

ใบงานที่ 5

Networking Concepts

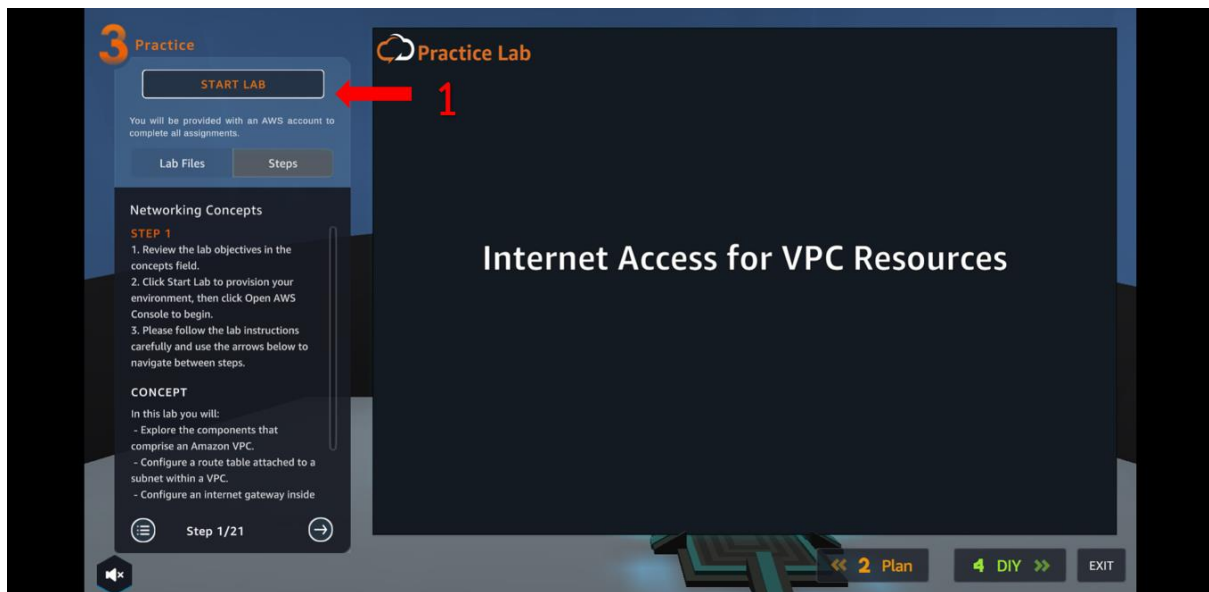
จุดประสงค์

1. กำหนดค่าตารางเส้นทางและแนบอินเทอร์เนตเกตเวย์
2. กำหนดค่ากลุ่มความปลอดภัย

เครื่องมือและอุปกรณ์การทดลอง

1. คอมพิวเตอร์ 1 เครื่อง

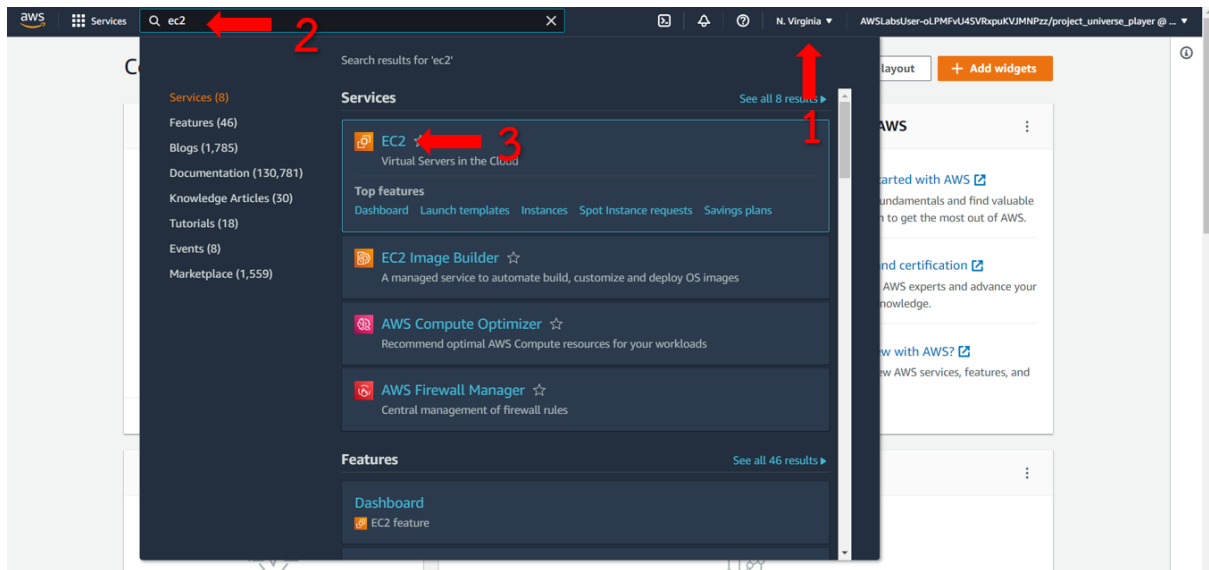
ลำดับขั้นตอนการทดลอง



รูปที่ 1 Step 1

STEP 1 :

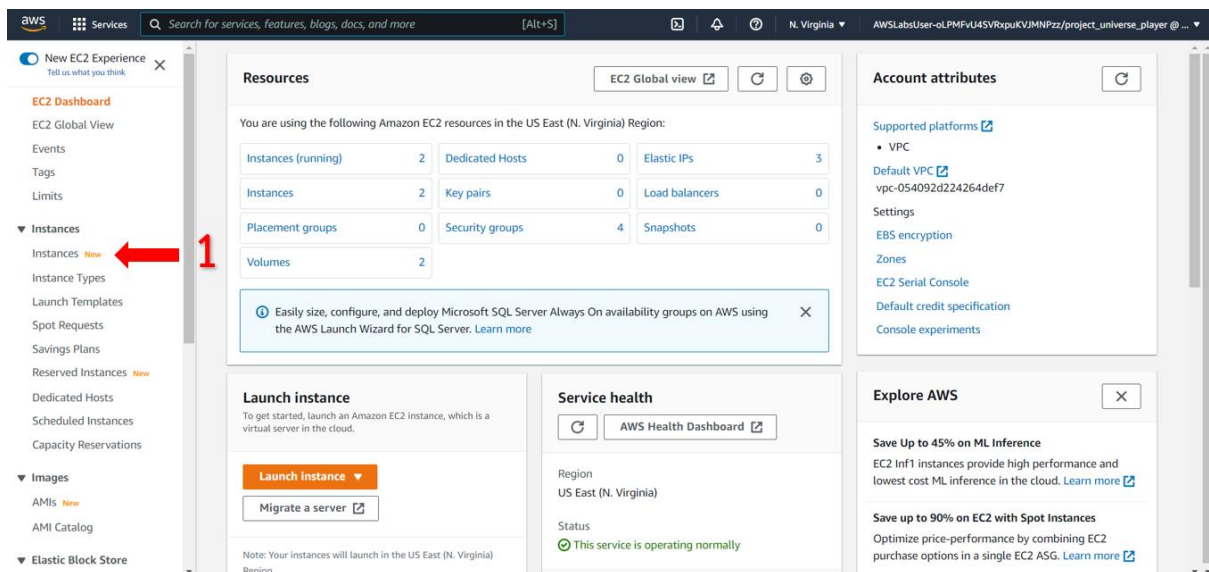
1. กด START LAB เพื่อเริ่ม
2. กด Open AWS Console



รูปที่ 2 Step 2

STEP 2 :

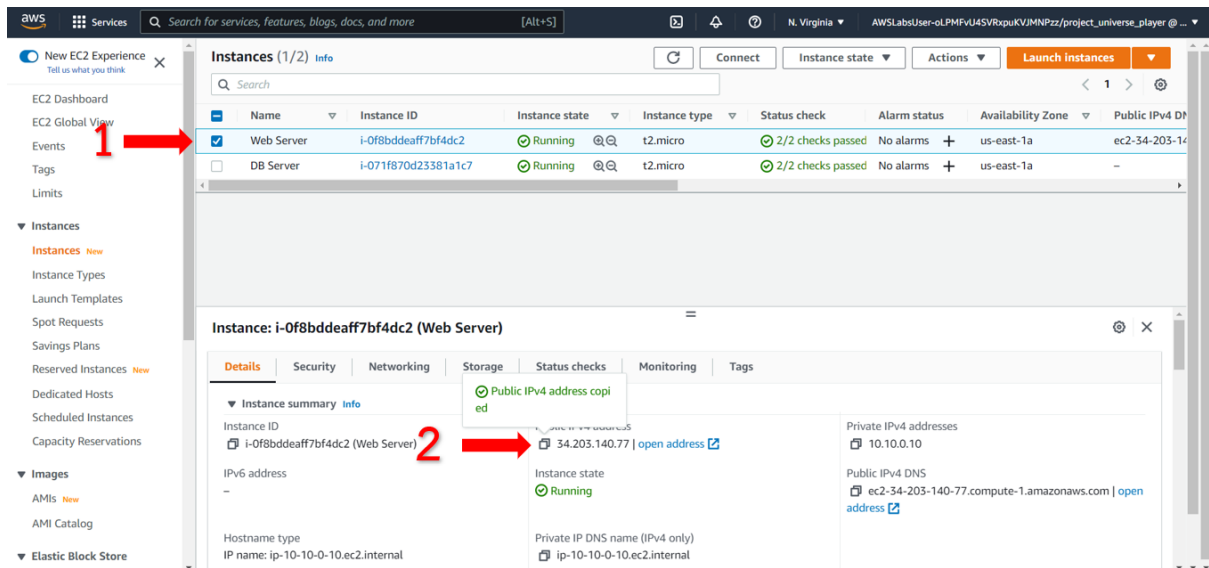
1. เปลี่ยนให้เป็น N. Virginia
2. พิมพ์ EC2 ในช่องค้นหา
3. กดตัวเลือก EC2



รูปที่ 3 Step 3

STEP 3 :

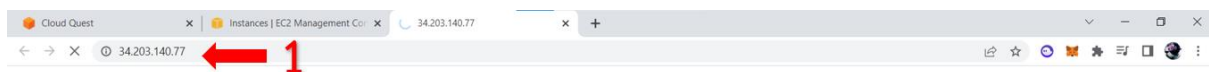
1. กดที่ Instances



รูปที่ 4 Step 4

STEP 4 :

1. เลือกหัวข้อ Web Server
2. กดคัดลอก Public IPv4 address



ไม่สามารถเข้าถึงเว็บไซต์นี้

34.203.140.77 ไม่สามารถเชื่อมถึงกันนานเกินไป

ลอง:

- ตรวจสอบการเชื่อมต่อ
- ตรวจสอบหรือแก้ไขไฟร์วอลล์
- เรียกใช้การวินิจฉัยเครือข่ายของ Windows

ERR_CONNECTION_TIMED_OUT

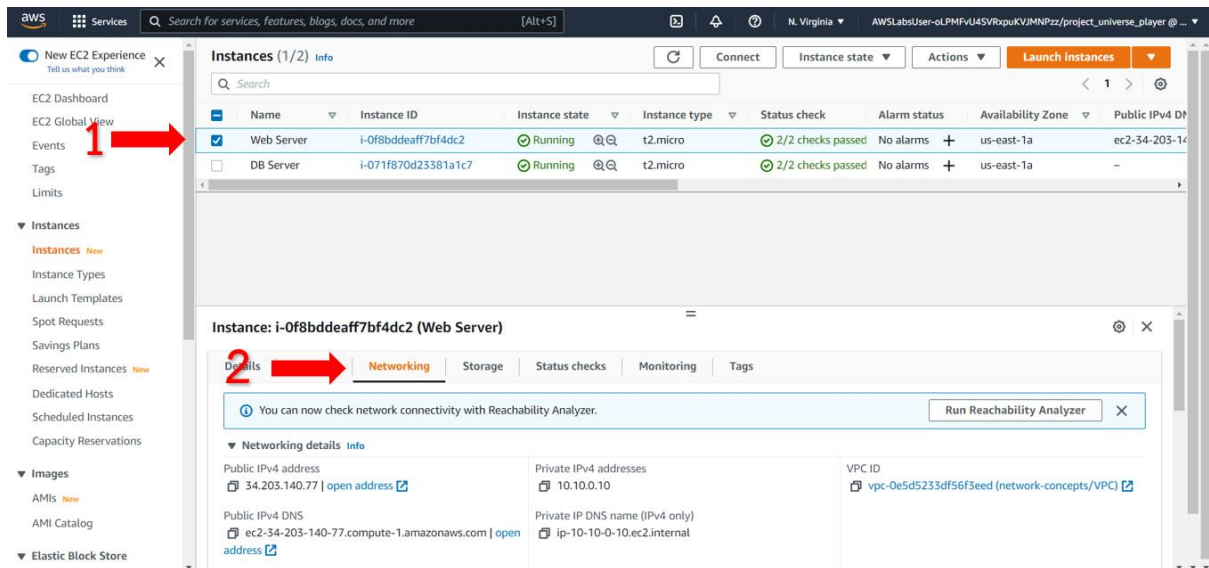
โหลดใหม่

รายละเอียด

รูปที่ 5 Step 5

STEP 5 :

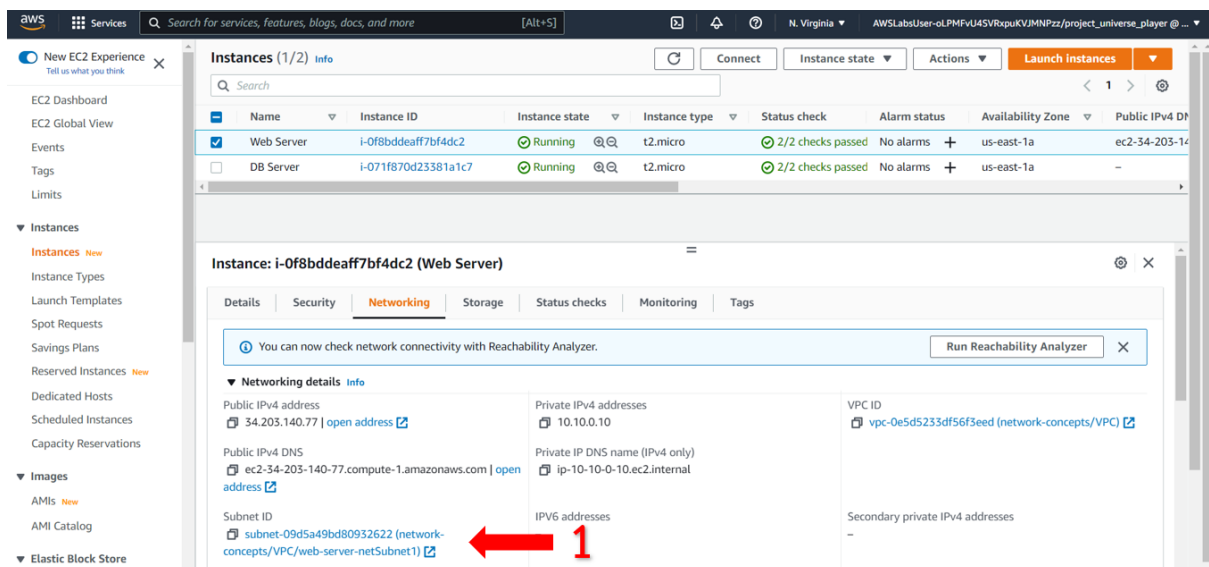
1. วาง Public IPv4 address ในช่องค้นหาหน้าต่าง Browser ใหม่ แล้วกด Enter



รูปที่ 6 Step 6

STEP 6 : Amazon VPC ช่วยให้คุณสามารถเปิดใช้ทรัพยากร AWS ในเครือข่ายเสมือน

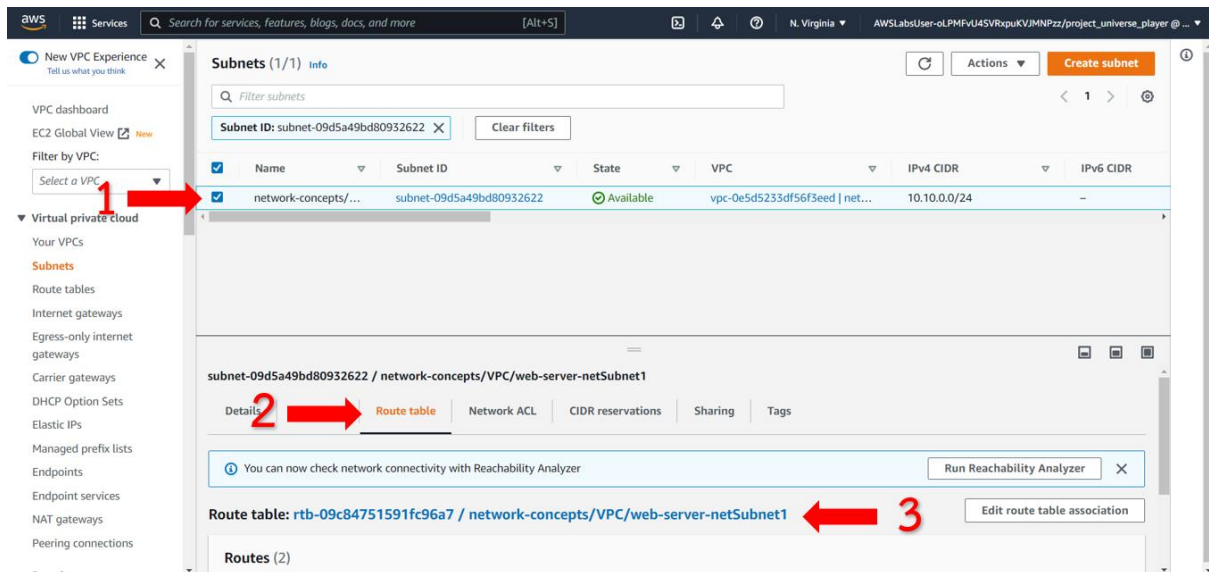
1. เลือกหัวข้อ Web Server
2. เลือกหัวข้อ Networking



รูปที่ 7 Step 7

STEP 7 : Subnet คือช่วงของที่อยู่ IP ใน VPC ของคุณ คุณสามารถเปิดใช้ทรัพยากร AWS ใน Subnet ที่ระบุได้ แต่ละ Subnet ต้องอยู่ภายใน Availability Zone เดียวและไม่สามารถขยายโซนได้

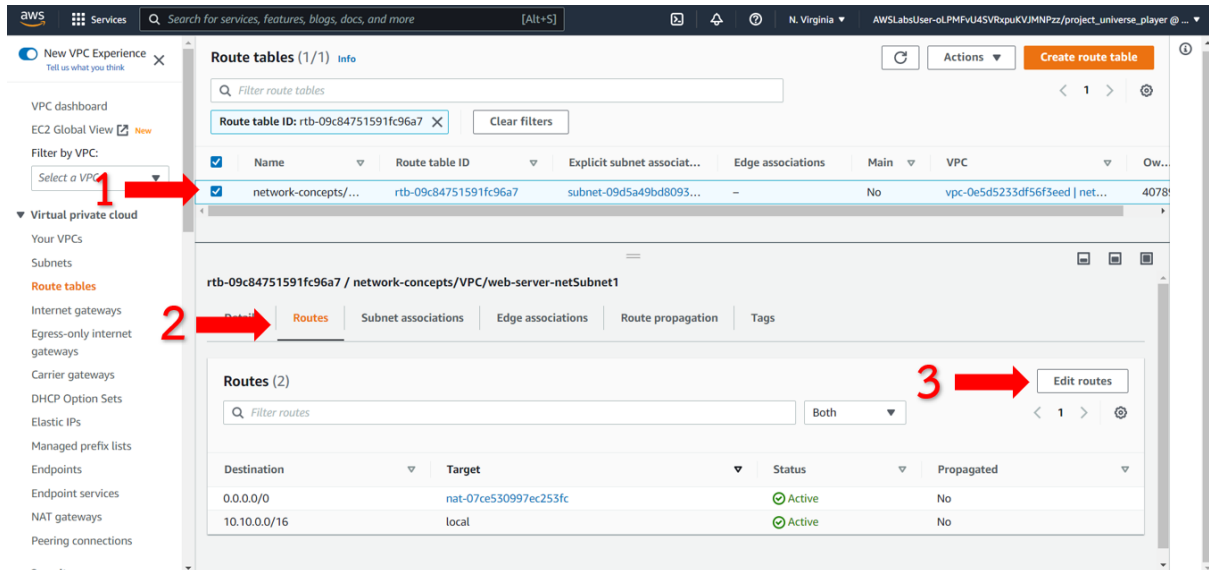
1. กดที่ Subnet ID



รูปที่ 8 Step 8

STEP 8 : ตารางเส้นทางประกอบด้วยชุดของกฎที่เรียกว่า Routes ซึ่งใช้เพื่อกำหนดว่า ทราฟฟิกเครือข่ายจาก ซับเน็ตหรือเกตเวย์ของคุณถูกนำไปที่ใด

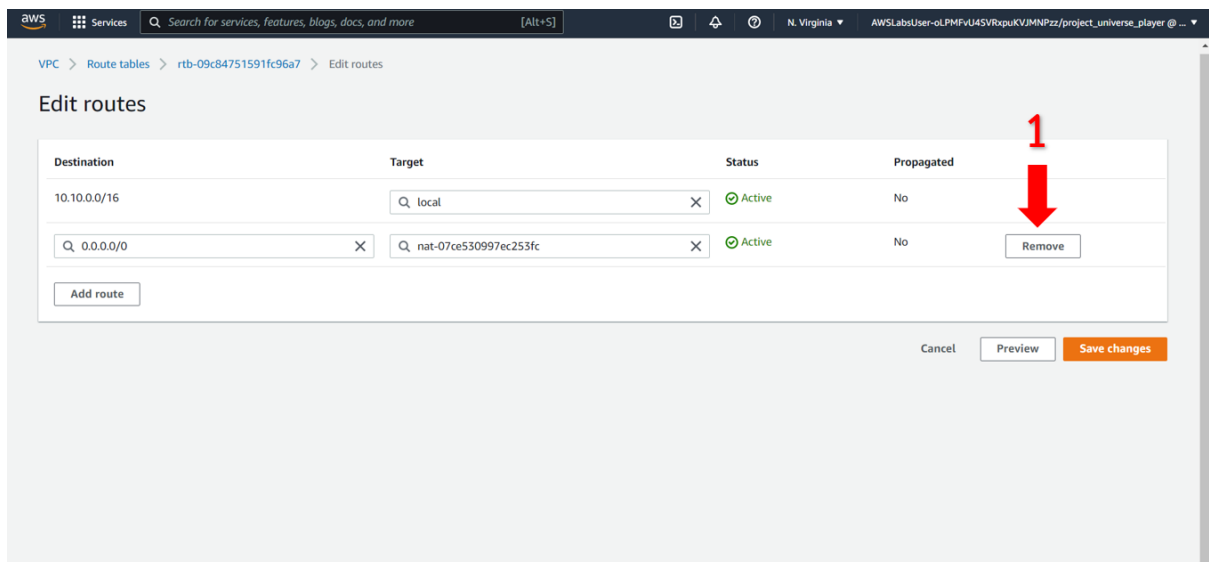
1. เลือกหัวข้อ network-concepts
2. เลือกหัวข้อ Route table
3. กดที่ Route table ลิงก์



รูปที่ 9 Step 9

STEP 9 :

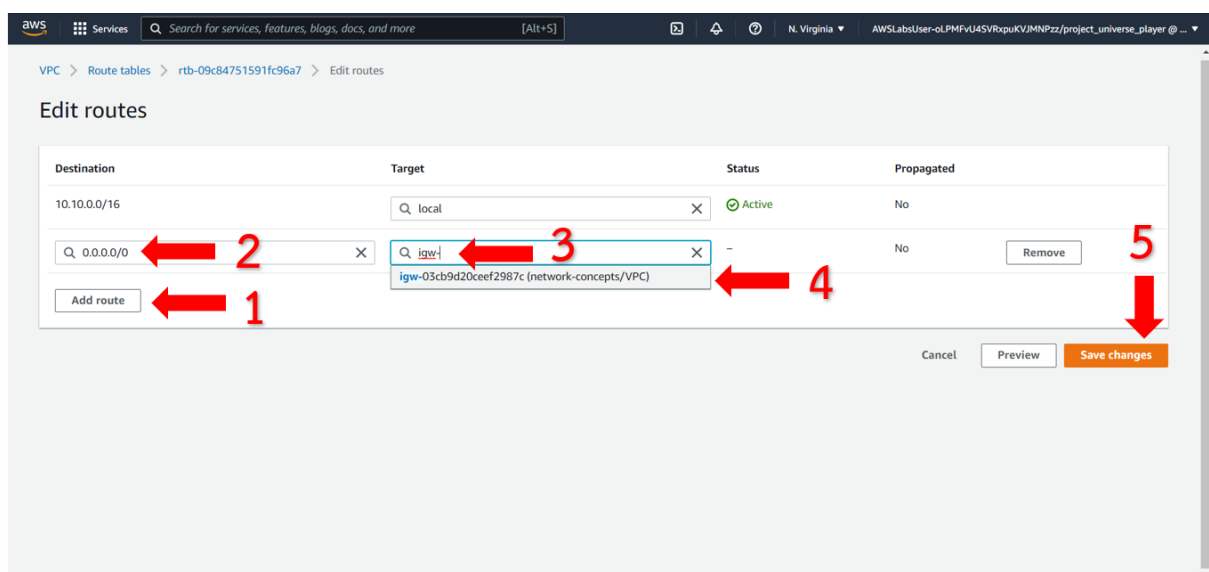
1. เลือกหัวข้อ network-concepts
2. เลือกหัวข้อ Route
3. กดที่ Edit routes



รูปที่ 10 Step 10

STEP 10 : เกตเวย์ NAT คือบริการ Network Address Translation คุณสามารถใช้ NAT เพื่อให้อินสแตนซ์ในซับเน็ตส่วนตัวสามารถเชื่อมต่อกับบริการภายนอก VPC ได้

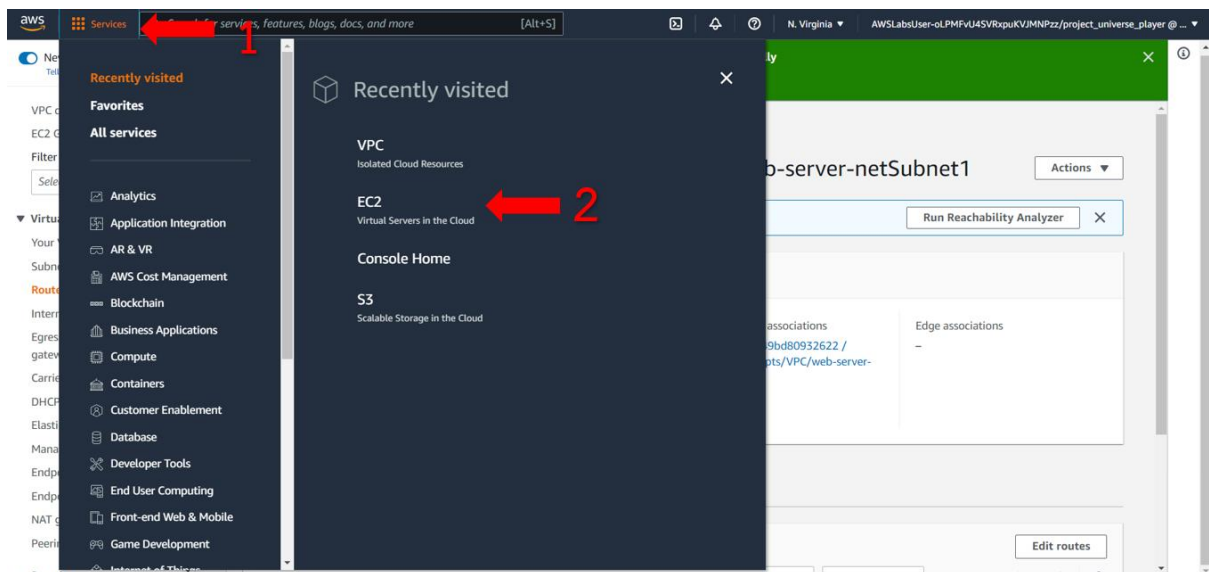
1. กด Remove เพื่อลบ NAT gateway



รูปที่ 11 Step 11

STEP 11 :

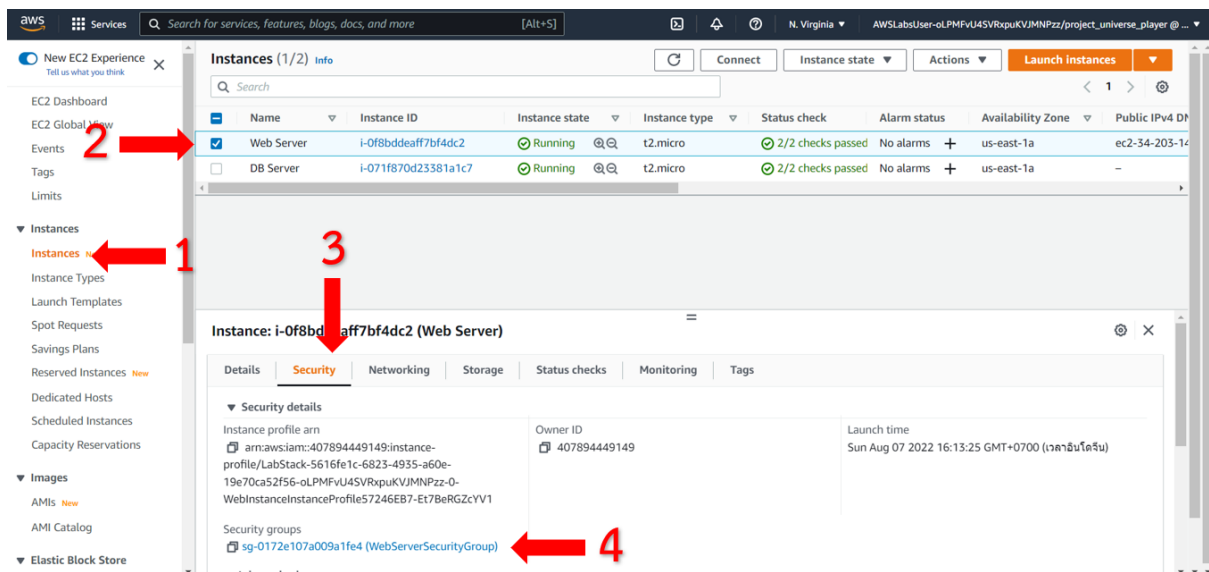
1. กดที่ Add route
2. พิมพ์ 0.0.0.0/0
3. พิมพ์ igw-
4. เลือก network-concept/VPC
5. กด Save changer



รูปที่ 12 Step 12

STEP 12 : อินเทอร์เน็ตเกตเวย์รองรับการรับส่งข้อมูล IPv4 และ IPv6 ไม่ก่อให้เกิดความเสี่ยงด้านความปลอดภัยหรือข้อจำกัดแบนด์วิดท์ในการรับส่งข้อมูลเครือข่ายของคุณ

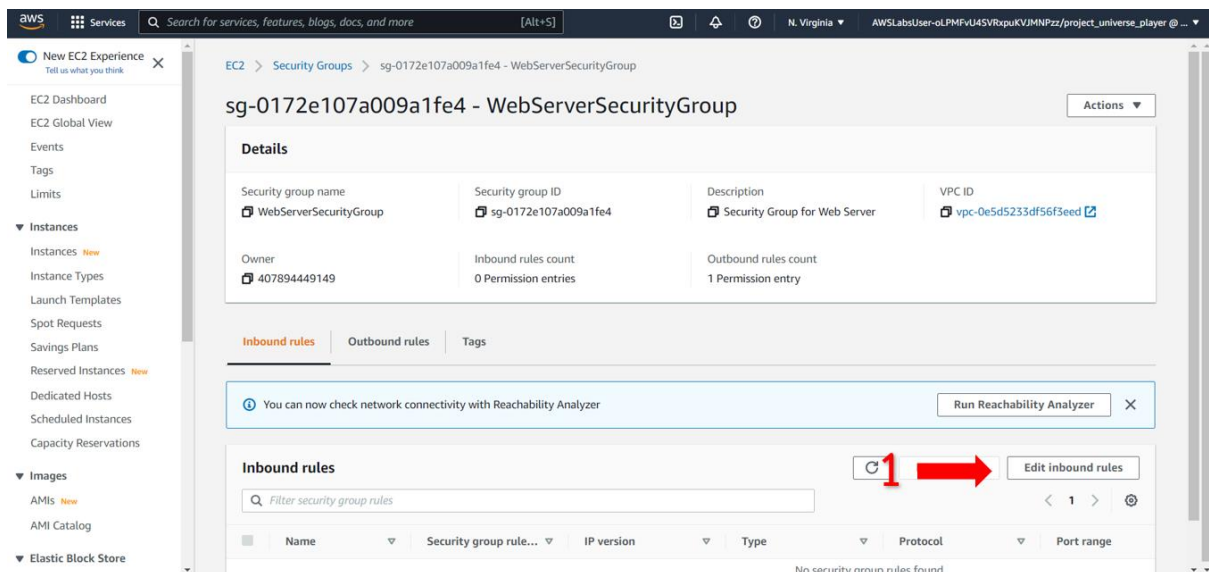
1. กดที่ Services
2. เลือก EC2



รูปที่ 13 Step 13

STEP 13 :

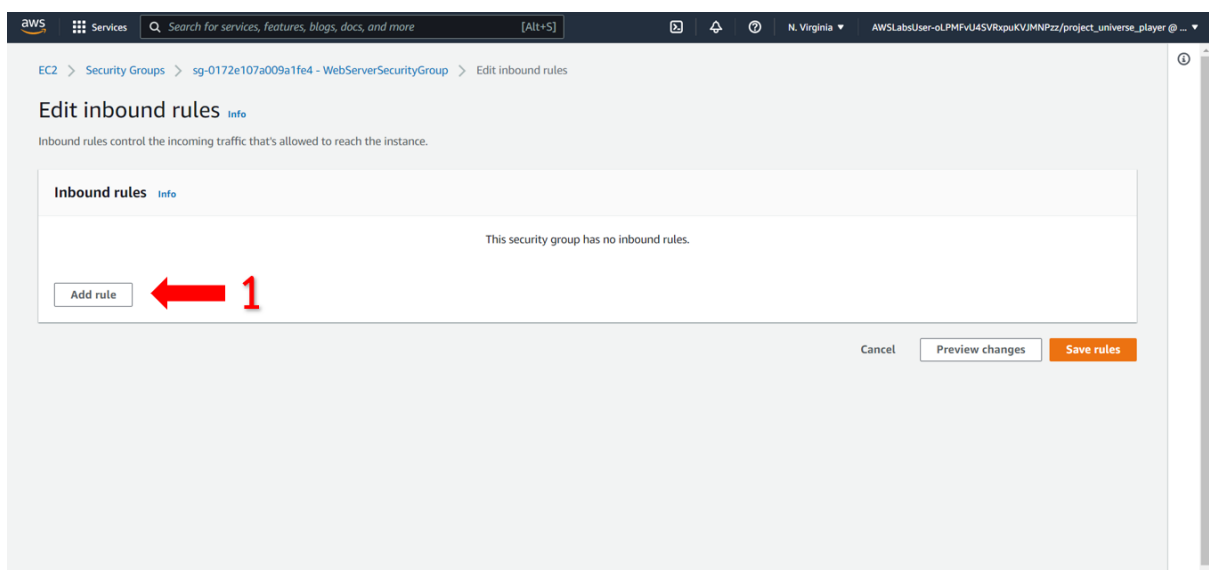
1. เลือก Instances
2. เลือกหัวข้อ Web Server
3. เลือกหัวข้อ Security
4. กดที่ Security groups ลิงก์



รูปที่ 14 Step 14

STEP 14 : สำหรับแต่ละกลุ่มความปลอดภัย คุณเพิ่มกฎที่ควบคุมการรับส่งข้อมูลตามโปรโตคอลและหมายเลขพอร์ต มีชุดกฎแยกสำหรับการรับส่งข้อมูลขาเข้าและขาออก

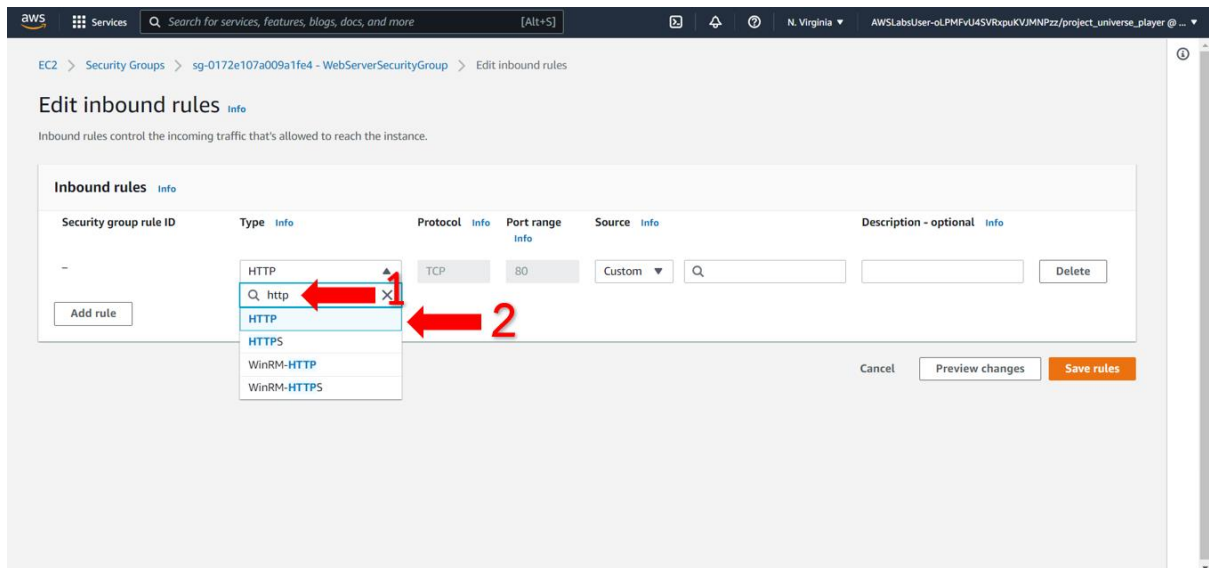
1. กดที่ Edit inbound rules



รูปที่ 15 Step 15

STEP 15 : เมื่อสร้าง VPC มันจะมาพร้อมกับกลุ่มความปลอดภัยเริ่มต้น คุณสามารถสร้างกลุ่มความปลอดภัยเพิ่มเติมสำหรับ VPC แต่ละรายการ

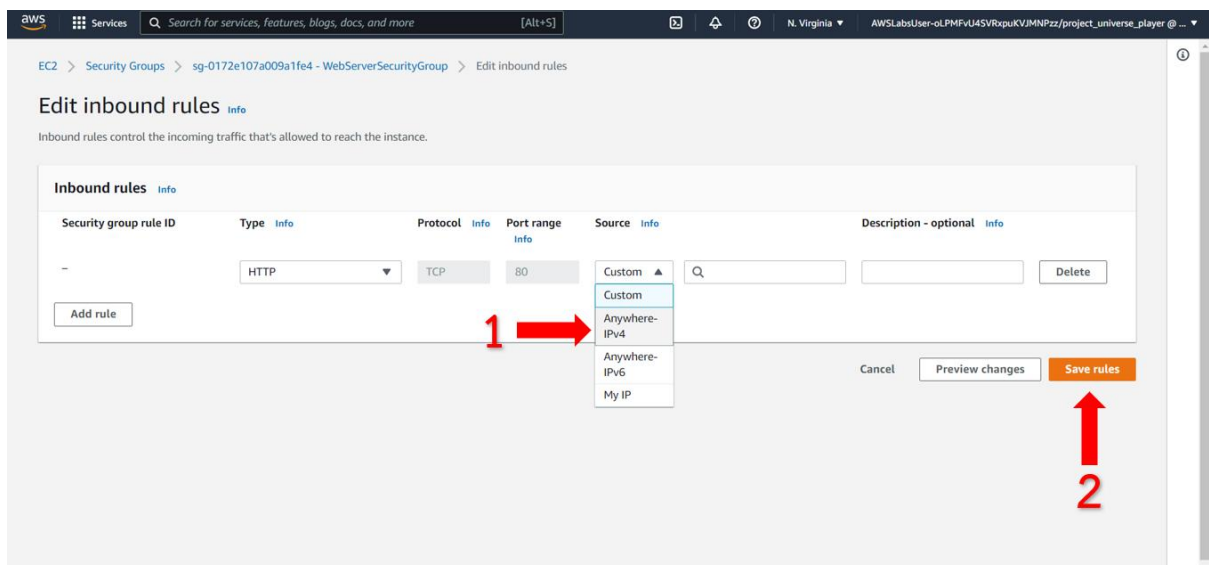
1. กดที่ Add rule



รูปที่ 16 Step 16

STEP 16 :

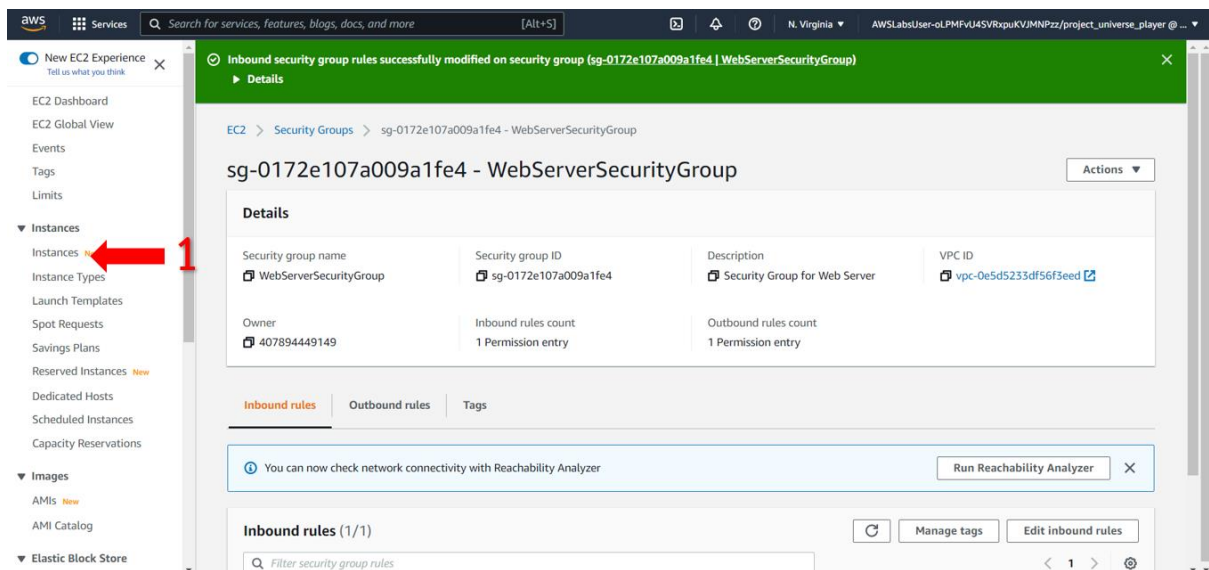
1. พิมพ์ HTTP
2. เลือก HTTP



รูปที่ 17 Step 17

STEP 17 : กลุ่มความปลอดภัยเป็นแบบเก็บสถานะ

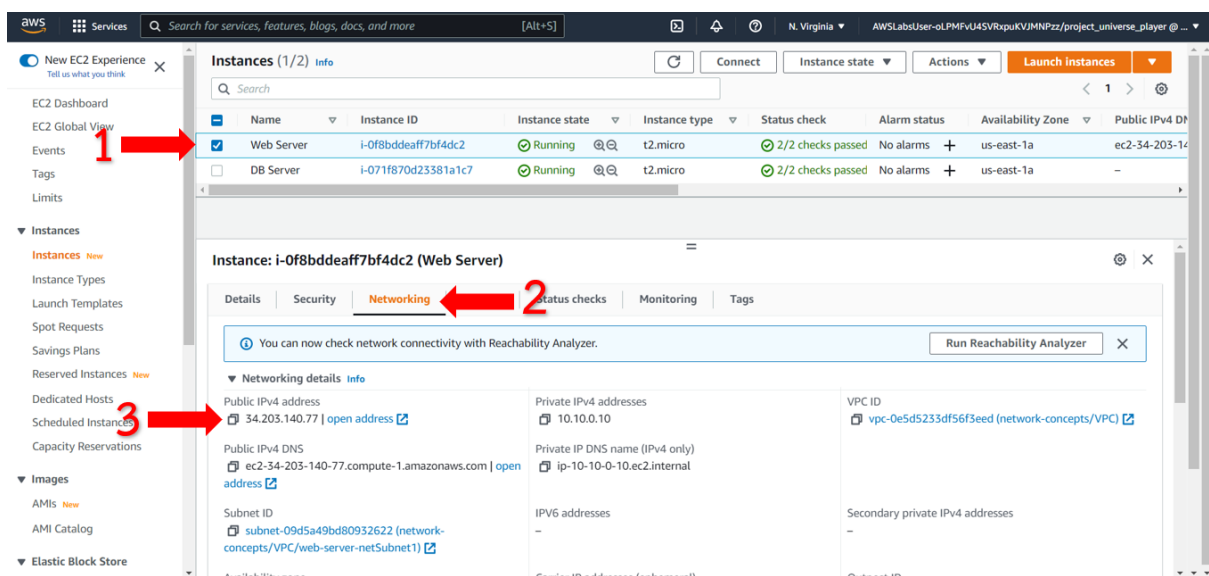
1. เลือก Anywhere-IPv4
2. กด save rules



รูปที่ 18 Step 18

STEP 18 :

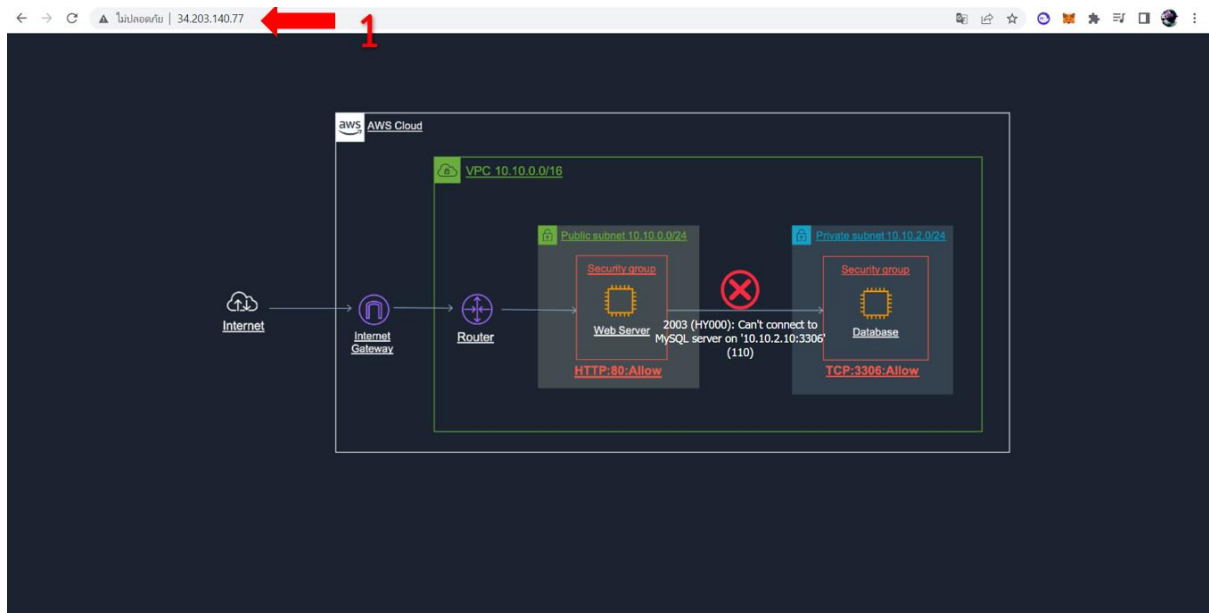
1. กดที่ Instances



รูปที่ 19 Step 19

STEP 19 :

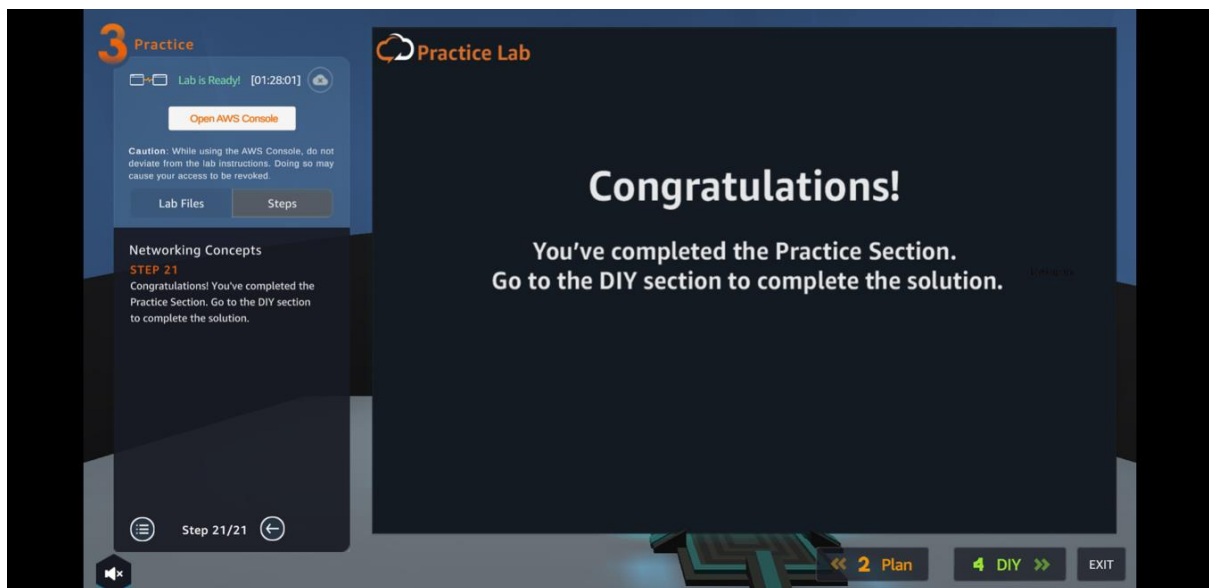
1. เลือกหัวข้อ Web Server
2. เลือกหัวข้อ Networking
3. คัดลอก Public IPv4 address



รูปที่ 20 Step 20

STEP 20 :

1. วาง Public IPv4 address ในช่องค้นหาหน้าต่าง Browser ใหม่ แล้วกด Enter

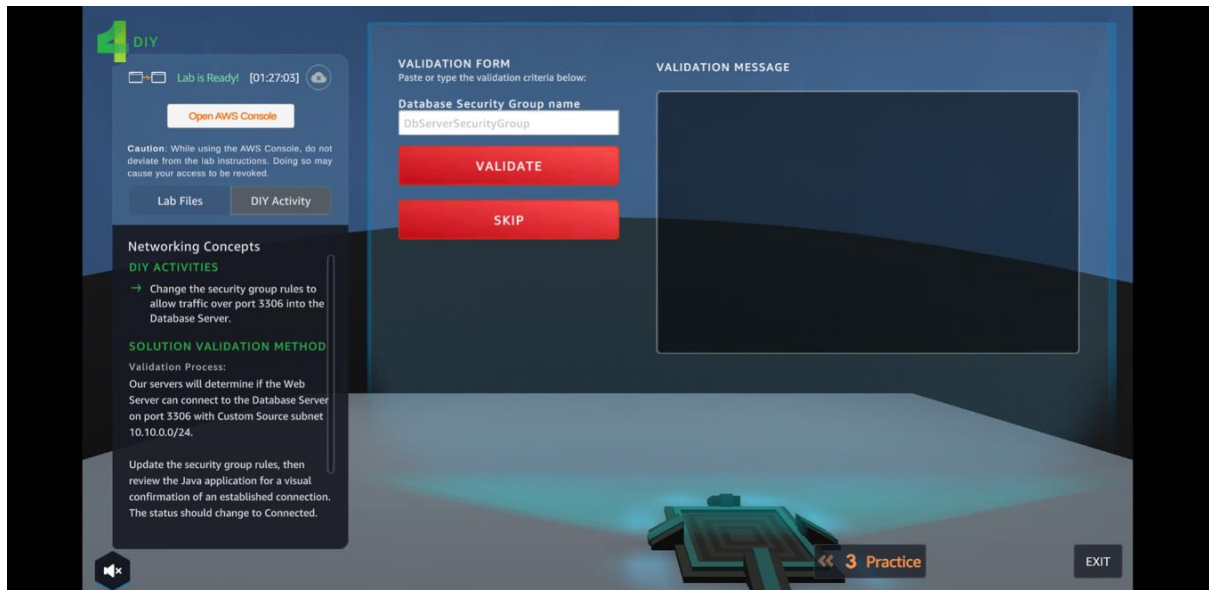


รูปที่ 21 Step 21

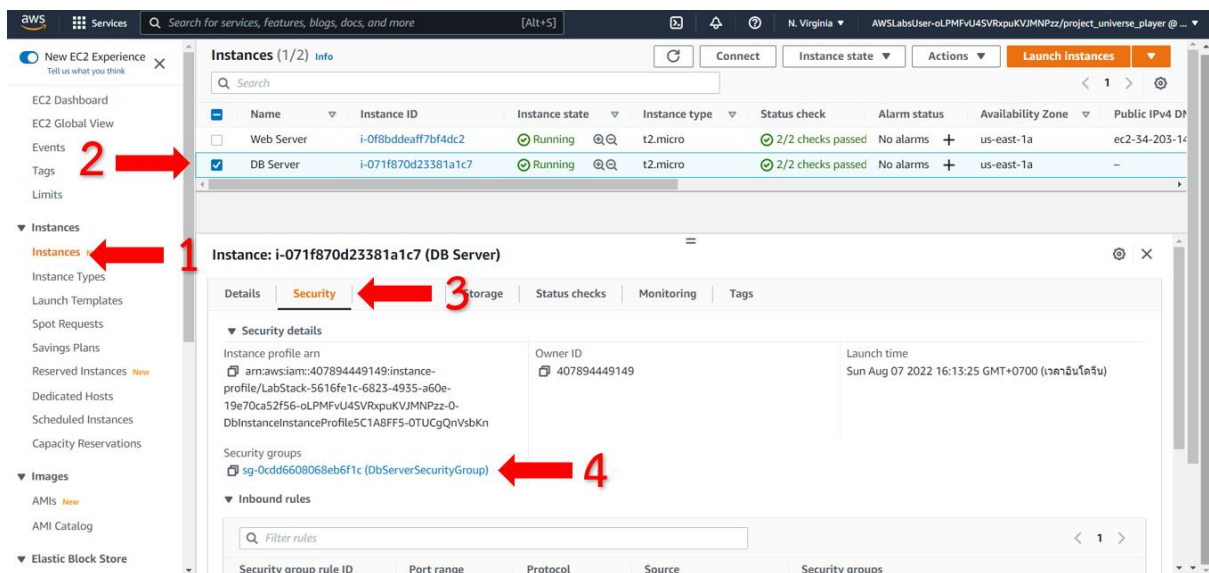
STEP 21 :

1. สำเร็จ ยินดีด้วย

DIY



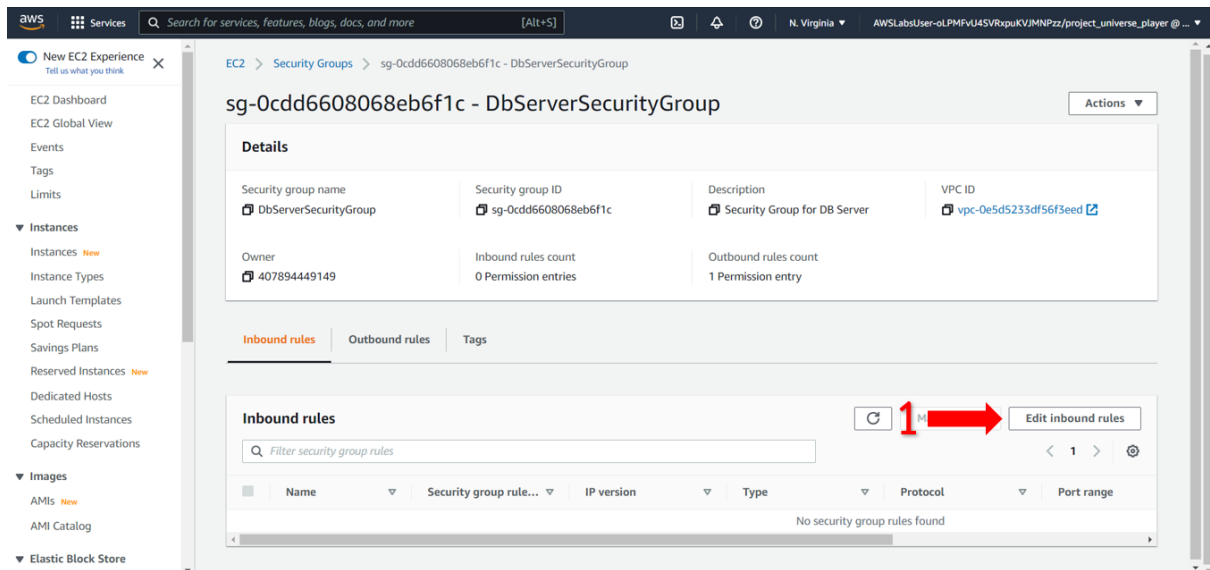
รูปที่ 22 DIY



รูปที่ 23 DIY Step 1

STEP 1 :

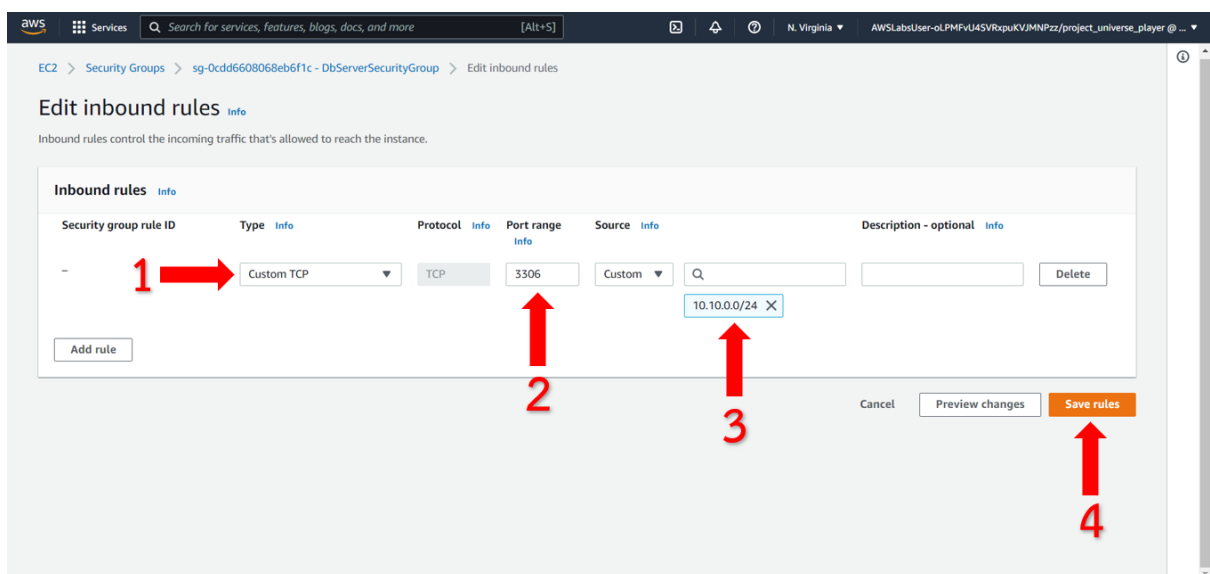
1. กดที่ Instances
2. เลือกหัวข้อ DB Server
3. เลือก Security
4. กดที่ Security groups ลิงก์



รูปที่ 24 DIY Step 2

STEP 2 :

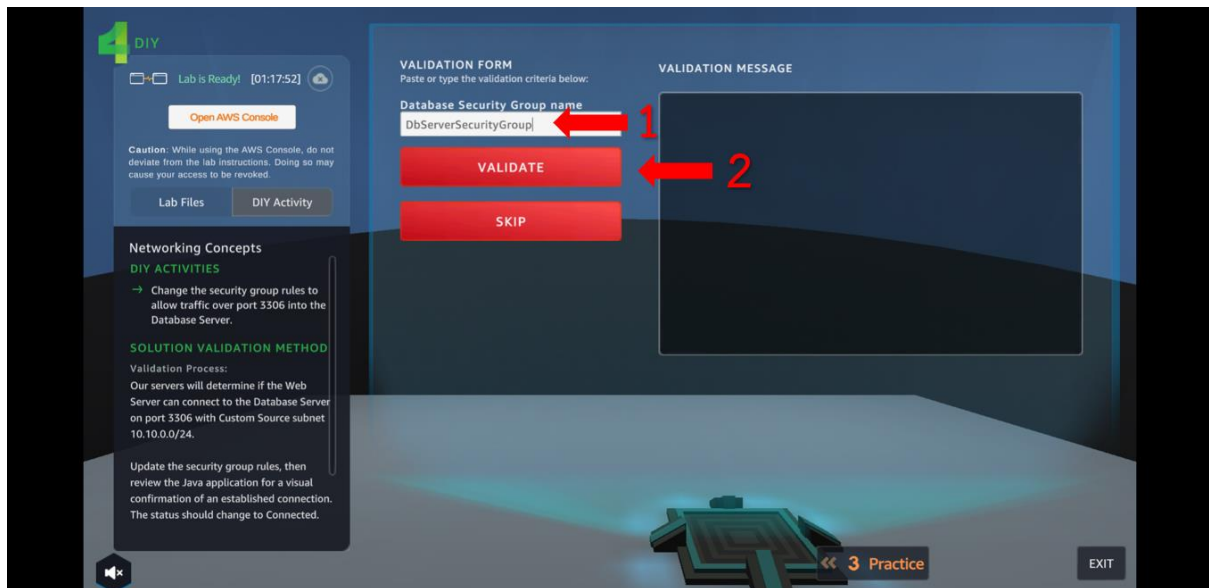
1. กดที่ Edit inbound rules



รูปที่ 25 DIY Step 3

STEP 3 :

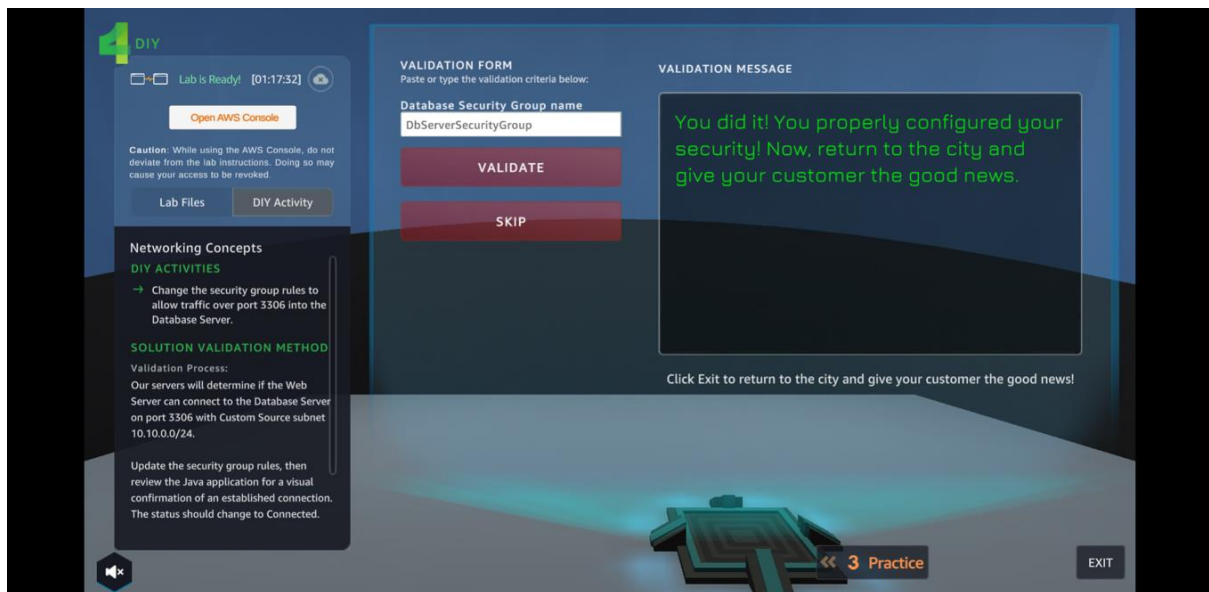
1. เลือก Custom TCP
2. พิมพ์ 3306
3. พิมพ์ 10.10.0.0/24
4. กดที่ Save rules



รูปที่ 26 DIY Step 4

STEP 4 :

1. พิมพ์ DbServerSecurityGroup
2. กด VALIDATE



รูปที่ 27 DIY Step 5

STEP 5 :

1. สำเร็จ ยินดีด้วย