GDCC OPENSTACK

User Guide

National Telecom Public Company Limited

support@gdcc.onde.go.th

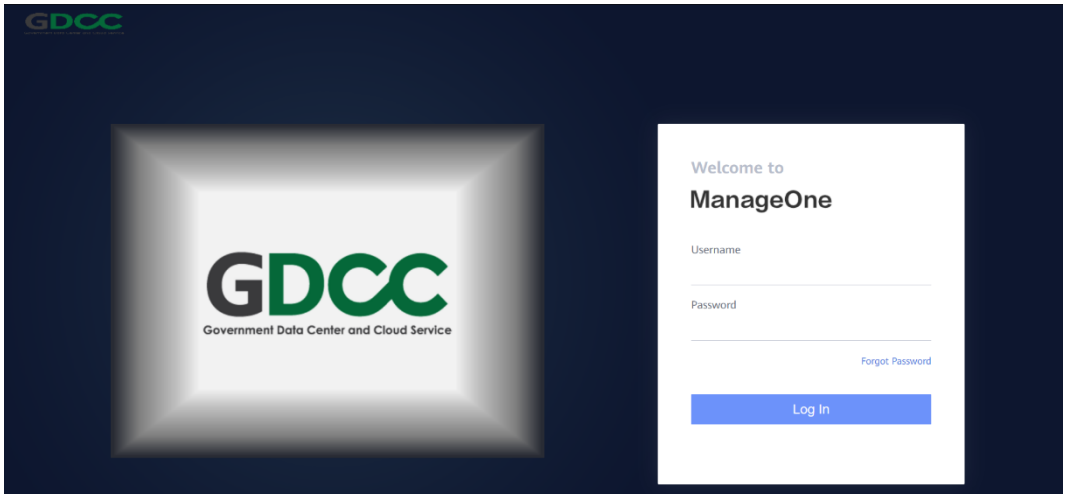
Contents

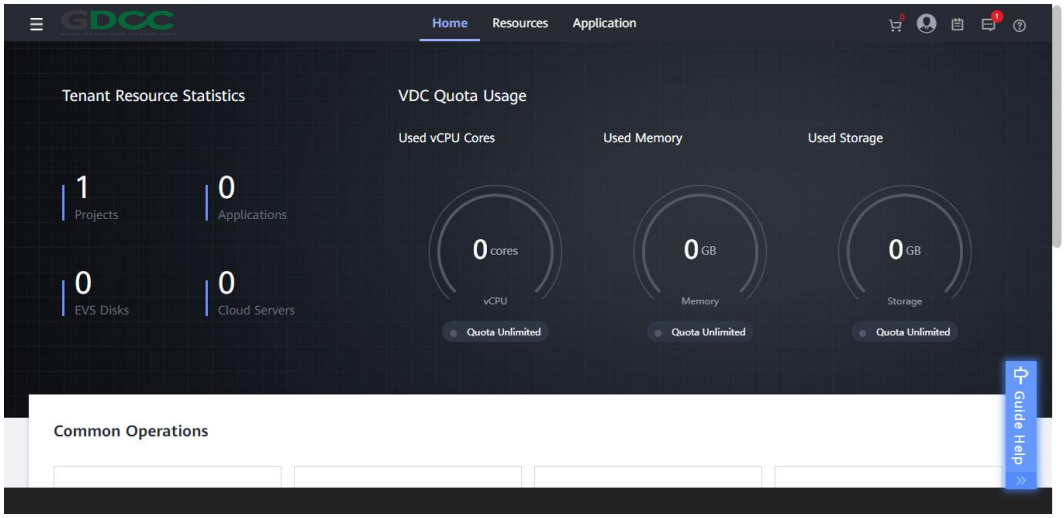
Tenant Portal Guide

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).



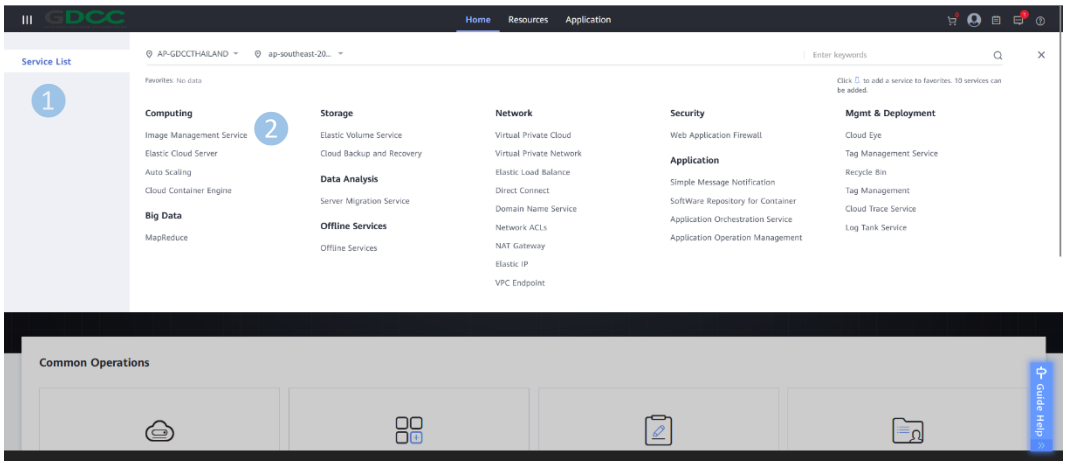


If you login success, you can see:

- 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**.



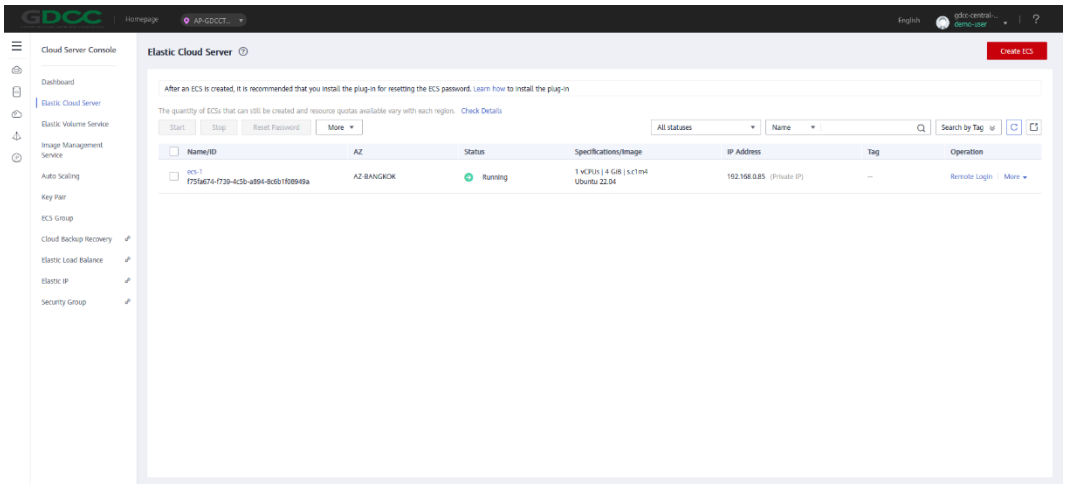
2.2 On the **Elastic Cloud Server** dashboard, click “**Create ECS”** and then click **“Apply Now”** on **Select Service** page.

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”**.

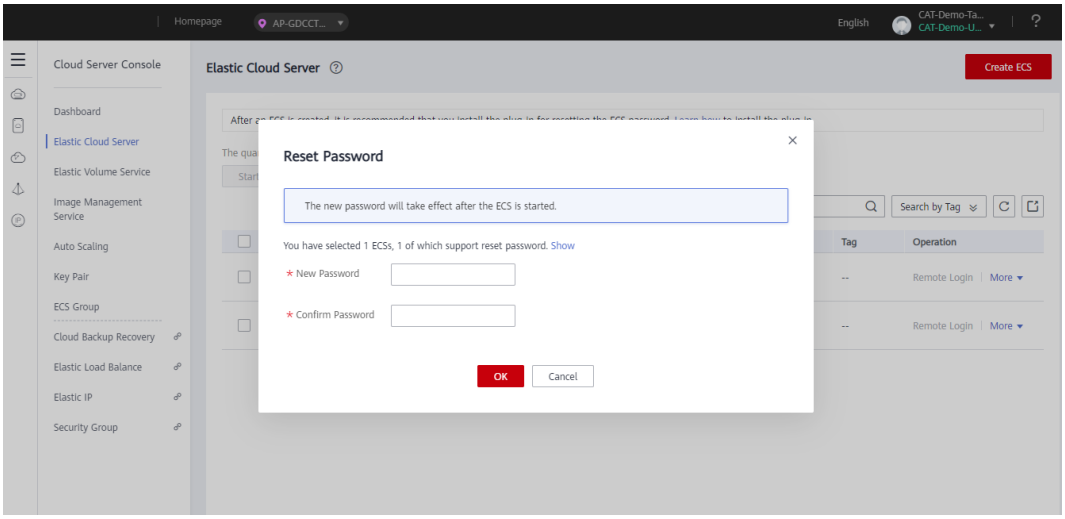
2.6 Wait system create ECS, If the system has proceeded successfully, it will show as below picture.



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 **“More”** and **“Reset Password”** and then system show a pop-up as follows (required power off ECS before reset password).

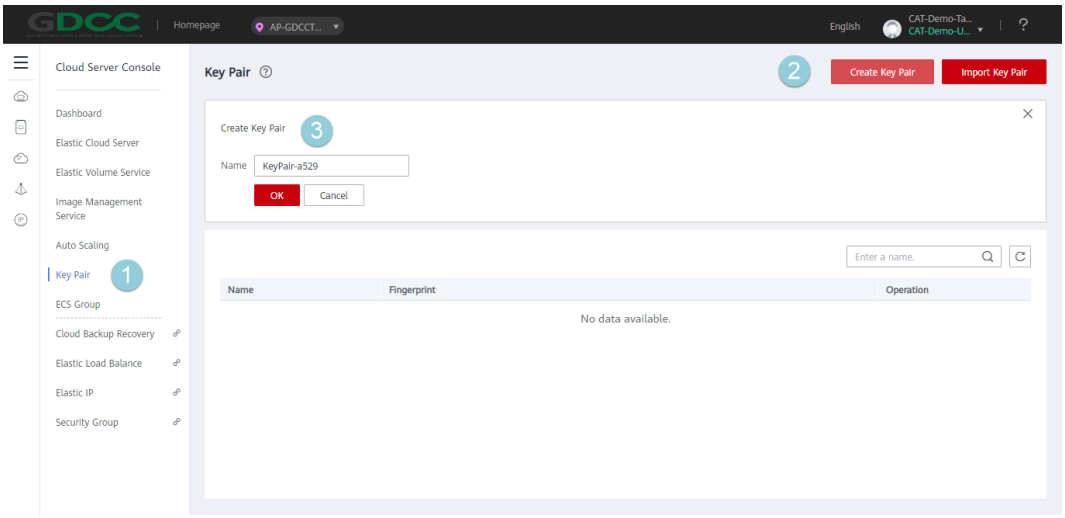


3.3 Enter **New Password** and **Confirm Password** and then click **“OK”**.

3.4 Power on ECS and password will be generated on the specify password text box.

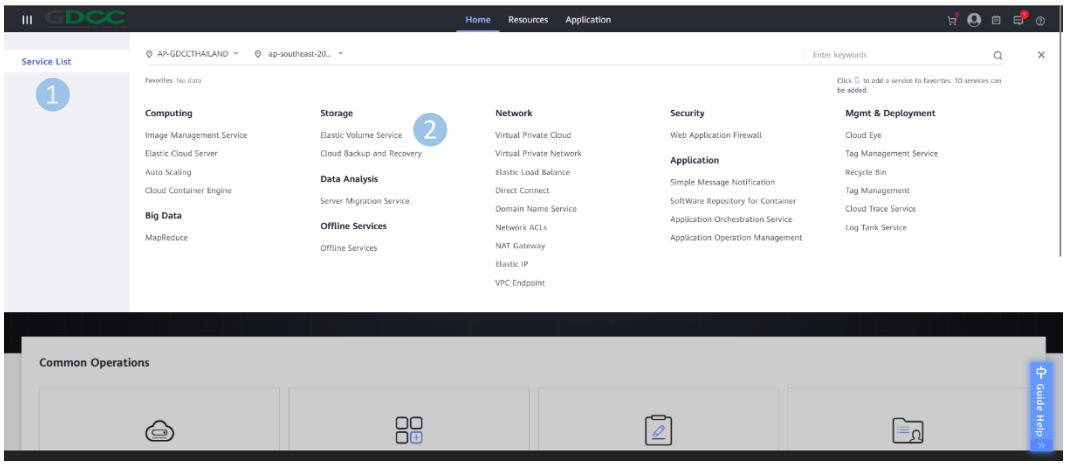
4. Create Keypair

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”**.

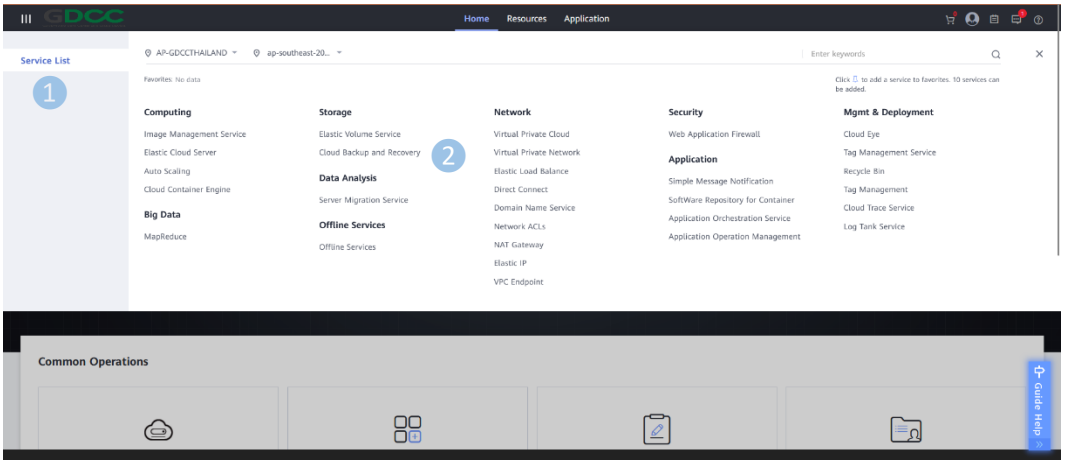
5.4 For Attach/Detach and Expand Capacity.

- **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

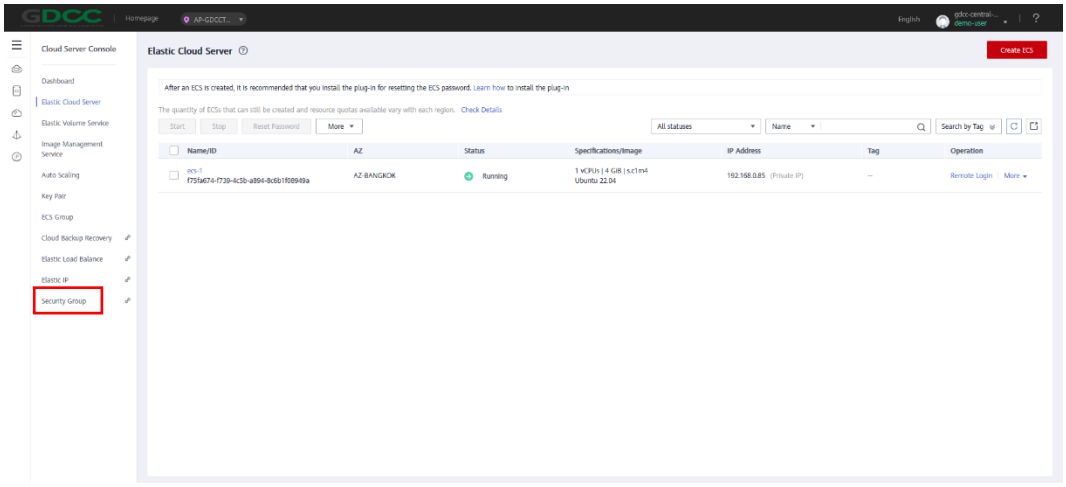
- **Automatic Backup:** Click tab **"Cloud Server Backup"**, click **"Create Server Backup Vault"** and click **"Next"**. Tab Associated Server select **"Configure"**, select **Server List** of ECS that you want to backup, enter **Capacity** of Vault, tab Automatic Association select **"Configure",** 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"**, select **Server List** of ECS that you want to 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. **Name**: Enter security group name.

b. **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.

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"**.

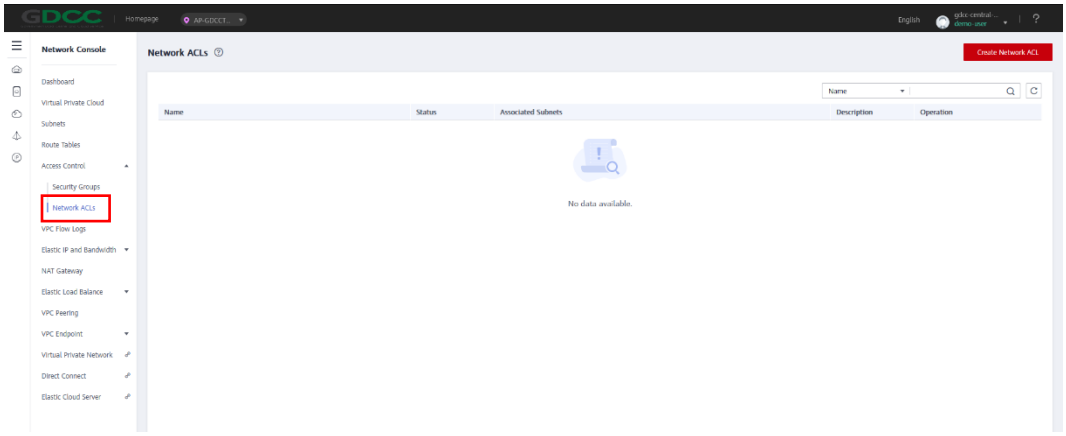
- **Protocol & Port**: Specifies the network protocol.
- **Source**: Specifies the source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example:
  - IP address: xxx.xxx.xxx.xxx
  - IP address/subnet 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. Managing Network ACLs

8.1 On the cloud tenant portal click menu **"Service List"** and select **Network > Virtual Private Cloud > Access Control > Network ACLs**.



8.2 On the **Network NACLs** page, click "**Create Network ACL"** .

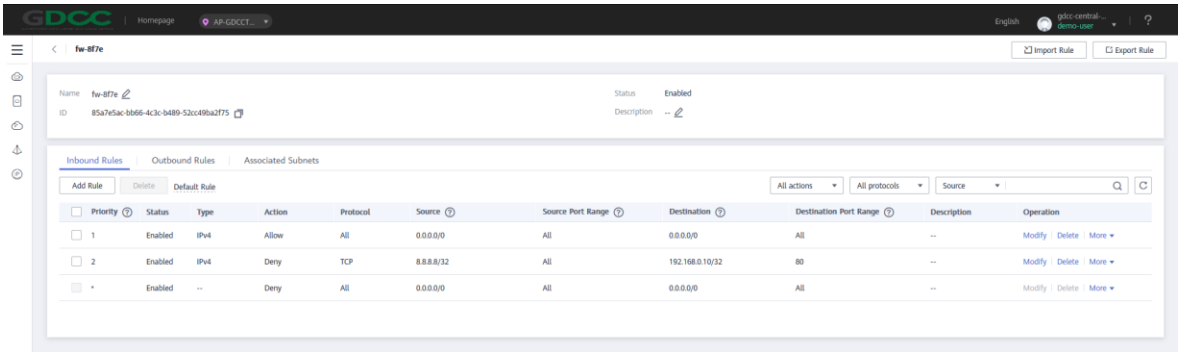
8.3 Specifies the network ACL name and click "**OK**".

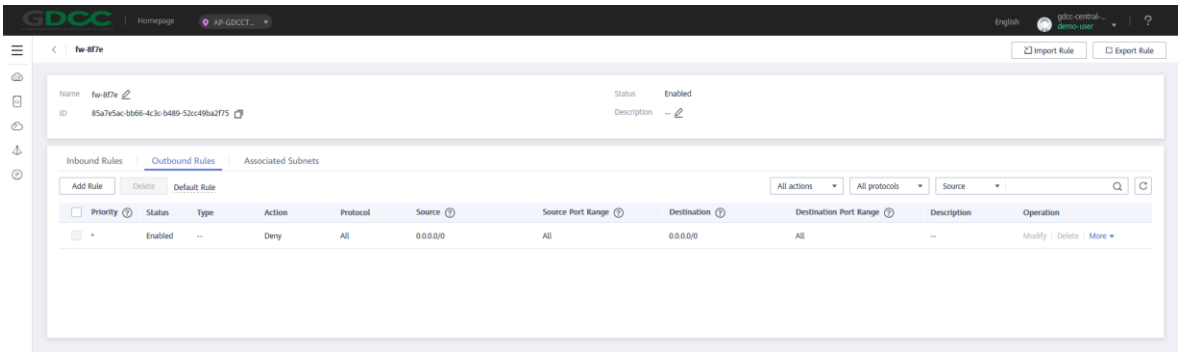
8.4 Click **"Add Rule"** to config Inbound Rules or Outbound Rules.

a. On the Inbound Rules tab or Outbound Rules, click Add Rule and Specifies parameter.

- **Network Type:** IPv4 or IPv6
- **Action:** Allow or Deny
- **Protocol:** TCP, UDP, ICMP, or All
- **Source:** Specifies the source from which the traffic is allowed. The source can be an IP address or IP address range. (example xxx.xxx.xxx.xxx/32 (IP address))
- **Source Port Range:** Specifies the source port number or port number range.
- **Destination:** Specifies the destination to which the traffic is allowed. The destination can be an IP address or IP address range.
- **Destination Port Range:** Specifies the destination port number or port number range.

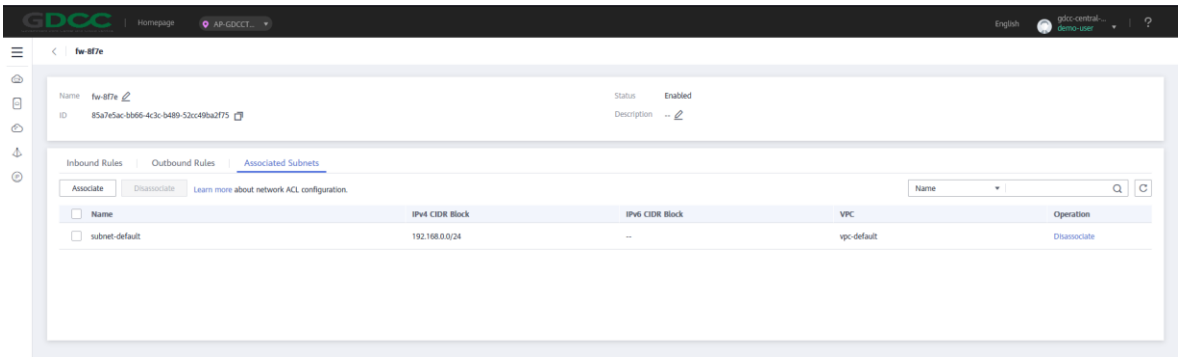
b. Click "**OK**".





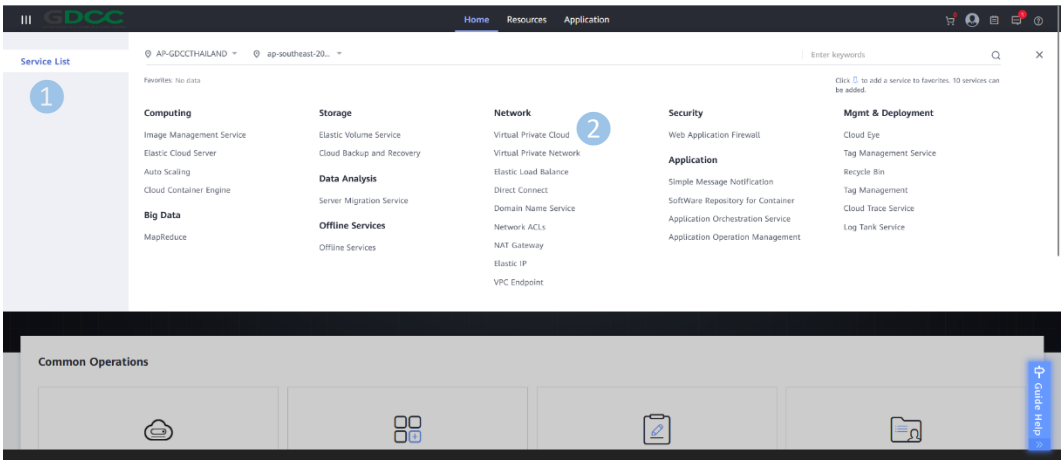
8.5 Click the Associated Subnets tab and click “**Associate**”.

8.6 Select the subnets to be associated with the network ACL, and click “**OK**”.
(Note: a subnet can only be associated with one network ACL.)



9. Create Virtual Private Cloud

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

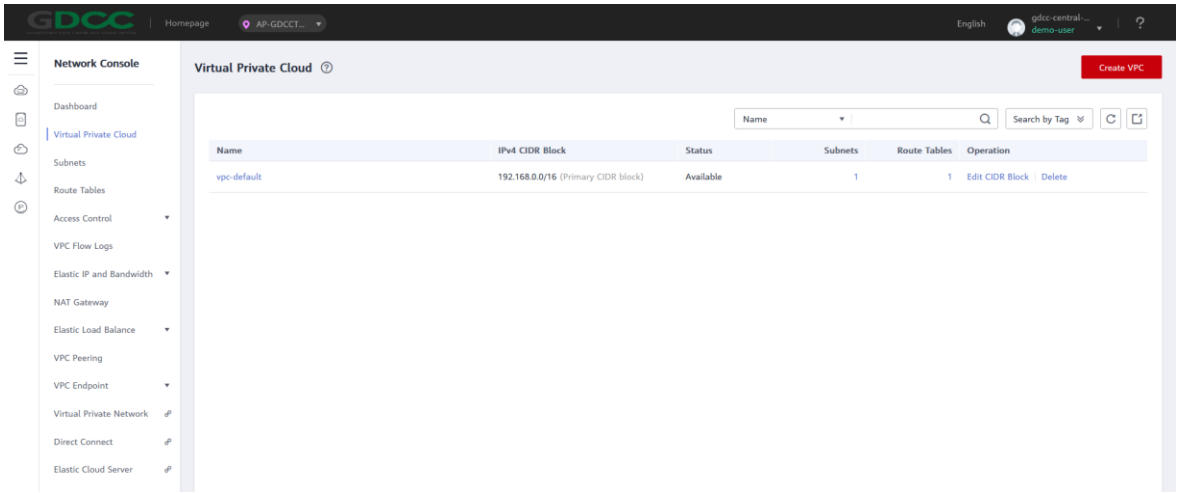


9.2 On the **Virtual Private Cloud** dashboard, click **“Create VPC”**.

9.3 Setting Basic Information, select **Region** (Project name), enter **Name** of VPC, setting **IPv4 CIDR Block**.

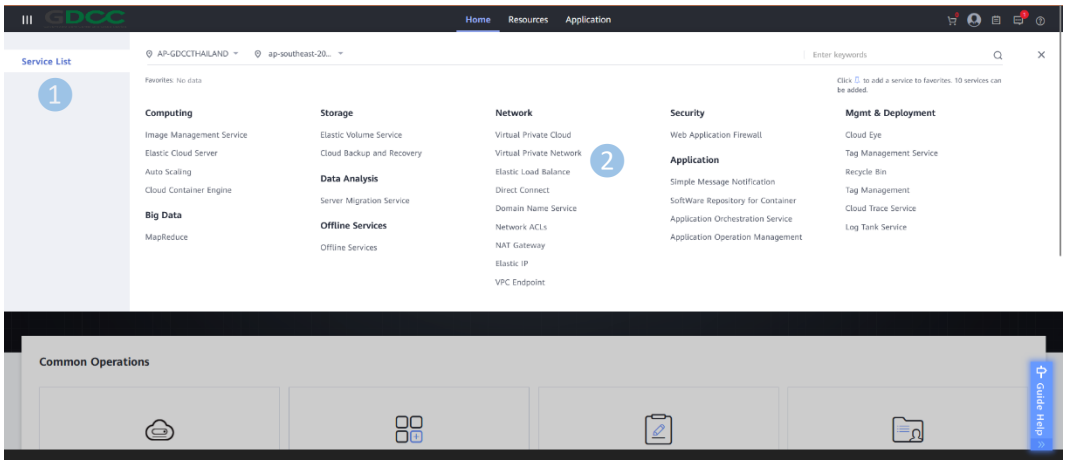
9.4 Setting Default Subnet, select **AZ**, **Name** of default subnet, **IPv4 CIDR Block** and click **"Create Now"**.

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



10. Create Virtual Private Network

10.1 On the cloud tenant portal click menu **"Service List"** and select **Network > Virtual Private Network**.



10.2 Click tab **"VPN Gateway"**, click **"Create VPN Gateway"**.

a. Create VPN Gateway.

- Enter **Name** of VPN Gateway, select **"VPC"**, select **"Bandwidth"**.

b. Create VPN Connection.

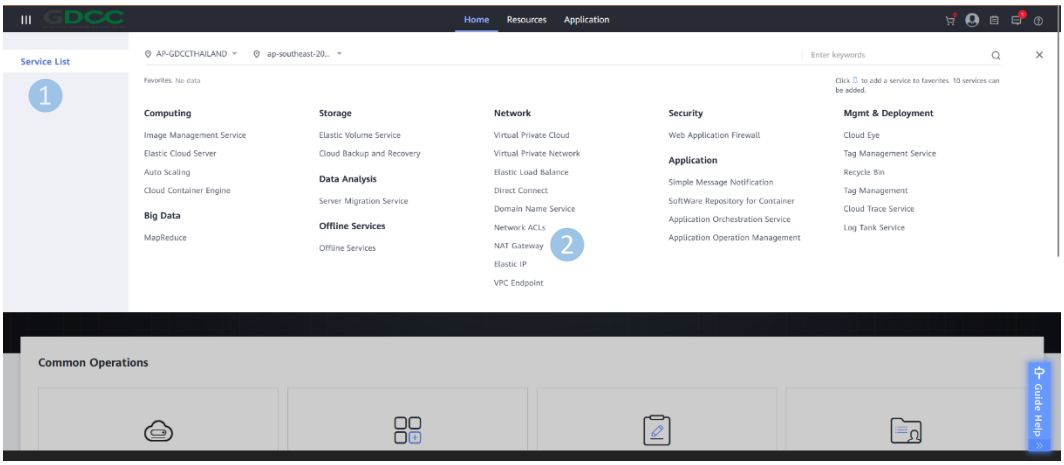
- Enter **Name** of VPN Connection, **"select Local Subnet"**, enter **IP Remote Gateway**, **Remote Subnet** and **PSK** for VPN Connection.

- Configure Advanced Settings (Policy IKE and IPSEC parameter that you want to connect to Remote Gateway), click **“Next”** and click **“Submit”**.

11. 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.

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



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

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

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

11.5 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”**.

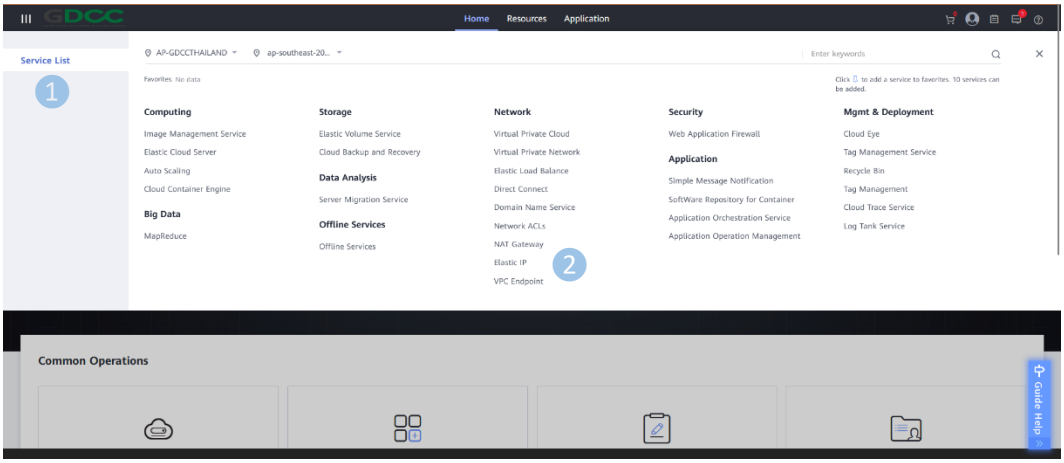
11.6 Add a DNAT rule to allow servers in a VPC to provide external services.

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 cloud server.
h. Click **“OK”.**

12. Managing Elastic IP

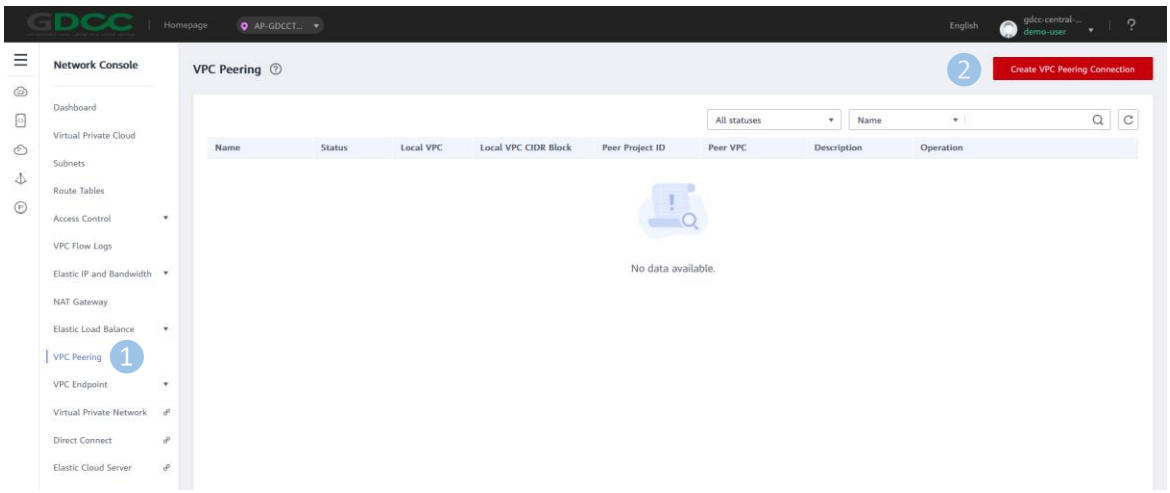
12.1 On the cloud tenant portal click menu **“Service List”** and select **Network > Elastic IP**.



12.2 On the **EIPs** dashboard, click **“Assign EIP”**.
12.3 Select **Region** (Project name).
12.4 Enter **“Bandwidth”** size.
12.5 Enter **“Bandwidth Name**” and **“Quantity”** and click **“Create Now”** and **“Submit”**.
12.6 On the **EIPs** dashboard, click **“Bind”**, select the instance to bind the EIP and click **“OK”**.

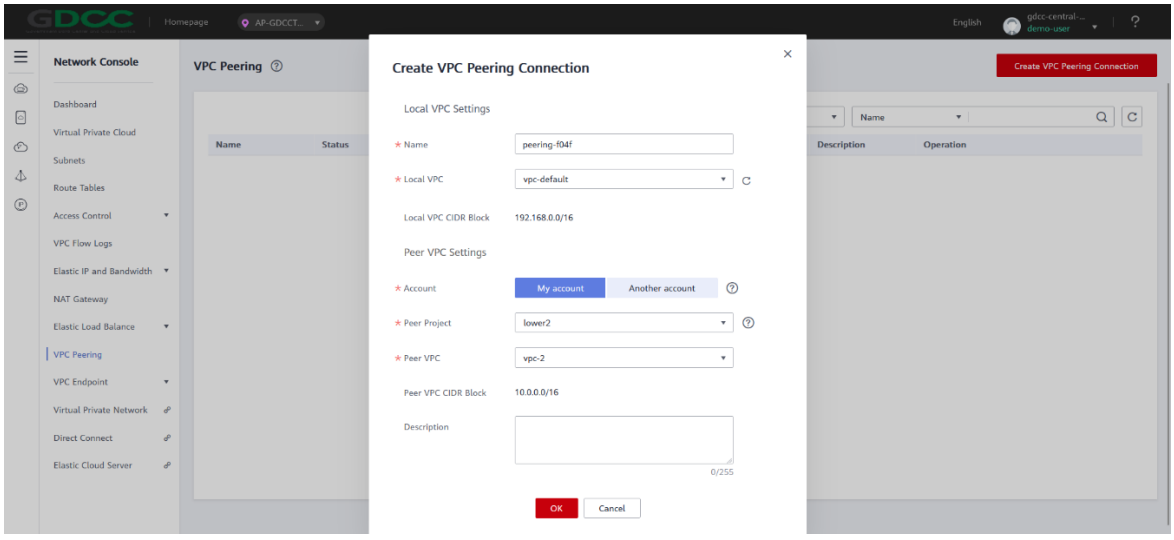
13. Create VPC Peering

13.1 On the cloud tenant portal click menu **“Service List”** and click **“Virtual Private Cloud”.**
13.2 Click tab **“VPC Peering”** and click **“Create VPC Peering Connection”**.

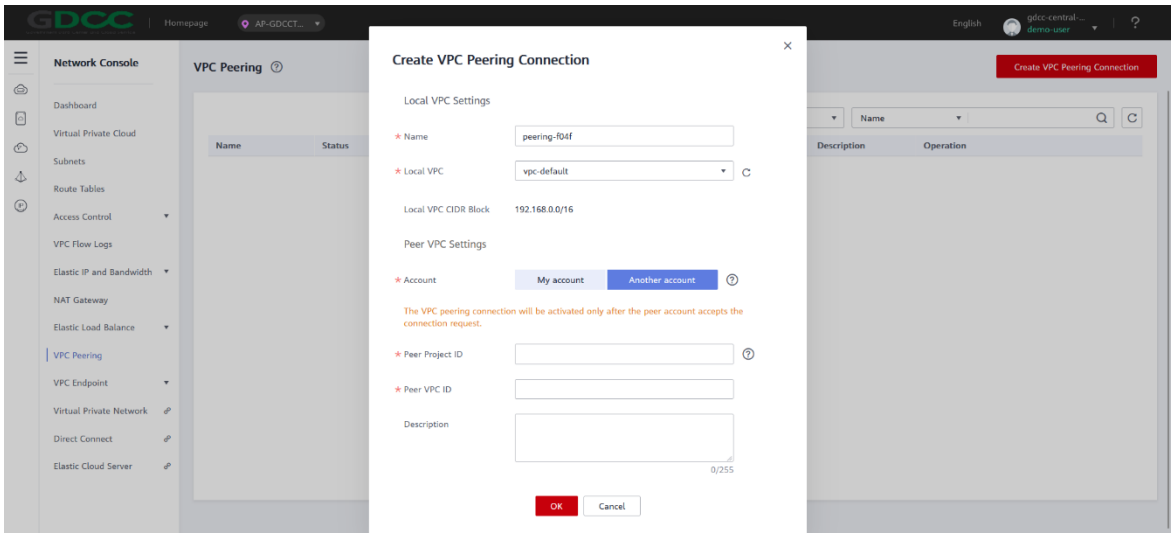


13.3 System shows a pop-up as follows.

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



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



13.4 Configure parameters as prompted.

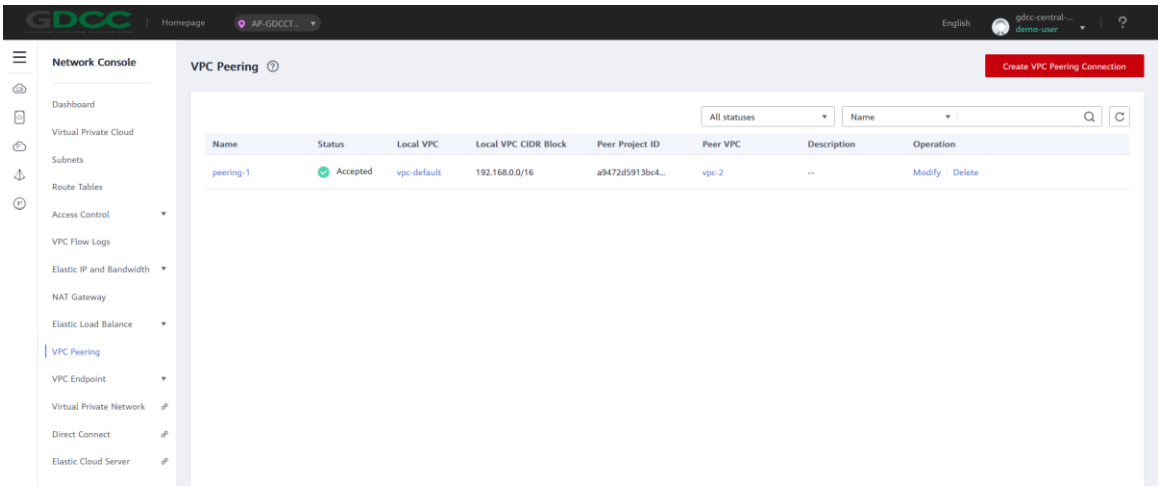
For Create a VPC Peering connection with another VPC in your account.

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.

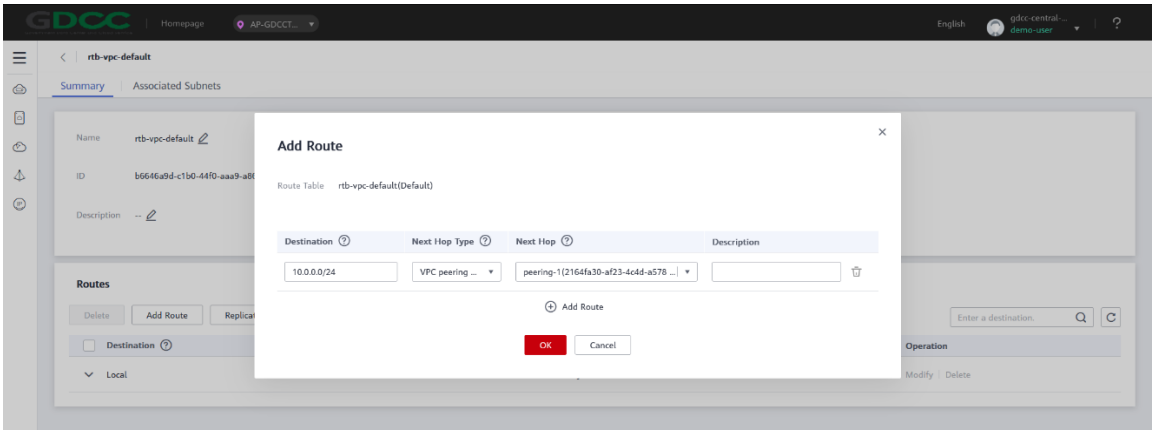
a. **Name:** Specifies the name of the VPC peering connection.
b. **Local VPC:** Specifies the local VPC. You can select one from the drop-down list.
c. **Another account**: The VPC peering connection will be created between your VPC and a VPC in another account, in the same region.
d. **Peer Project ID:** Enter Project ID for peering (obtain the Project ID by clicking the username in the upper right corner and selecting My Settings and choose Resource Sets ID).
e. **Peer VPC ID:** Enter VPC ID for peering.

13.5 After configuring parameters already, click **"OK"** and wait system create VPC Peering, If the system has proceeded successfully, it will show as below picture.



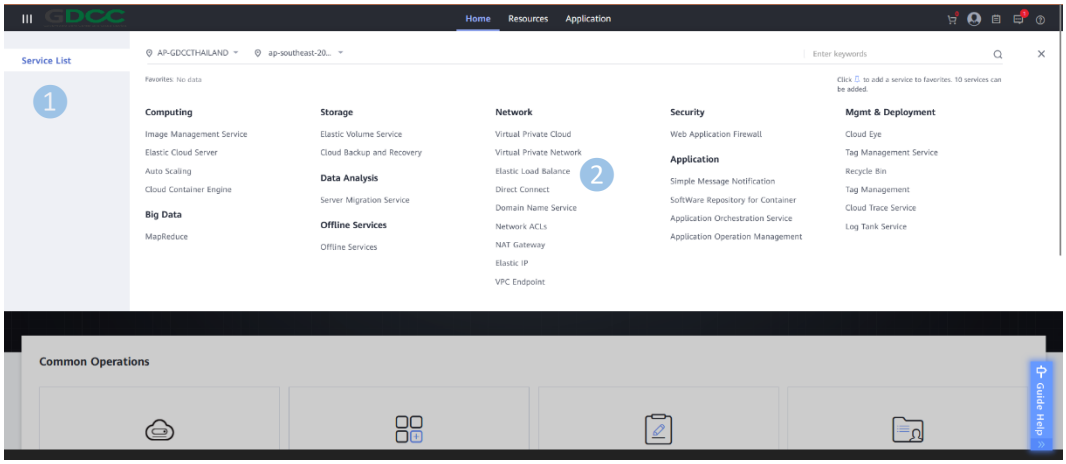
13.6 Adding Routes for a VPC Peering Connection.

a. Click **VPC Peering** that previously created, click **"Route Tables"**, click **"Add Route",** enter **IP Destination routes** for a VPC Peering another account connection, select Next Hop Type to **"VPC Peering Connection"**, select Next Hop and click **"OK"**.



14. Create Elastic Load Balance

On the cloud tenant portal click menu **"Service List"** and select **Network > Elastic Load Balance**.



14.1 **Create Elastic Load Balancer**

14.1.1 Click "**Create Elastic Load Balancer**". Set the parameters

a. **Region:** Specifies region
b. **AZ:** Specifies one or more AZs of the load balancer
c. **Network Type:** Specifies the network where the load balancer works
   - **Public IPv4 network**
   - **Private IPv4 network**
   - **IPv6 network**
d. **VPC:** Specifies the VPC where the load balancer works.
e. **EIP:** Specifies EIP if select Network Type as Public IPv4 network.
f. **Subnet:** Specifies Subnet if select Network Type as Private IPv4 network or IPv6 network.
g. **Name:** Specifies load balancer name.

14.1.2 Click **"Create Now"**.

14.1.3 Confirm the configuration and click **"Submit"**.

14.2 **Create Listeners**

14.2.1 On the Load Balancers page, click Load Balancer that previously created, click **"Listeners tab**" and then click **"Add Listener"**. Set the parameters

a. **Name:** Specifies Listener name.
b. **Frontend Protocol/Port:** Select TCP or UDP for load balancing at Layer 4. Select HTTP or HTTPS for load balancing at Layer 7.

14.2.2 Click **"Next"**

14.2.3 Create Backend Server Group by select **"Create new"** or "**Use existing"**

a. **Name:** Specifies Backend Group name.
b. **Backend Protocol:** Specifies the protocol used by backend servers to receive requests.
c. **Load Balancing Algorithm:** Specifies the algorithm the load balancer uses to distribute traffic (Weighted round robin, Weighted least connections or Source IP hash).

14.2.4 Click **"Finish"**.

14.3 **Create Backend Server Groups**

14.3.1 On the Load Balancers page, click Load Balancer that previously created, click **"Backend Server Groups"** tab.

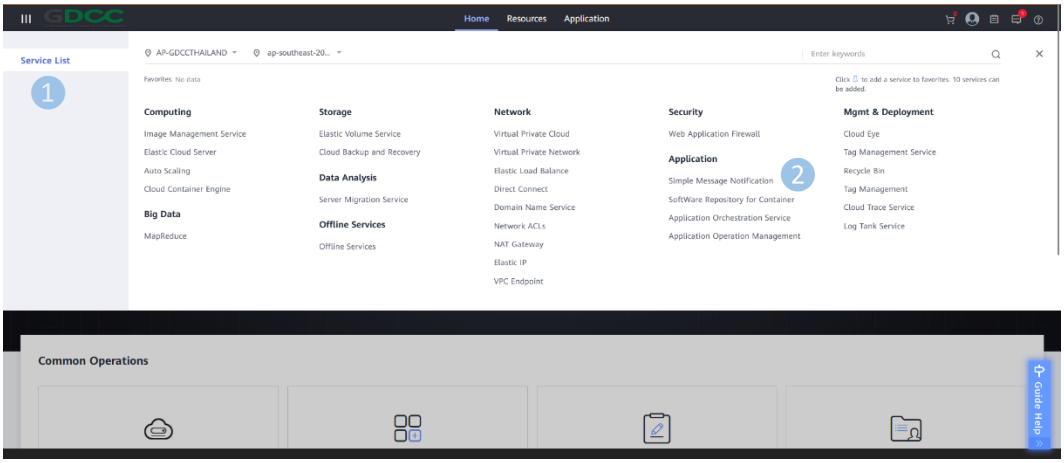
14.3.2 Select Backend Server Group that create in 14.2.3, and click **"Add"**.

14.3.3 Select the ECS to add in backend server group, and click **"Next"**.

14.3.4 Specifies Port for each the ECS in backend server group, and click **"Finish"**.

15. Create Simple Message Notification

15.1 On the cloud tenant portal click menu **"Service List"** and select **Application > Simple Message Notification**.



15.2 Click tab **"Topics"**, click **"Create Topic"**.

a. Specifies Topic Name.

b. Specifies Display Name.

15.3 Click **"OK".**

15.4 Click tab **"Subscriptions"** , click **"Add Subscription"**

a. Select Topic Name.

b. Select Protocol to **"Email"**.

c. Specifies Endpoint.

15.5 Click **"OK".**

16. Create Auto Scaling

16.1 On the cloud tenant portal click menu **"Service List"** and select **Computing > Auto Scaling**.

16.2 Click **"Create AS Configuration".** Set the parameters.

a. **Name:** Specifies AS Configuration Name**.**

b. **Configuration Template:** Select Template for Scale**.**

c. **Specifications, Image, Disk, Security Group:** Specifies if choose Configuration Template as "Create a new specifications template"**.**

d. **EIP:** Specifies EIP**.**

e. **Login Mode:** Select Login Mode "Keypair" of "Password"**.**

16.3 Click **"Create Now"**

16.4 Click **"Create AS Group"**. Set the parameters.

a. **AZ:** Select AZ**.**
b. **Name**: Specifies AS group Name**.**
c. **Max. Instances:** Specifies the maximum number of ECS in an AS group**.**
d. **Expected Instances:** Specifies the expected number of ECS in an AS group.
e. **Min. Instances:** Specifies the minimum number of ECS in an AS group**.**
f. **AS Configuration:** Select AS Configuration Template**.**
g. **VPC:** Specifies VPC for ECS**.**
h. **Subnet:** Specifies subnet for ECS.
i. **Load Balancing:** Optional for use Elastic Load Balancer.
j. **Instance Removal Policy:** Specifies the priority for removing instances from an AS group.
k. **EIP:** Release or Do not release**.**
l. **Health Check Method:** Select ECS health check or ELB health check.
m. **Health Check Interval: Specifies the health check period for an AS group**

16.5 Click **"Create Now".**

17. Create Web Application Firewall (WAF)

17.1 On the cloud tenant portal click menu **"Service List"** and select **Security > Web Application Firewall**.

17.2 On the tab Dashboard, Click **"Create WAF"**, select a **"Region"**, click **"Next"** and Click **"Back to Website Settings"** and add domain names to be protected.

17.3 Adding a Domain Name to WAF

a. Click **"Add Website"** and click **"OK"**.
b. Configure Domain Name.
c. Configure Server Configuration
   - **Client Protocol**: protocol used by a client to access a server.
   - **Server Protocol**: protocol used by WAF to forward client requests.
   - **Server Address:** public IP address or domain name of the web server that a client accesses.

   (Optional) Import a certificate.
   If Client Protocol is set to HTTPS, following steps to import a certificate.
   - Click **"Import New Certificate"**, enter the certificate name and paste the certificate file and private key to the text boxes.
   - Click **"OK".**

d. Set Proxy Configured. The default value is No.
e. Click **"Confirm"**. If Domain name added successfully is displayed, the domain name information is added to WAF.
f. Click **"Whitelist WAF Now"**, click "**Yes"** and click **"Finished"**.
g. Click **"Test WAF Now"** Configure the CNAME record at your DNS provider by copy the CNAME record and create a CNAME record on your DNS provider.

h. Click **“Finished”.**

17.4 Adding or Editing a Policy

a. In the navigation pane on the left, choose “**Policies”.**

b. click **“Add Policy”** or choose an existing policy to edit.

c. Set other parameters.

- To add a Basic Web Protection rule
- To add a CC attack protection rule
- To add a Precise protection rule
- To add a Blacklist or whitelist rule
- To add a Known Attack Source rule
- To add a Geolocation access control rule
- To add a Web Tamper Protection rule
- To add an Anti-Crawler rule
- To add an Information leakage prevention rule
- To add a Global Protection Whitelist (Formerly False Alarm Masking) rule
- To add a Data masking rule