GDCC SELF SERVICE PORTAL

คู่มือการใช้งาน GDCC OPENSTACK

National Telecom Public Company Limited

support@gdcc.onde.go.th

Contents

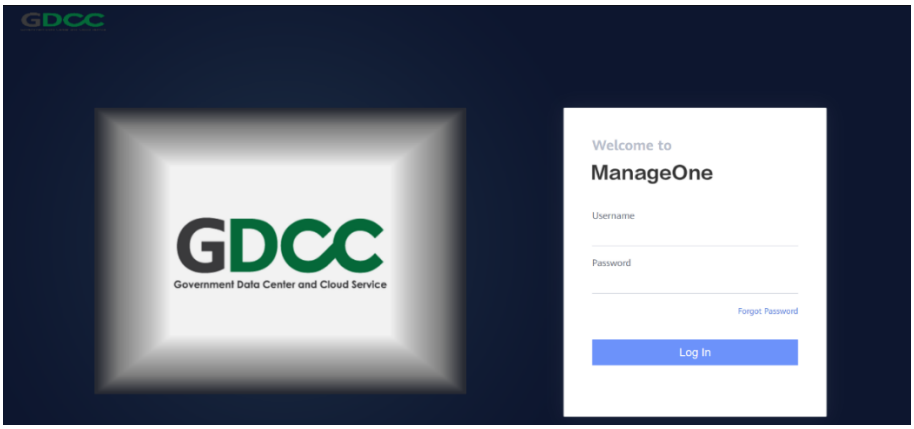
ข้อควรระวังในการใช้งาน GDCC OpenStack

GDCC OpenStack เป็นระบบในรูปแบบ Self-Service ที่ผู้ใช้งานสามารถบริหารจัดการทรัพยากรและดำเนินการต่าง ๆ ได้ด้วยตนเอง ดังนั้นผู้ใช้งานจึงมีหน้าที่รับผิดชอบต่อการดำเนินการทุกขั้นตอนในระบบเพื่อป้องกันความผิดพลาด ระบบได้ออกแบบให้มีการแสดงข้อความแจ้งเตือน (Notifications) ในขั้นตอนสำคัญก่อนยืนยันการทำรายการ โดยเฉพาะการดำเนินการที่มีผลกระทบต่อข้อมูลหรือทรัพยากร เช่น การลบ ECS, การลบ EVS Disk เป็นต้น ซึ่งระบบจะแสดงหน้าต่าง “Risk Notice” หรือข้อความแจ้งเตือนความเสี่ยงบนหน้า Portal ทุกครั้งก่อนยืนยันการดำเนินการ **ผู้ใช้งานต้องอ่านและตรวจสอบรายละเอียดในหน้าต่างแจ้งเตือนดังกล่าวอย่างครบถ้วนก่อนกดปุ่ม “Confirm”** เนื่องจากการลบข้อมูลหรือทรัพยากรในระบบ Self-Service เป็นการดำเนินการแบบ**ไม่สามารถกู้คืนได้ (Non-Recoverable)** เมื่อยืนยันการลบเรียบร้อยแล้ว ข้อมูลและทรัพยากรที่เกี่ยวข้องจะถูกลบออกจากระบบอย่างถาวรทันที

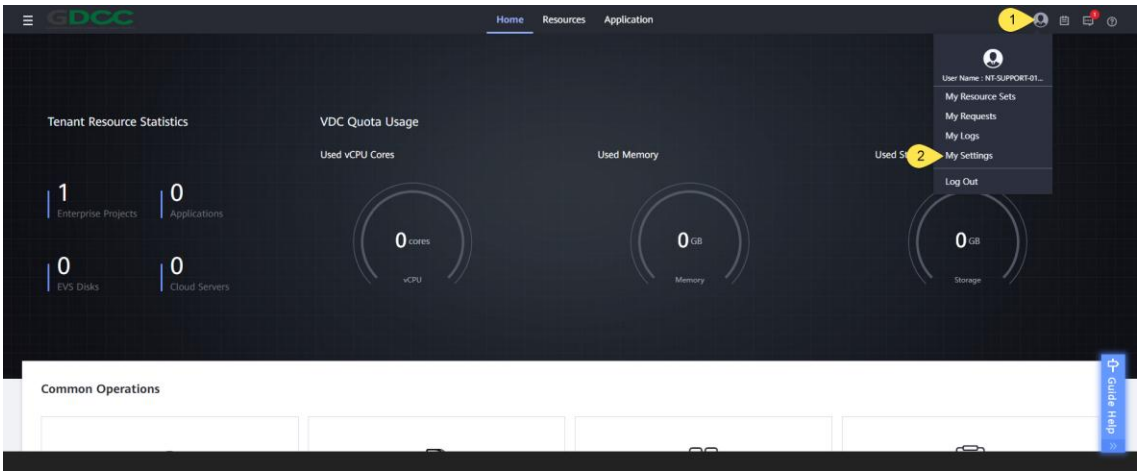
ทั้งนี้ ผู้ให้บริการขอสงวนสิทธิ์ไม่รับผิดชอบต่อความเสียหาย ความผิดพลาด หรือการสูญหายของข้อมูลใด ๆ ที่เกิดจากการตัดสินใจหรือการดำเนินการของผู้ใช้งานในทุกกรณี

Tenant Portal Guide

1. **วิธีการเข้าใช้งานหน้า Self Service Portal**
   1.1 เปิด web browser และไปที่ลิงก์ https://console.mycloud.gdcc.onde.go.th/
   1.2 กรอก **Username, Password ที่ทาง GDCC จัดส่งให้**, click **“Log In”** (เมื่อ Log in ครั้งแรกระบบจะบังคับให้เปลี่ยน Password)

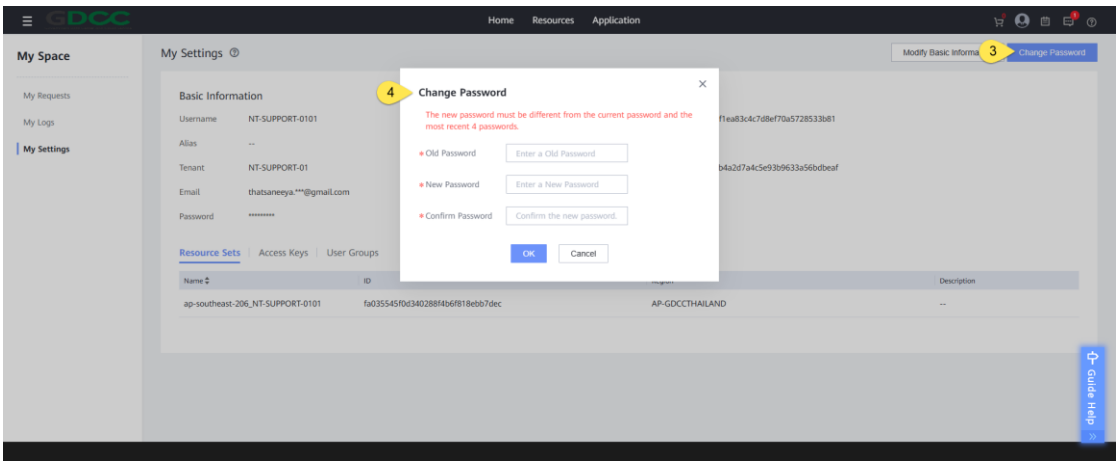


1.2.1 กรณีหน่วยงานมีความประสงค์จะเปลี่ยนรหัสผ่าน (Password) ของผู้ใช้งานอีกครั้ง สามารถดำเนินการได้โดยไปที่เมนู Profile บริเวณมุมขวาบนของหน้าจอ จากนั้นคลิก Dropdown และเลือกเมนู My Settings เพื่อทำการเปลี่ยนรหัสผ่าน



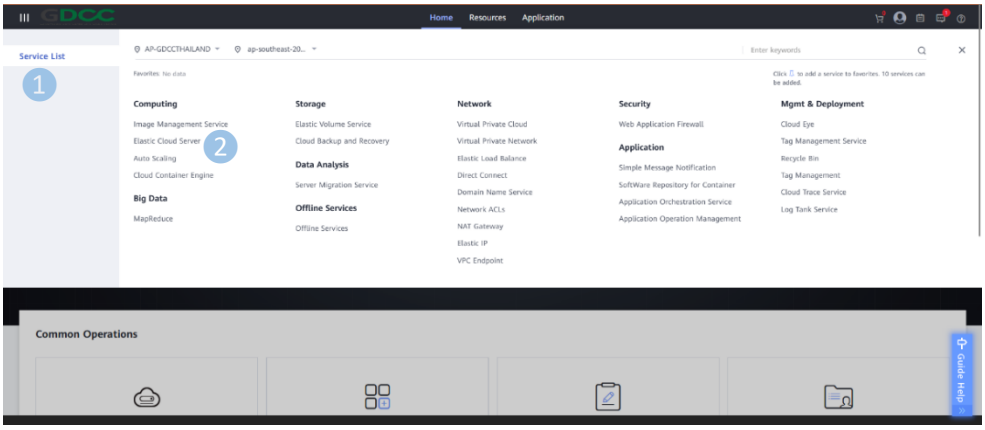
เมื่อเข้าสู่หน้า My Settings ให้เลือกเมนู Change Password โดยมีเงื่อนไขดังนี้:

- ความยาว 8–32 ตัวอักษร
- รหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสผ่านปัจจุบัน และต้องไม่ซ้ำกับรหัสผ่านย้อนหลัง 4 ครั้งล่าสุด
- ต้องมีอักขระอย่างน้อย 3 ใน 4 ประเภทต่อไปนี้
  - ตัวพิมพ์ใหญ่ (A–Z)
  - ตัวพิมพ์เล็ก (a–z)
  - ตัวเลข (0–9)
  - อักขระพิเศษ ~!@#$%^&*()-_=+[{]}|;:'",<.>/?
  - ต้องมีอักขระพิเศษอย่างน้อย 1 ตัว
  - ต้องไม่ประกอบด้วย Username หรือ Username แบบกลับหลัง



2. การสร้าง Elastic Cloud Server (ECS)

2.1 ไปที่เมนู “**Service List**” หมวด **Computing > Elastic Cloud Server**



2.2 เมื่อมาหน้า **Elastic Cloud Server** แล้ว ไปที่ “**Create ECS**” และ “**Apply Now**”

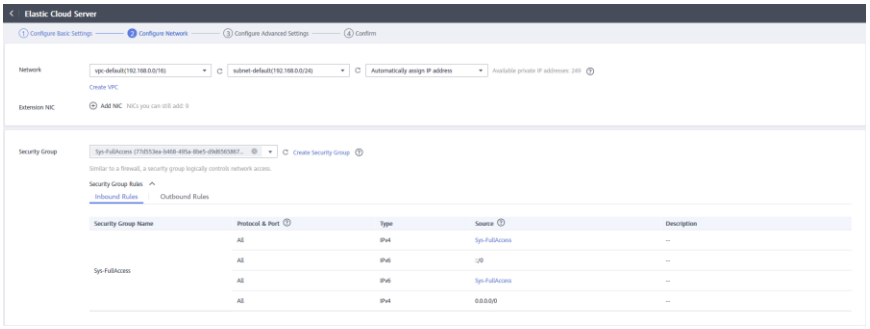
2.3 หน้านี้จะเป็นการตั้งค่า ECS เบื้องต้น

- AZ เลือก Site ที่ต้องการจะสร้าง ECS ฝั่งนนทบุรี หรือ ฝั่งบางรัก
- Specifications เลือก Spec CPU และ RAM
- image เลือก OS
- System Disk กำหนด Disk

  เมื่อทำการตั้งค่า ECS เรียบร้อยแล้ว เลือกที่ “Next: Configure Network”

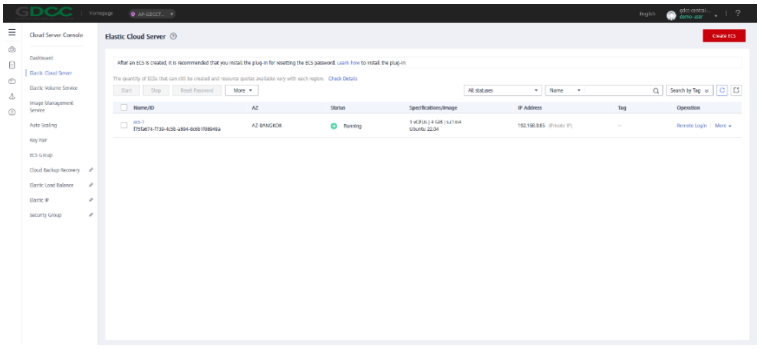
2.4 กำหนด (VPC) หรือกำหนด Subnet ที่ต้องการใช้งาน

2.5 Security Group จะเป็นการเปิด Port ภายใน ECS (ขาเข้า Inbound แนะนำให้เปิด port เฉพาะที่ใช้งาน เช่น SSH 22, RDP 3389, HTTP 80,HTTPS 443)



2.6 EIP ถ้าเลือก Auto assign ECS ที่ทำการสร้างขึ้นมาจะมี IP Public Address มาด้วย หากเรียบร้อยแล้ว คลิกที่ “Next: Configure Advanced Settings”

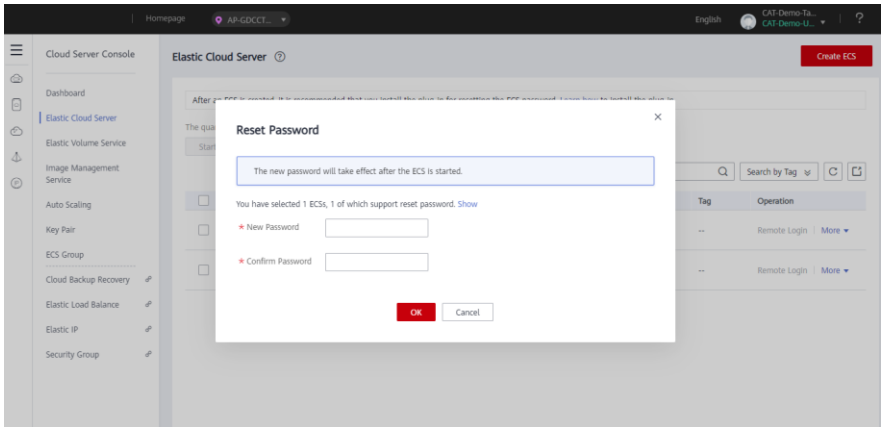
2.7 ตั้งชื่อ ECS และ ตั้งค่าการ log in จะสามารถเลือกเป็นแบบ password หรือ keypair ได้ หากเรียบร้อยแล้ว คลิก“Next :Confirm” และ “Apply Now”



3. การเปลี่ยนรหัสผ่าน Elastic Cloud Server

3.1 ไปที่เมนู **“Service List” > หมวด Elastic Cloud Server**

3.2 เลือก ECS ที่ต้องการเปลี่ยนรหัสผ่าน และ ไปที่ “More”และ“Reset Password” (ก่อนเปลี่ยน รหัสผ่านต้องทำการ Power off ECS ก่อนเสมอ)

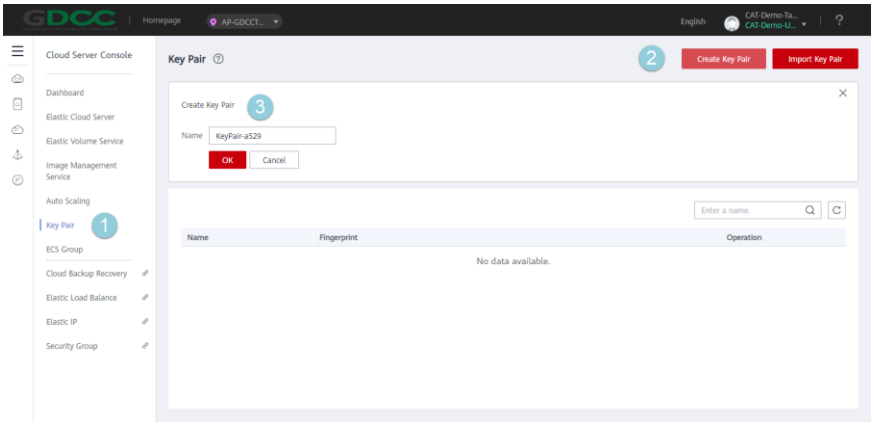


3.3 เมื่อทำการใส่รหัสผ่านใหม่ที่ช่อง New Password และ Confirm Password เสร็จแล้ว เลือก “OK”

3.4 หลังจากนั้น Power on และเข้าใช้งาน ECS ด้วยรหัสผ่านใหม่

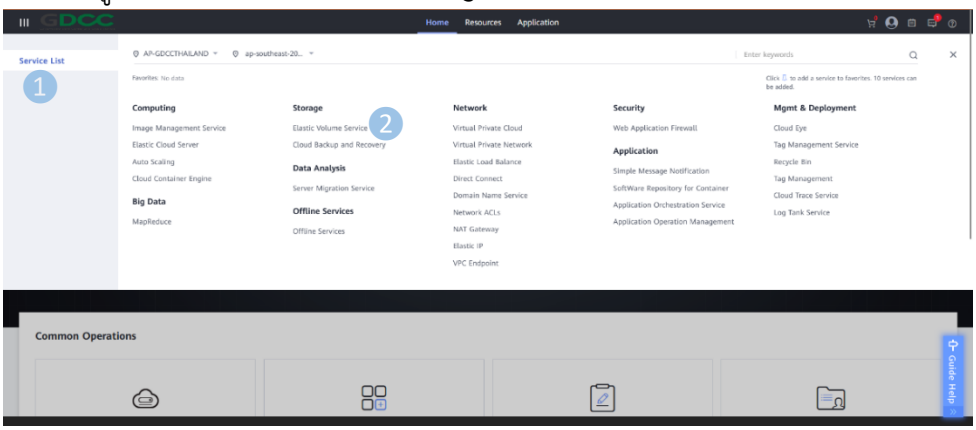
4. การสร้าง Keypair

4.1 ไปที่เมนู “**Service List**” **หมวด Computing > Elastic Cloud Server > Key pair** คลิก “Create Key Pair” และ กำหนดชื่อ keypair จากนั้น กด “OK”



5. การจัดการ Elastic Volume Service (EVS)

5.1 ไปที่เมนู “**Service List**” หมวด **Storage > Elastic Volume Service**



5.2 เมื่อมาหน้า Elastic Volume Service แล้วกด “Create Disk” และ “Apply Now”

5.3 เลือก AZ , กำหนดขนาด Disk Size และใส่ชื่อที่ช่อง Disk Name , จากนั้น“Next” และ “Submit”

5.4 การ Attach/Detach และ Expand Capacity

5.4.1 Attach: เป็นการนำ Disk ที่เราสร้างนั้นใส่ไปที่ ECS
หลังจาก Attach ให้เลือก ECS และทำการ Add Disk เรียบร้อยแล้ว กด “OK”

5.4.2 Detach: เป็นการนำ Disk ออกมาจาก ECS โดยไปที่ “More”เลือก “Detach” และคลิก “Yes” (กรณีที่เป็น System Disk ต้องการทำการ Power off ECS ก่อน Detach)

5.4.3 Expand Capacity: คลิกที่ “Expand Capacity” กำหนดขนาด Disk ที่ช่อง Add Capacity (GB) คลิก “Next” กด “Submit” (การทำExpand Capacity จะต้อง Detach Disk ออกมาจาก ECS ก่อน)

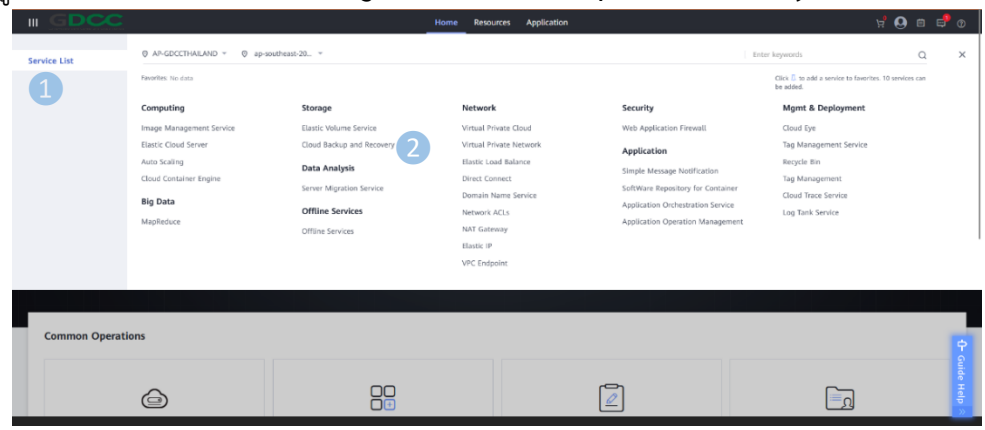
5.5 การลบ Elastic Volume, คลิกที่ “More”, เลือก Delete > Yes (การลบ Elastic Volume ต้องการทำ Detach Disk ออกจาก ECS ก่อน)

6. การจัดการ Cloud Backup and Recovery

ขอบเขตและแนวทางการให้บริการ

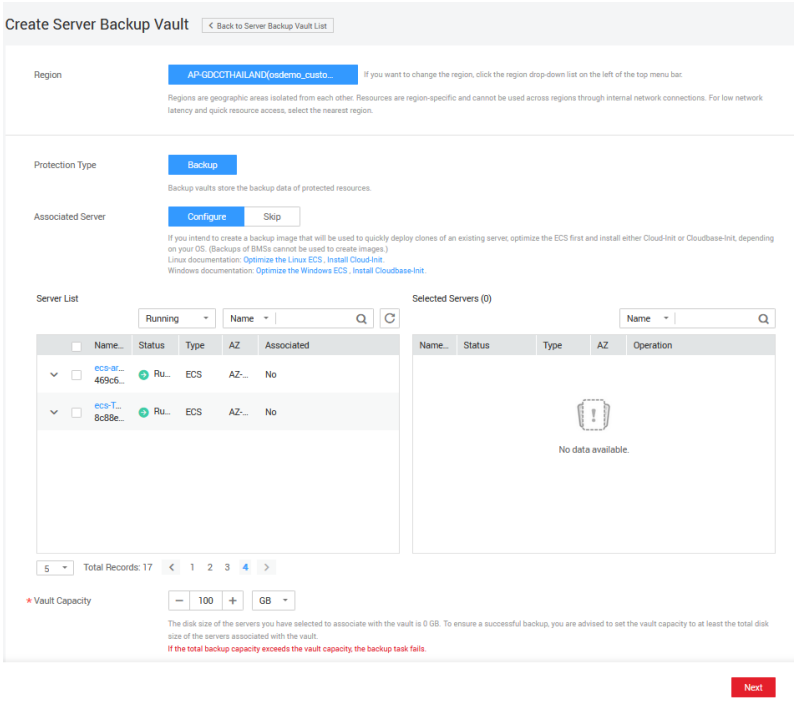
ปัจจุบันระบบมีการสำรองข้อมูล (Backup) สำหรับเครื่องแม่ข่าย (Elastic Cloud Server: ECS) โดยผู้ให้บริการ GDCC กำหนดรอบการสำรองข้อมูลเป็นรายวัน และใช้รูปแบบการสำรองข้อมูลแบบ Full ร่วมกับ Incremental เป็นค่าเริ่มต้น พร้อมจัดเก็บข้อมูลในรูปแบบ Block-level Image (Binary Disk Image) ทั้งนี้ ระบบจะจัดเก็บข้อมูลสำรองย้อนหลังเป็นระยะเวลา 7 วัน หรือเทียบเท่า 7 เวอร์ชั่น และจะดำเนินการเขียนทับ (Overwrite) ข้อมูลสำรองที่เก่าที่สุดโดยอัตโนมัติเมื่อครบกำหนดระยะเวลาการจัดเก็บ การสำรองข้อมูลของหน่วยงานแต่ละรายจะถูกกำหนดช่วงเวลาโดยระบบแบบสุ่ม จึงอาจมีเวลาการสำรองข้อมูลแตกต่างกันเพื่อลดผลกระทบต่อประสิทธิภาพการทำงานของระบบ ซึ่งข้อมูลสำรองดังกล่าวจัดเก็บไว้ ณ NT Data Center กรุงเทพมหานคร และจังหวัดนนทบุรี ทั้งนี้ หน่วยงานสามารถดำเนินการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore) ได้ด้วยตนเองผ่านหน้า Portal ในรูปแบบ Self-Service Portal.

ไปที่เมนู “**Service List**” หมวด **Storage > Cloud Backup and Recovery**



6.1 Backup

6.1.1 Automatic Backup: ไปที่ “Cloud Server Backup”คลิก“Create Server Backup Vault” และคลิก “Next” ตรง Associated Server เลือกเป็น“Configure” ด้านล่างจะมี Server List ที่เราจะสามารถเลือก ECS มาทำ Backup ได้ และกำหนด **Capacity** ของ Vault ในส่วน Automatic Association ให้เลือก “Configue” ต่อมาระบุชื่อ **Vault** , คลิก **“Next”**และ **“Submit”**

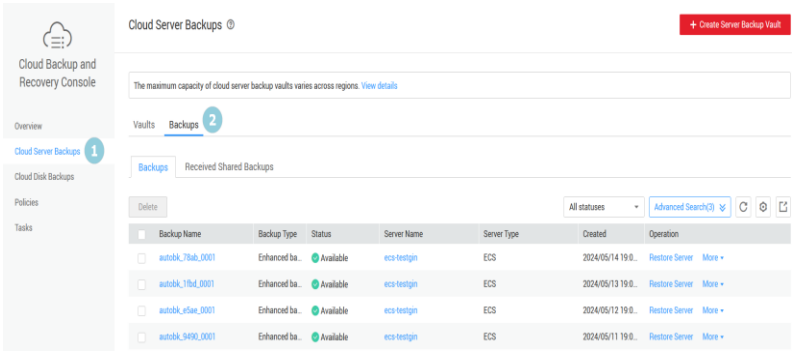


6.1.2 Manual Backup : ไปที่ “Cloud Server Backup” เลือก Vault Backup ที่ต้องการจะเพิ่ม ECS เข้าไป คลิก “More” คลิก “Perform Backup”เลือก ECS ที่อยู่ใน Server list และตั้งชื่อของ Backup และ คลิก “OK”

6.2 Recovery หรือ Restore

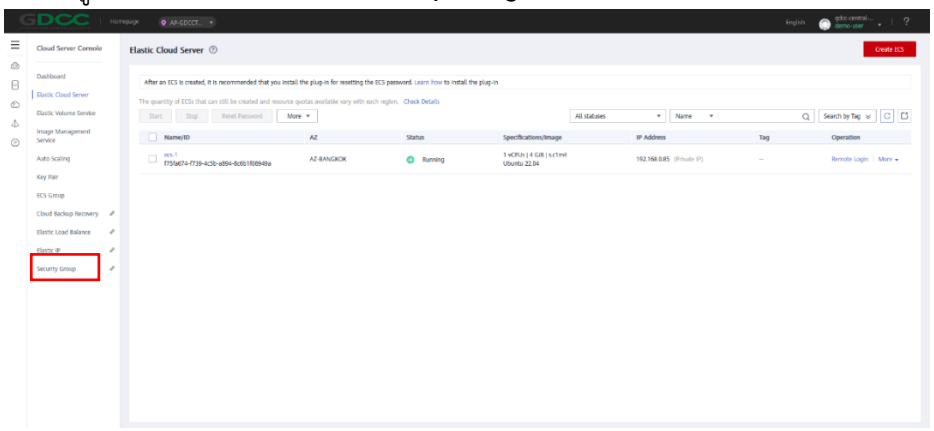
6.2.1 “Cloud Server Backup”เลือก “Backups”หน้านี้จะแสดง ECS และวันที่ทำการ Backup

6.2.2 หลังจากนั้นไปที่ ECS ที่เราเลือก “Restore Server” และ คลิก “Yes”



7. การจัดการ Security Group

7.1 ไปที่เมนู “**Service List**” หมวด **Computing > Elastic Cloud Server > Security Group**



7.2 เมื่อเข้ามาที่หน้า Security Groups แล้วให้ไปที่ “Create Security Group”

7.2.1 Name: ตั้งชื่อ security Group

7.2.2 เลือกประเภท security group

- **Custom** : จะสามารถให้ผู้ใช้งาน กำหนด Rules security group เองได้
- **General-purpose web server** : จะเป็น Rule พื้นฐาน ที่จะ Allow all inbound ICMP traffic และ allow inbound traffic port 22, 80, 443 และ 3389
- **All ports open** : จะ Allow inbound ทุก Port **(ไม่ปลอดภัย, ควรระวัง)**

7.2.3 เรียบร้อยแล้ว คลิก “OK”

7.3 วิธีการเพิ่ม Rule ใน Security Group

7.3.1เลือก security group และคลิก “Manage Rule” เมื่อเข้ามาแล้วจะมีคอลัมน์ inbound rules และ outbound rules

7.3.2 คอลัมน์ Inbound Rules คลิก “Add Rule”

- Protocol & Port: เลือก Port ที่ต้องการจะ Allow
- Source: กำหนด Source IP ก็คือ IP Address ต้นทาง
  - IP address: xxx.xxx.xxx.xxx
  - IP address/subnet mask: xxx.xxx.xxx.0/24
  - All IP address: 0.0.0.0/0

กำหนดเสร็จเรียบร้อยแล้วกด “OK”

7.3.3 คอลัมน์ Outbound Rules เบื้องต้น ขาออกจะเป็น All Ports อยู่แล้ว หรือ หากต้องการแก้ไข Rule คลิก “Add Rule”

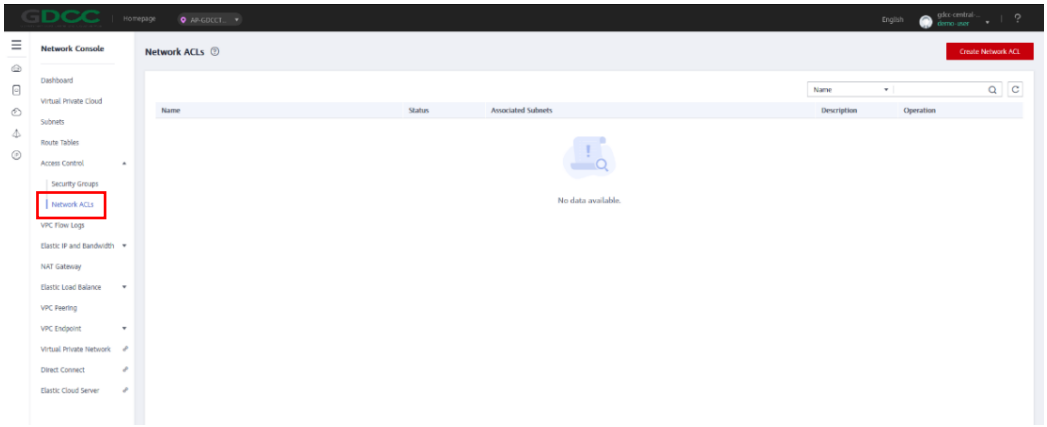
- Protocol & Port: เลือก Port ที่ต้องการจะ Allow

- Destination: กำหนด IP Address ปลายทาง ที่ต้องการจะไป
    - IP address: xxx.xxx.xxx.xxx
    - IP address/subnet mask: xxx.xxx.xxx.0/24
    - All IP address: 0.0.0.0/0

กำหนดเสร็จเรียบร้อยแล้วกด “OK”

8. การจัดการ Network ACLs

8.1 ไปที่เมนู “**Service List**” **หมวด Network > Virtual Private Cloud > Access Control > Network ACLs**



8.2 ในหน้า Network ACLs ให้ทำการคลิกไปที่ “Create Network ACL”, และคลิก “Create Now”

8.3 ทำการคลิกเลือก “Create Network ACL” จากนั้น ทำการกำหนด ชื่อ Network ACL และคลิก “OK”

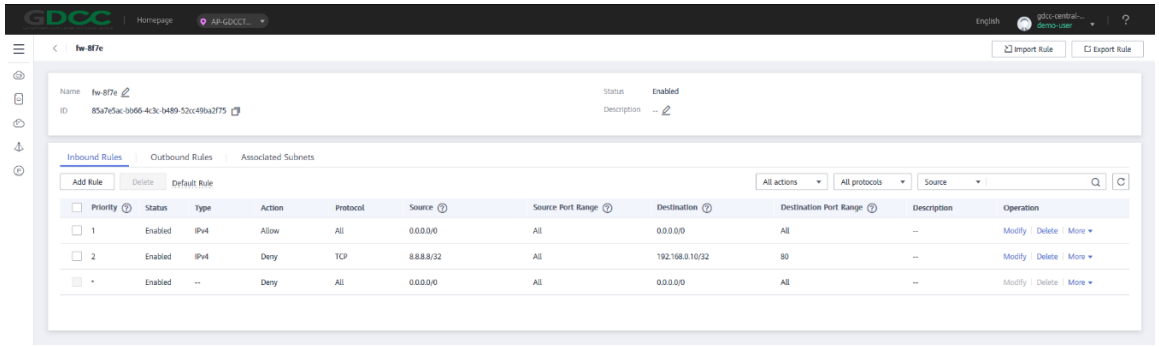
8.4 คลิก เลือก network ACL เพื่อทำการตั้งค่า Inbound Rules หรือ Outbound Rules เพื่อกำหนด network rules

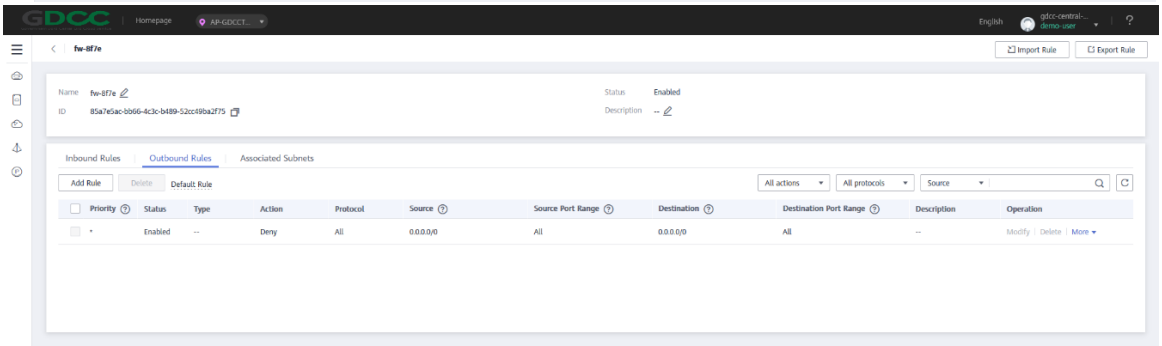
a. เลือกที่ Add Rule ตั้งค่า Inbound Rules หรือ Outbound Rules
ตั้งค่าพารามิเตอร์ ดังนี้

- Network Type: IPv4 หรือ IPv6
- Action: Allow หรือ Deny
- Protocol: สามารถทำการกำหนดโปรโตคอล ได้ เช่น TCP, UDP, All, หรือ ICMP
- Source: สามารถกำหนด IP Address ที่เป็น IP Address ต้นทาง ให้ระบบอนุญาต ให้ traffic ผ่านได้ โดยสามารถกำหนดเฉพาะเจาะจงเป็น IP address หรือ IP address range ได้ เช่น xxx.xxx.xxx.xxx/32 เป็นต้น

- Source Port Range: สามารถกำหนด source port number หรือ port number range ได้
- Destination: สามารถกำหนด IP Address ที่เป็น IP Address ปลายทาง ให้ระบบอนุญาต ให้ traffic ผ่านได้ โดยสามารถกำหนดเฉพาะเจาะจงเป็น IP address หรือ IP address range ได้
- Destination Port Range: สามารถกำหนด destination port number หรือ port number range ได้

b. จากนั้นทำการกด “OK”

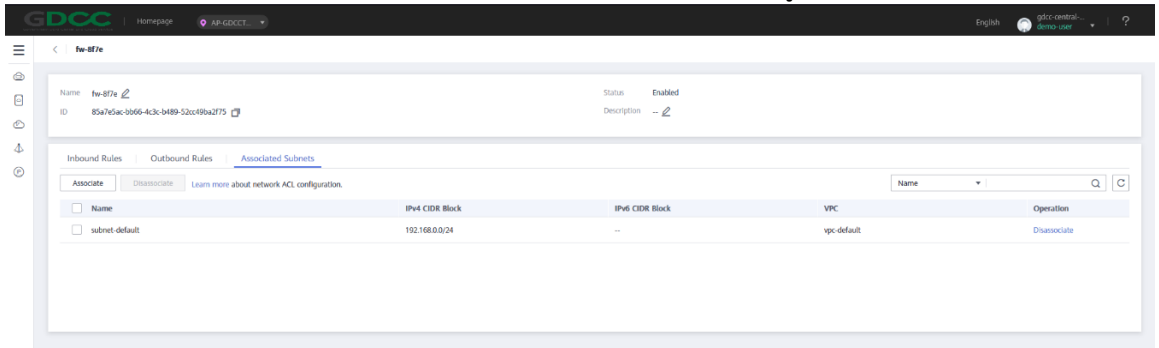




8.5 ทำการคลิกเลือก Associated Subnets tab จากนั้น เลือก “Associate”

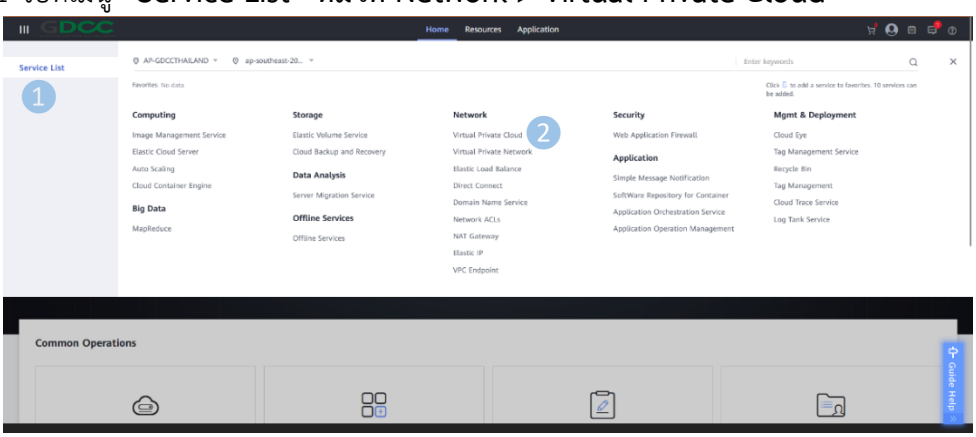
8.6 ทำการเลือก subnets ที่ต้องการเชื่อมต่อ กับ network ACL ที่ต้องการ จากนั้นคลิก “OK”

(**ข้อควรทราบ:** แต่ละ subnet จะสามารถ เชื่อมต่อหรือ associated ได้เพียงหนึ่ง network ACL เท่านั้น และหากต้องการยกเลิกการเชื่อมต่อ สามารถเลือกเมนู Disassociate เพื่อทำการยกเลิกได้)



9. การสร้าง Virtual Private Cloud (VPC)

9.1 ไปที่เมนู “Service List” หมวด Network > Virtual Private Cloud

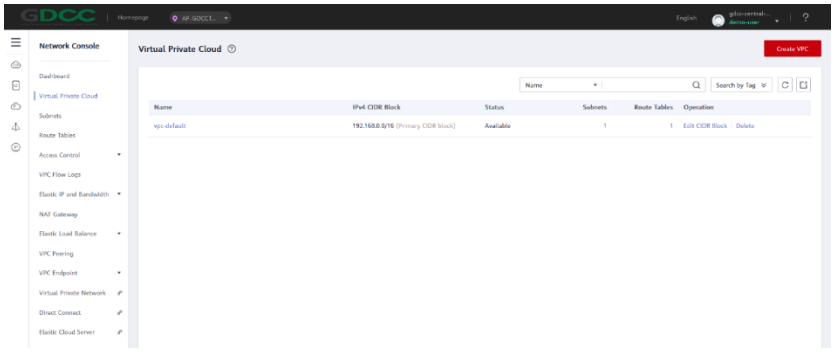


9.2 ในหน้าต่าง Virtual Private Cloud ให้ทำการคลิก “Create VPC”

9.3 การตั้งค่าพื้นฐานของ VPC นั้น สามารถเลือก Region (Project name) และทำการตั้งชื่อ VPC ตั้งค่า IPV4 CIDR Block

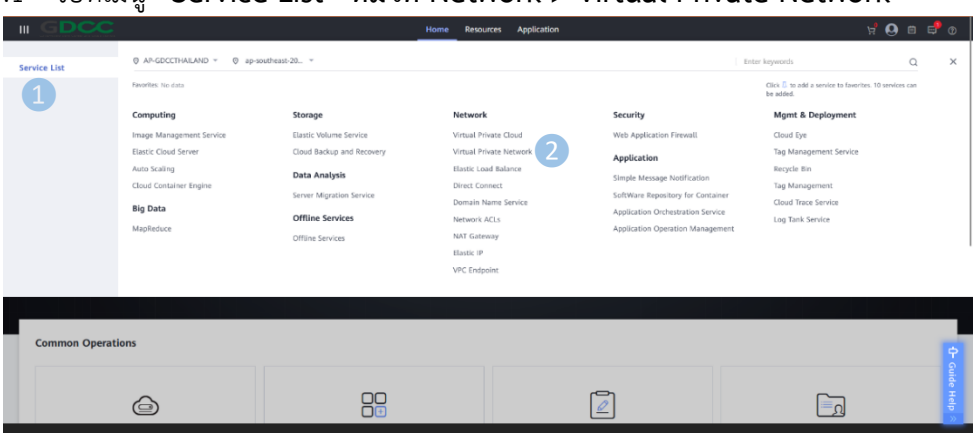
9.4 การตั้งค่าพื้นฐานของ Subnet ให้ทำการเลือก AZ, Name เพื่อกำหนดค่า default subnet กำหนดค่า IPV4 CIDR Block จากนั้น คลิก “Create Now”

9.5 ทำการรอ จนกระทั่งระบบ สร้าง VPC แล้วเสร็จ เมื่อเสร็จแล้ว ระบบจะแสดงผลลัพธ์ ดังภาพ



10. การสร้าง Virtual Private Network (VPN)

10.1 ไปที่เมนู “Service List” หมวด Network > Virtual Private Network



10.2 ทำการคลิกที่แถบ “VPN Gateway” แล้ว คลิก “Create VPN Gateway”.

a. ทำการสร้าง VPN Gateway

- ระบุชื่อ VPN Gateway แล้วเลือก “VPC”, เลือก “Bandwidth”ที่ต้องการ

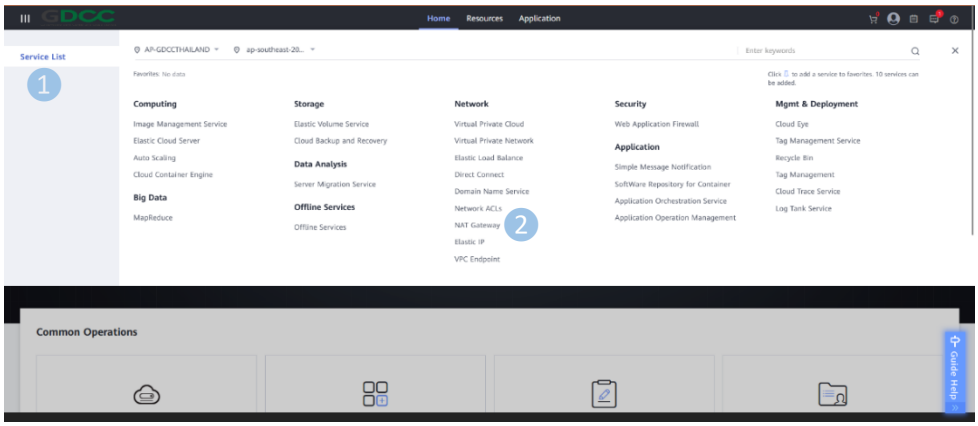
b. ทำการสร้าง VPN Connection

- ระบุชื่อ VPN Connection, จากนั้นเลือก “Local Subnet” ใส่ข้อมูล IP Remote Gateway, Remote Subnet และ PSK สำหรับ VPN Connection.
- นอกจากนี้สามารถทำการตั้งค่า Advanced Settings เพิ่มเติม เพื่อกำหนดพารามิเตอร์ ในการเชื่อมต่อ VPN Remote Gateway ได้ โดยกำหนด Policy IKE และ IPSEC เพิ่มเติม จากนั้นคลิก “Next” และกด “Submit”

11. การจัดการ NAT Gateway

- ในส่วนของฟังก์ชั่นการทำงานของ SNAT จะทำการแปลงค่า private IP addresses ให้เป็น EIPs, เพื่ออนุญาตให้ servers ภายใน VPC นั้น ๆ สามารถทำการ share EIP เพื่อใช้ในการเข้าถึงระบบอินเทอร์เน็ต ได้ อย่างปลอดภัยและมีประสิทธิภาพ
- ในส่วนของ ฟังก์ชั่น การทำงานของ DNAT จะเป็นการเปิดให้ servers ภายใน VPC นั้น ๆ share EIP เพื่อให้สามารถเข้าถึงได้จากอินเทอร์เน็ตภายนอก ผ่าน IP address หรือ port ที่ทำการกำหนดไว้

11.1 ให้ทำการคลิกด้านบนของ tenant portal แล้วเลือกเมนู “Service List” จากนั้นเลือก Network > NAT Gateway



11.2 ในหน้าต่างของ NAT Gateway ให้ทำการคลิก “Create Public NAT Gateway”

11.3 ทำการกำหนด Region (Project name) และ NAT Gateway Name, เลือก VPC, เลือก Subnet, เลือก NAT Gateway Type และทำการคลิก “Create Now” แล้วกด “Submit”

11.4 เมื่อทำการสร้าง NAT gateway เรียบร้อยแล้วให้ทำการ “Add Rule”

11.5 ในส่วนของการ Add SNAT rule เพื่ออนุญาตให้ servers ใน VPC สามารถเชื่อมต่อไปยังอินเทอร์เน็ต ผ่าน การ EIP ที่ถูกจัดสรรมา

a. คลิก “Add SNAT Rule”
b. เลือก Subnet, เลือก EIP และกด“OK”

11.6 ในส่วนของการ DNAT rule to เพื่ออนุญาตให้ servers ใน VPC เข้าถึงได้จากภายนอก

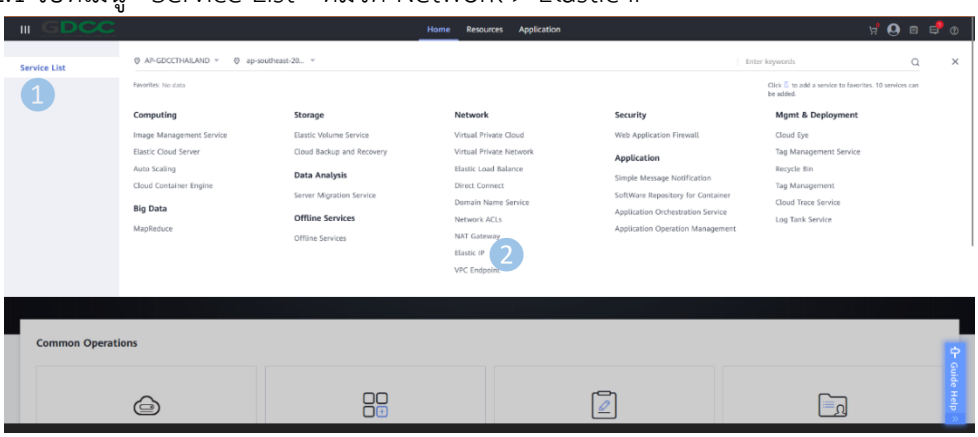
a. คลิก “Add DNAT Rule”
b. Port Type สามารถใช้ All ports เพื่ออนุญาตทั้งหมด หรือจำกัดเฉพาะบาง port ได้
    - All ports: หมายถึง port ทั้งหมด ที่มีการ requests บน EIP จะถูก forwarded โดย NAT gateway ตาม server IP address ที่ได้ตั้งค่าไว้
    - Specific port: หมายถึง protocol หรือ port ใด ๆ ที่มีการกำหนดไว้ จะถูก forwarded โดย NAT gateway ที่อยู่บน EIP ไปยัง server ปลายทางตามที่มีการกำหนดไว้
c. Protocol
    - All ports: ตั้งค่าพารามิเตอร์ไว้ทั้งหมดทุก ports เป็นค่า default
    - Specific port: ระบุเฉพาะบาง port หรือบาง port type
d. EIP: กำหนด EIP สำหรับการเข้าถึง services ผ่านอินเทอร์เน็ต
e. Outside Port: กำหนด port ของ EIP
f. Private IP Address: กำหนด private IP address ของ server ที่ต้องการให้เข้าถึง service ผ่านอินเทอร์เน็ต ผ่าน DNAT rule

g. Inside Port: กำหนด port ของ cloud server

h. คลิก “OK”

12. การจัดการ Elastic IP

12.1 ไปที่เมนู “Service List” หมวด Network > Elastic IP



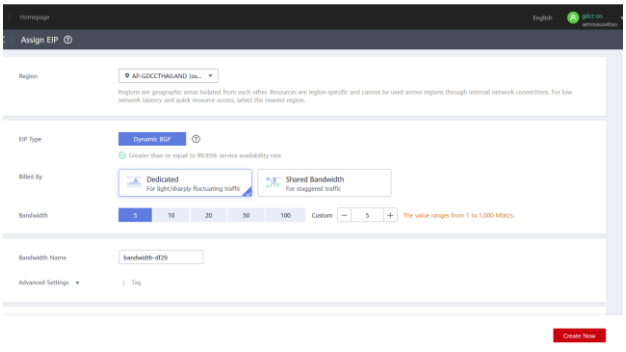
12.2 ในหน้าต่าง EIPs ให้ทำการคลิก “Assign EIP”

12.3 ทำการเลือก Region (Project name)

12.4 กำหนด “Bandwidth” size

12.5 กำหนด “Bandwidth Name” และ “Quantity” และ “Create Now” และ “Submit”

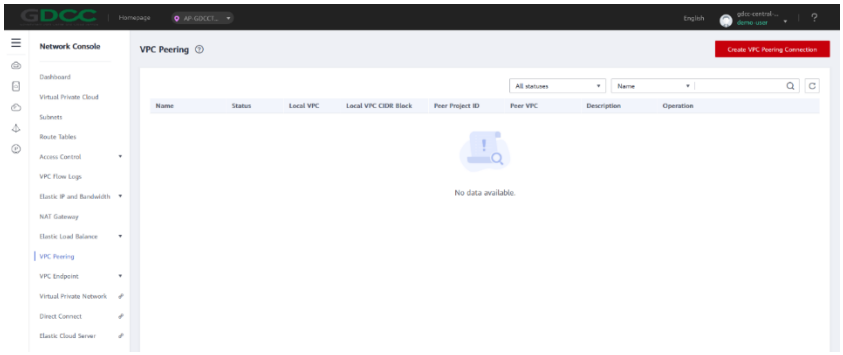
12.6 ในหน้า EIPs ให้ทำการคลิก “Bind”, จากนั้นเลือก instance ที่จะกำหนด bind EIP และคลิก “OK”



13. การสร้าง VPC Peering

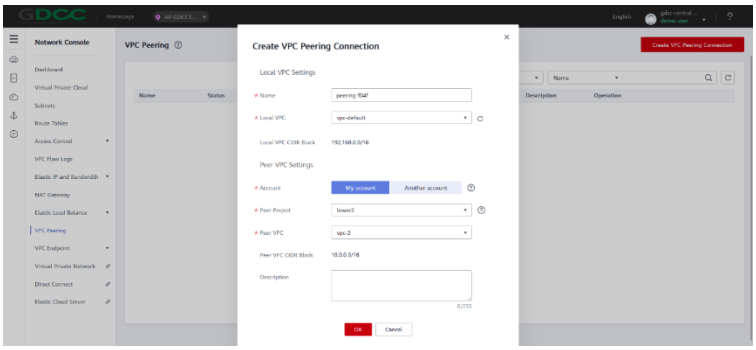
13.1 ไปที่เมนู “Service List” หมวด “Virtual Private Cloud”

13.2 คลิกที่แถบ “VPC Peering” แล้วคลิก“Create VPC Peering Connection”

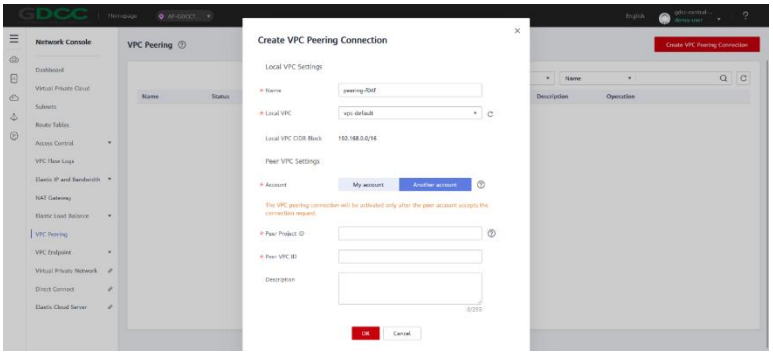


13.3 ระบบจะแสดงหน้าต่าง Create VPC peering Connection ให้ดำเนินการดังนี้

a. ทำการสร้าง VPC Peering connection เพื่อเชื่อมต่อกับ VPC อื่นๆ ภายใน Project



b. ทำการสร้าง VPC Peering Connection เพื่อเชื่อมต่อไปยัง VPC อื่นๆ



13.4 การตั้งค่าพารามิเตอร์ เพื่อเชื่อมต่อระหว่าง VPC connection กับ VPC อื่นๆ ภายใน Tenant เดียวกัน

a. Name: กำหนดชื่อ VPC peering connection

b. Local VPC: กำหนด local VPC โดยสามารถเลือกได้จาก รายการที่ขึ้นใน drop-down list

c. My Account: การเชื่อมต่อ VPC peering connection จะสร้างได้ระหว่าง VPCs ตั้งแต่ 2 VPC ขึ้นไปใน region เดียวกัน ภายใน account เดียวกัน

d. Peering Project: การกำหนดชื่อ project name จะเป็นค่ามาตรฐานที่ระบบกำหนดให้

e. Peer VPC: สามารถเลือก รายการต่าง ๆ ใน Peer VPC เพื่อกำหนดการเชื่อมต่อระหว่าง 2 VPC ภายใน account เดียวกัน

การสร้าง VPC Peering Connection สำหรับ VPC Tenant อื่น

a. Name: กำหนดชื่อ VPC peering connection

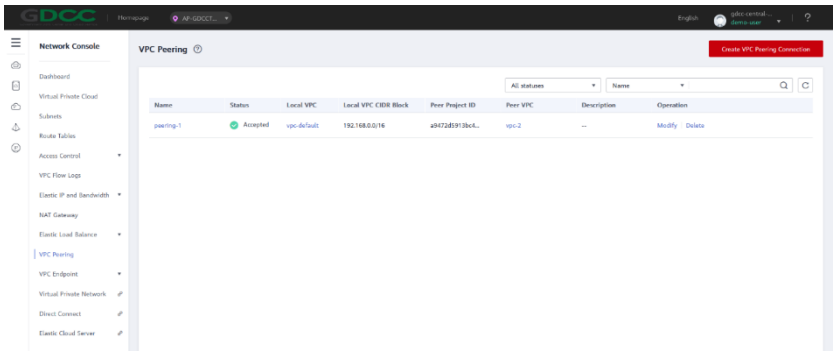
b. Local VPC: กำหนด local VPC โดยสามารถเลือกได้จาก รายการที่ขึ้นใน drop-down list.

c. Another account: การเชื่อมต่อ VPC peering connection จะสร้างได้ระหว่าง VPCs ตั้งแต่ 2 VPC ขึ้นไป แต่จะต้องอยู่ใน region เดียวกัน

d. Peer Project ID: ไปที่มุมขวาบนของหน้าจอ คลิกชื่อผู้ใช้ของคุณ เลือก "My Settings" และคัดลอก Resource Sets ID

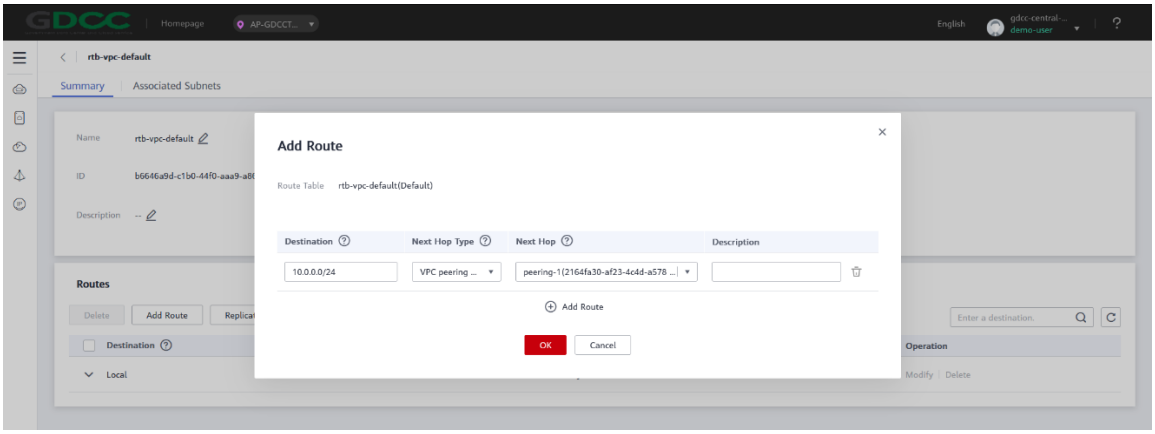
e. Peer VPC ID: กำหนด VPC ID สำหรับ peering

13.5 หลังจากการตั้งค่าพารามิเตอร์เรียบร้อยแล้ว ให้ทำการกด “OK” จากนั้นทำการรอเพื่อให้ระบบทำการ VPC Peering เมื่อเสร็จสิ้นกระบวนการแล้วระบบจะแสดงผล ดังภาพ



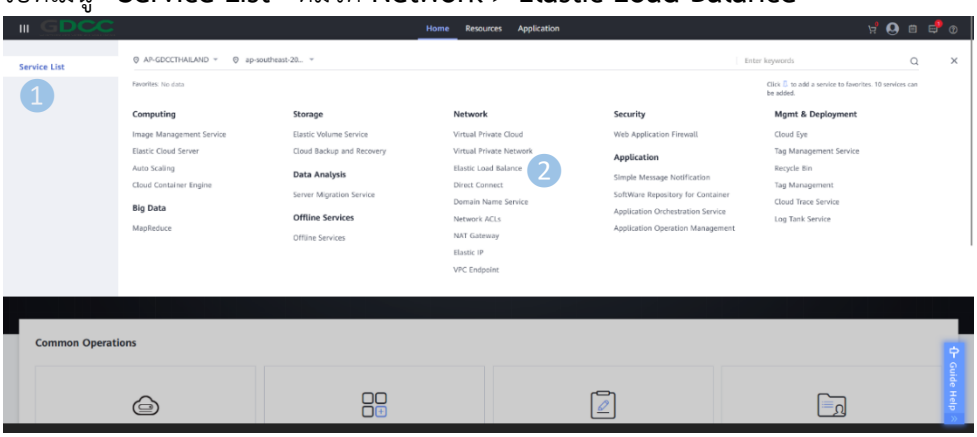
13.6 การ Add Route สำหรับ VPC Peering Connection

a. คลิก VPC Peering ที่ทำการสร้างไว้ก่อนหน้านี้ จากนั้นคลิกเลือก “Route Tables” และคลิก “Add Route” ทำการระบุ IP Destination routes สำหรับการเชื่อมต่อไปยัง VPC อื่นๆ ภายใน account เดียวกัน .ตั้งค่า “Next Hop Type” เป็น VPC Peering Connection เลือก Next Hop ที่ต้องการ และ คลิก OK เพื่อบันทึก



14. การสร้าง Elastic Load Balance

ไปที่เมนู “**Service List**” หมวด **Network** > **Elastic Load Balance**



14.1 การสร้าง Elastic Load Balancer

14.1.1 คลิก “Create Elastic Load Balancer” จากนั้นทำการตั้งค่าพารามิเตอร์ ดังนี้

a. Region: ทำการกำหนด region

b. AZ: ทำการกำหนด หนึ่ง หรือหลาย AZs สำหรับ load balancer

c. Network Type: ทำการกำหนด network สำหรับการทำงานของ load balancer

- Public IPv4 network
- Private IPv4 network
- IPv6 network

d. VPC: กำหนด VPC ที่จะทำ load balancer

e. EIP: กำหนด EIP หากเป็นการเลือก load balancer เป็น Public IPv4

f. Subnet: กำหนด Subnet เพิ่มเติมหากเป็นการทำงานของ load balancer ที่เป็น Private IPv4 network หรือ IPv6 network.

g. Name: กำหนดชื่อ load balancer

14.1.2 คลิก “Create Now”

14.1.3 ทำการยืนยันการตั้งค่า จากนั้นกด “Submit”

14.2 การสร้าง Listeners

14.2.1 ในหน้าต่าง Load Balancers ให้ทำการคลิก Load Balancer ที่ทำการสร้างไว้ก่อนหน้านี้แล้ว ให้คลิก “Listeners tab” แล้วทำการ “Add Listener” เพื่อตั้งค่าพารามิเตอร์ ดังนี้

a. Name: กำหนดชื่อ Listener

b. Frontend Protocol/Port: เลือกโปรโตคอล TCP หรือ UDP สำหรับ load balancing ที่อยู่ใน Layer 4 จากนั้นเลือก HTTP หรือ HTTPS เพื่อทำ ใน Layer 7 (OSI Model)

14.2.2 คลิก “Next”

14.2.3 คลิก Backend Server Group โดยทำการเลือก “Create new” เพื่อสร้างใหม่ หรือเลือกที่สร้างไว้อยู่แล้วโดยกดที่ “Use existing”

a. Name: กำหนด Backend Group

b. Backend Protocol: กำหนดโปรโตคอลโดยใช้ backend servers ที่จะให้ receive requests

c. Load Balancing Algorithm: กำหนดอัลกอลิทึม สำหรับ load balancer เพื่อใช้สำหรับการกระจายโหลดของข้อมูล (ตัวอย่างการตั้งค่า เช่น Weighted round robin, หรือ Weighted least connections หรือ Source IP hash).

14.2.4 คลิก “Finish”

14.3 สร้าง Backend Server Groups

14.3.1 ในหน้าต่าง Load Balancers คลิกที่ Load Balancer ที่สร้างไว้ก่อนหน้านี้ จากนั้นคลิกที่แถบ “Backend Server Groups”

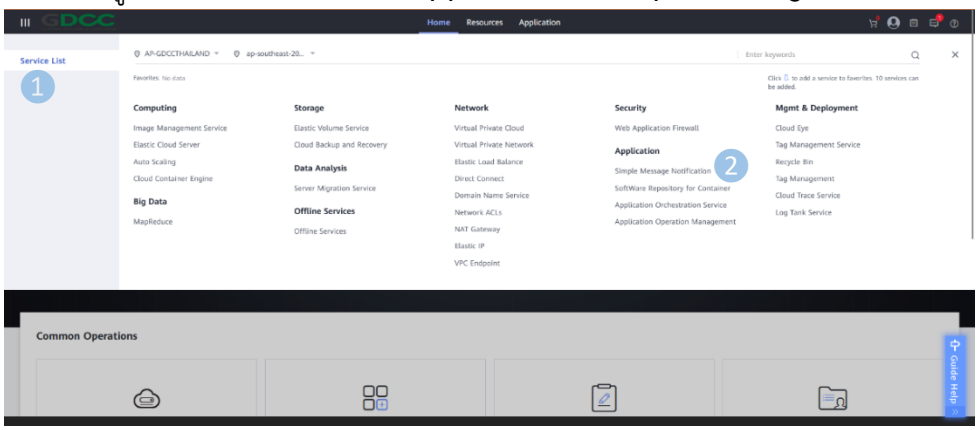
14.3.2 เลือก Backend Server ที่สร้างไว้ใน ข้อที่ “14.3.1” แล้วคลิก “Add”

14.3.3 เลือก ECS เพื่อทำการเพิ่มใน backend server group จากนั้นคลิก “Next”

14.3.4 กำหนด Port ต่าง ๆ สำหรับ ECS ที่ใช้ใน backend server group และทำการกด “Finish”

15. การสร้าง Simple Message Notification

15.1 ไปที่เมนู “Service List” หมวด Application > Simple Message Notification



15.2 ทำการสร้าง “Topics”ก่อน คลิกไปที่ “Create Topic”

a. Topic Name : กำหนดชื่อ topic

b. Display Name : หัวข้อที่แจ้งไปทาง Email

15.3 คลิก “OK”

15.4 ไปที่แท็บ “Subscriptions”คลิก “Add Subscription”

a. เลือก Topic Name ที่ได้ทำการสร้าง

b. เลือก Protocol เพื่อแจ้งเตือนไปยัง Email

c. กำหนด Endpoint

15.5 เสร็จเรียบร้อยแล้วแล้วคลิก“OK”

16. การสร้าง Auto Scaling

16.1 ไปที่เมนู“Service List” หมวด Computing > Auto Scaling

16.2 คลิกที่ “Create AS Configuration”

- Name: ตั้งชื่อ ECS
- Configuration Template: เลือกวิธีในการ Scale

Create new Specifications template : จะเป็นการสร้างเครื่องขึ้นมาใหม่โดยจะใช้ OS , resource ตามที่เราตั้งค่าไว้

Use Specifications of an exiting ECS : หากเครื่องที่ได้เลือกไว้ มีการใช้ทรัพยากรสูง ระบบจะทำการสร้างเครื่องมาให้อัตโนมัติโดยเครื่องจะสร้างขึ้น OS และ resource จะเหมือนกับเครื่องหลัก

- กำหนด Image OS , Disk, Security Group

- EIP: กำหนด EIP ว่าต้องการให้ Auto assign หรือไม่
- Login Mode: เลือกวิธีการใส่รหัสผ่านจะเป็นแบบ “Password” หรือ “key pair”

16.3 คลิก “Create Now”

16.4 คลิก “Create AS Group”

- AZ: เลือก AZ
- Name: กำหนดชื่อ AS group
- Max. Instances: ระบุจำนวนการ scale จะสามารถสร้างเครื่องสูงสุดได้กี่เครื่อง
- Expected Instances: หากค่านี้มากกว่าที่ตั้งไว้ระบบจะดำเนินการปรับขนาดอัตโนมัติเพื่อเพิ่มจำนวนเครื่อง
- Min. Instances: กำหนดการ scale อย่างต่ำ
- AS Configuration: เลือก AS Configuration Template ที่เราได้ทำการสร้างไว้
- VPC: เลือก VPC สำหรับ ECS
- Subnet: เลือก subnet สำหรับ ECS
- Load Balancing: กำหนดว่าจะเลือกให้มีการใช้ Elastic Load Balancer หรือไม่
- Instance Removal Policy:จะเป็นการกำหนด Policy เวลามีการสร้างเครื่องขึ้นมาใหม่
- EIP: จะลบ EIP ทิ้งเลยไหมเมื่อไม่ใช้งาน
- Health Check Method: เลือก ECS health check หรือ ELB health check
- Health Check Interval: กำหนดเวลาของการ health check AS group

16.5 คลิก “Create Now”

17. การสร้าง Web Application Firewall (WAF)

17.1 ไปที่เมนู “**Service List**” **หมวด Security > Web Application Firewall**

17.2 ในหน้าต่าง Web Application Firewall ให้คลิก “Create WAF” เลือก “Region” คลิก “Next” และคลิก “Back to Website Settings” จากนั้นใส่ข้อมูล domain names ที่จะทำการป้องกันการโจมตี

17.3 การเพิ่ม Domain Name ใน Web Application Firewall (WAF)

a. คลิก “Add Website”และ คลิก“OK”

b. ตั้งค่า Domain Name

c. ตั้งค่า Server Configuration

- Client Protocol: เป็นโปรโตคอล ที่ใช้สำหรับให้ผู้ใช้บริการเว็บไซต์ใช้ในการเข้าถึง server.

- Server Protocol: เป็นโปรโตคอล ที่ใช้สำหรับให้ Web Application Firewall (WAF) forward ไปตามที่ผู้ใช้บริการเว็บไซต์ร้องขอ
- Server Address: กำหนด public IP address หรือ domain name สำหรับ web server เพื่อให้ผู้ใช้บริการเว็บไซต์เข้าถึง

(เพิ่มเติม) การ Import a certificate

หากผู้ใช้บริการเว็บไซต์มีการตั้งค่าการเข้าถึงโดยใช้ HTTPS ให้ดำเนินการเพิ่ม Certificate ดังนี้

- คลิก “Import New Certificate” จากนั้นทำการกำหนดชื่อ certificate และวางไฟล์ certificate และ private key ลงใน text box.
- จากนั้นกด “OK”

d. ทำการตั้งค่า Proxy โดยค่ามาตรฐานเดิมจะมีค่าเป็น No

e. คลิก “Next”. หากทำการเพิ่ม Domain name เสร็จเรียบร้อยแล้ว ข้อมูลของ domain จะถูกเพิ่มเข้าไปในระบบ Web Application Firewall (WAF)

f. การตั้งค่า CNAME record กรณีมีการใช้ DNS provider ที่ให้บริการภายนอกนั้น สามารถทำการคัดลอก CNAME record นี้ที่ถูกสร้างขึ้นในระบบนี้ เพื่อส่งแจ้งให้ DNS provider ได้

g. คลิก “Next” และกด “Finish”

17.4 การเพิ่ม Policy

a. เลือกในเมนูด้านซ้ายของแถบหน้าต่าง Web Application Firewall ให้เลือกที่เมนู “Policies”

b. คลิก “Add Policy”

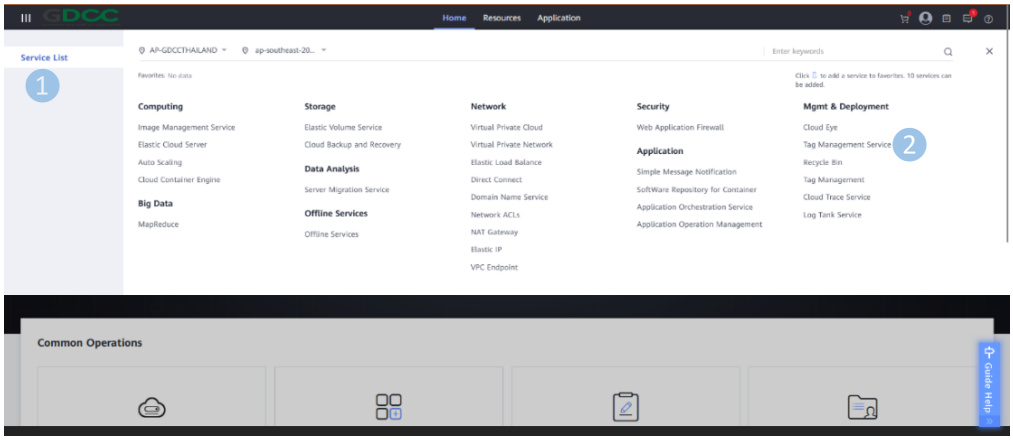
c. กำหนดชื่อ policy แล้วคลิก “OK”

d. คลิก “Add Domain Name” และเลือก Domain Name ที่จะใช้ policy นี้

e. เลือก policy name และทำการ add เพิ่ม rule ใน policy

18. การสร้าง Tag Management Service

18.1 ไปที่ “Service List” หมวด Management & Deployment > Tag Management Service



18.2 ในหน้าต่าง Tag Management Serviceให้คลิก “Predefined Tags”สร้าง Tags เพื่อที่จะนำไปผูกแยกประเภททรัพยากร