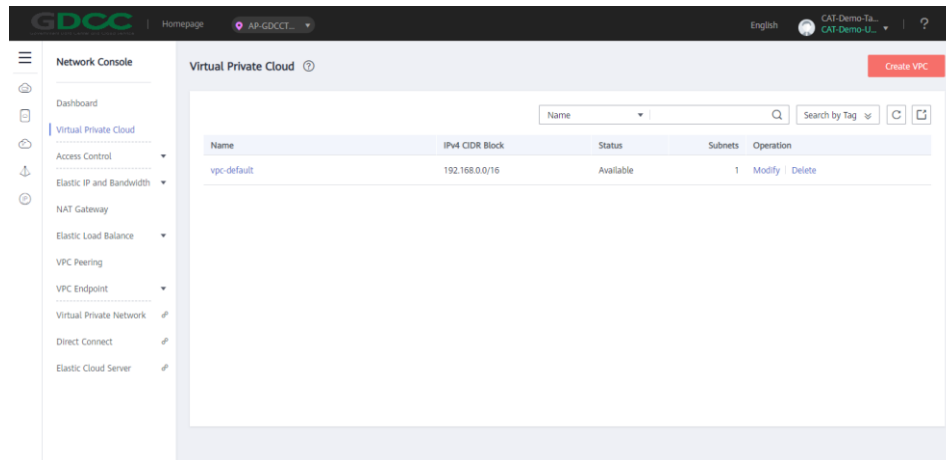
7.4 Adding a Security Group Rule

- a. Select the target security group and click **“Manage Rule”** in the Operation column to switch to the page for managing inbound and outbound rules.
- b. On the Inbound Rules tab, click **“Add Rule”**. In the displayed dialog box, set required parameters to add an inbound rule and click **“OK”**.
 - **Protocol & Port:** Specifies the network protocol.
 - **Source:** Specifies the source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example:
 - IP address: xxx.xxx.xxx.xxx
 - IP address/subnet mask: xxx.xxx.xxx.0/24
 - All IP address: 0.0.0.0/0
 - Security group name
- c. On the Outbound Rules tab, click **“Add Rule”**. In the displayed dialog box, set required parameters to add an outbound rule and click **“OK”**.
 - **Protocol & Port:** Specifies the network protocol.
 - **Source:** Specifies the destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example:
 - IP address: xxx.xxx.xxx.xxx
 - IP address/subnet mask: xxx.xxx.xxx.0/24
 - All IP address: 0.0.0.0/0
 - Security group name

8. Create Virtual Private Cloud

- 8.1 On the cloud tenant portal click menu **“Service List”** and select **Network > Virtual Private Cloud**.
- 8.2 On the **Virtual Private Cloud** dashboard, click **“Create VPC”** and then click **“Create Now”**.
- 8.3 Setting Basic Information, select **Region** (Project name), enter **Name** of VPC.
- 8.4 Setting Default Subnet, select **AZ**, **Name** of default subnet, **CIDR Block** and click **“Create Now”**.

8.5 Wait system create VPC, If the system has proceeded successfully, it will show as below picture.



9. Create Virtual Private Network

9.1 On the cloud tenant portal click menu “**Service List**” and select **Network > Virtual Private Network**.

9.2 Click tab “**VPN Gateway**”, click “**Create VPN Gateway**”.

a. Create VPN Gateway.

- Enter **Name** of VPN Gateway, select “**VPC**”.

b. Create VPN Connection.

- Enter **Name** of VPN Connection, “**select Local Subnet**”, enter **IP Remote Gateway, Remote Subnet** and **PSK** for VPN Connection.
- Configure Advanced Settings (Policy IKE and IPSEC parameter that you want to connect to Remote Gateway), click “**Next**” and click “**Submit**”.

10. Managing NAT Gateway

- The SNAT function translates private IP addresses into EIPs, allowing servers in a VPC to share an EIP to access the Internet in a secure and efficient way.
- The DNAT function enables servers in a VPC to share an EIP to provide services accessible from the Internet through IP address mapping or port mapping.

10.1 On the cloud tenant portal click menu “**Service List**” and select **Network > NAT Gateway**.

10.2 On the **NAT Gateway** dashboard, click “**Create Public NAT Gateway**”.

10.3 Select **Region** (Project name), enter **NAT Gateway Name**, select **VPC**, select **Subnet**, select **NAT Gateway Type** and then click “**Create Now**” and “**Submit**”.

10.4 When NAT gateway created successfully click “**Add Rule**”.

10.5 Add an SNAT rule to allow servers in a VPC to access the Internet using a shared EIP.

a. Click “**Add SNAT Rule**”.

b. Select **Subnet**, select **EIP** and click “**OK**”.

10.6 Add a DNAT rule to allow servers in a VPC to provide external services.

- a. Click **“Add DNAT Rule”**
- b. **Port Type** including All ports and Specific port.
 - **All ports:** Any requests on the EIP will be forwarded by the NAT gateway to server based on IP address mapping.
 - **Specific port:** The requests with specific protocol and port will be forwarded by the NAT gateway on the EIP to the port of the target server.
- c. **Protocol**
 - **All ports:** The value of this parameter will be All by default.
 - **Specific port:** Specific port for Port Type.
- d. **EIP:** Specifies the EIP to provide services accessible from the Internet.
- e. **Outside Port:** Specifies the port of the EIP.
- f. **Private IP Address:** Specifies the private IP address of the server that provides services accessible from the Internet through the DNAT rule.
- g. **Inside Port:** Specifies the port of the server.

11. Managing Elastic IP

11.1 On the cloud tenant portal click menu **“Service List”** and select **Network > Elastic IP**.

11.2 On the **EIPs** dashboard, click **“Assign EIP”** and then click **“Create Now”**.

11.3 Select **Region** (Project name).

11.4 Enter Bandwidth size.

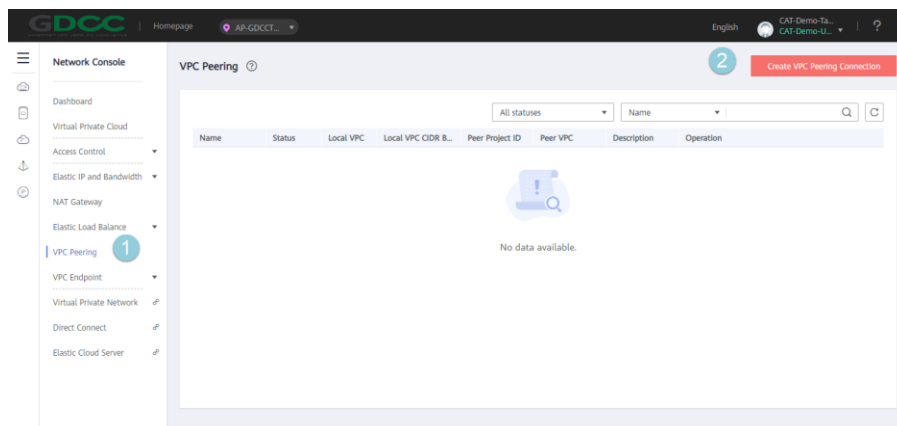
11.5 Enter Bandwidth Name and click **“Create Now”** and **“Submit”**.

11.6 On the **EIPs** dashboard, click **“Bind”**, select the instance to bind the EIP and click **“OK”**.

12. Create VPC Peering

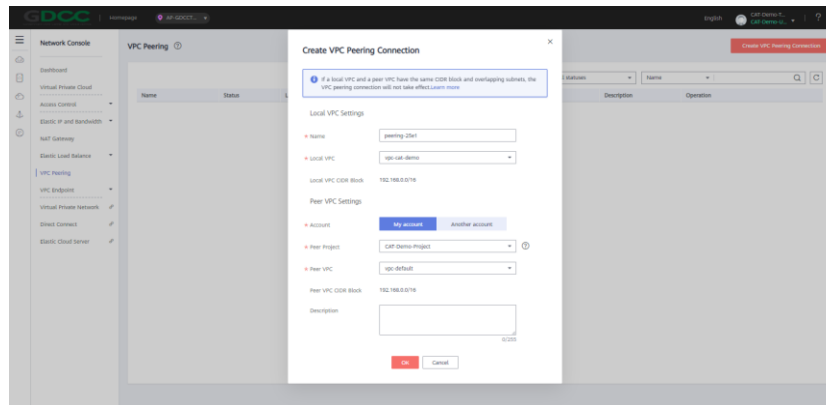
12.1 On the cloud tenant portal click menu **“Service List”** and click **“Virtual Private Cloud”**.

12.2 Click tab **“VPC Peering”** and click **“Create VPC Peering Connection”**.

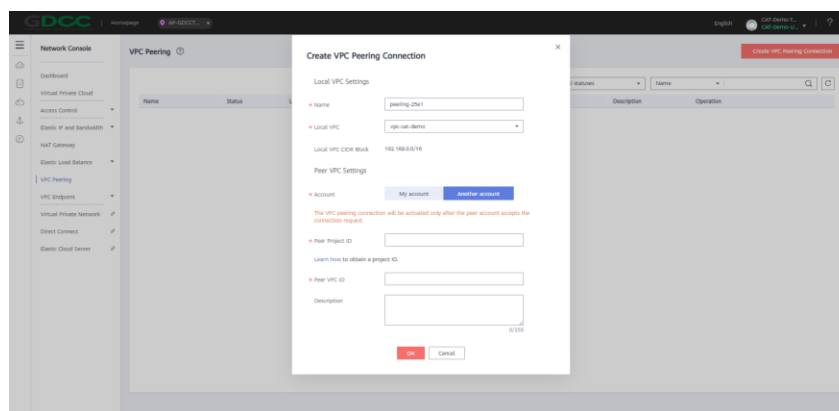


12.3 System shows a pop-up as follows.

- a. Create a VPC Peering connection with another VPC in your account.



- b. Create a VPC Peering Connection with a VPC in another account.



12.4 Configure parameters as prompted.

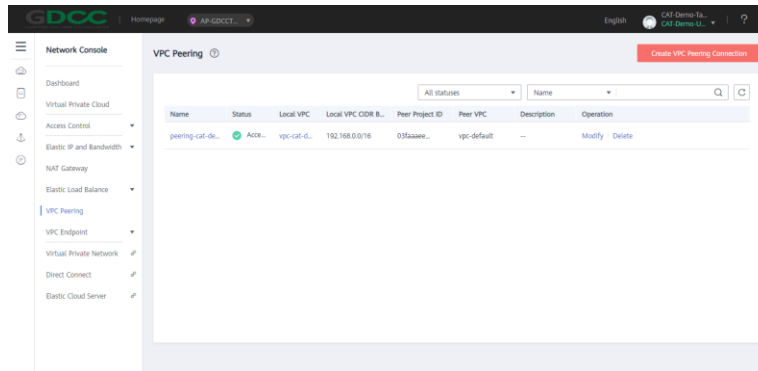
For Create a VPC Peering connection with another VPC in your account.

- a. **Name:** Specifies the name of the VPC peering connection.
- b. **Local VPC:** Specifies the local VPC. You can select one from the drop-down list.
- c. **My Account:** The VPC peering connection will be created between two VPCs, in the same region, in your account.
- d. **Peering Project:** Specifies the peer project name. The project name of the current project is used by default.
- e. **Peer VPC:** You can select one from the drop-down list if the VPC peering connection is created between two VPCs in your own account.

For Create a VPC Peering Connection with a VPC in another account.

- a. **Name:** Specifies the name of the VPC peering connection.
- b. **Local VPC:** Specifies the local VPC. You can select one from the drop-down list.

- c. **Another account:** The VPC peering connection will be created between your VPC and a VPC in another account, in the same region.
 - d. **Peer Project ID:** Enter Project ID for peering.
 - e. **Peer VPC ID:** Enter VPC ID for peering.
- 12.5 After configuring parameters already, click **“OK”** and wait system create VPC Peering, If the system has proceeded successfully, it will show as below picture.



12.6 Adding Routes for a VPC Peering Connection.

- a. Click **VPC Peering** that previously created, click **“Add Local Route”**, enter **IP Destination routes** for a VPC Peering another account connection.
- b. Click **“Add Local Route”** and **“Add Peer Route”** for a VPC Peering with another VPC in your account.

