

## Expectation for Exercise 2:

- Create new VPC:

The screenshot shows the AWS VPC console for a VPC named 'vpc-0549cd2a8ac68c457 / EPIC-HW4'. The 'Details' tab is active, displaying the following information:

Property	Value
VPC ID	vpc-0549cd2a8ac68c457
State	Available
DNS hostnames	Disabled
DNS resolution	Enabled
Tenancy	Default
DHCP option set	dopt-0b1da60a0397d4aa7
Main route table	rtb-09b3a969cbc930cf1
Main network ACL	acl-0422d9f42f1ae347b
Default VPC	No
IPv4 CIDR	10.0.0.0/16
IPv6 pool	-
IPv6 CIDR (Network border group)	-
Network Address Usage metrics	Disabled
Route 53 Resolver DNS Firewall rule groups	-
Owner ID	339712893849

## Expectation for Exercise 3:

- Create 2 subnets:

The screenshot shows the AWS Subnets console for the VPC 'vpc-0549cd2a8ac68c457'. Two subnets are listed:

Name	Subnet ID	State	VPC	IPv4 CIDR
public-01	subnet-01080ac2c2aa44fe2	Available	vpc-0549cd2a8ac68c457   EPIC...	10.0.1.0/24
public-02	subnet-01f039b2223b8a02c	Available	vpc-0549cd2a8ac68c457   EPIC...	10.0.2.0/24

- create route table and attach your subnets to it:

The screenshot shows the AWS Route Tables console for a route table named 'rtb-06ce31f5e2edd2962 / route-table-01'. The 'Subnet associations' tab is active, showing the following explicit subnet associations:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
public-01	subnet-01080ac2c2aa44fe2	10.0.1.0/24	-
public-02	subnet-01f039b2223b8a02c	10.0.2.0/24	-

# Expectation for Exercise 4:

- Create EC2 instance :

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	Epic-HW4	i-021e9533545891d63	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1a

[EC2](#) > [Instances](#) > i-021e9533545891d63

## Instance summary for i-021e9533545891d63 (Epic-HW4) [Info](#)

Updated less than a minute ago



Connect

Instance state

Actions

Instance ID

i-021e9533545891d63 (Epic-HW4)

IPv6 address

–

Hostname type

IP name: ip-10-0-1-162.ec2.internal

Answer private resource DNS name

–

Auto-assigned IP address

3.85.11.86 [Public IP]

IAM Role

epic-hws [↗](#)

Public IPv4 address

3.85.11.86 | [open address](#) [↗](#)

Instance state

Running

Private IP DNS name (IPv4 only)

ip-10-0-1-162.ec2.internal

Instance type

t2.micro

VPC ID

vpc-0549cd2a8ac68c457 (EPIC-HW4) [↗](#)

Subnet ID

subnet-01080ac2c2aa44fe2 (public-01) [↗](#)

Private IPv4 addresses

10.0.1.162

Public IPv4 DNS

–

Elastic IP addresses

–

AWS Compute Optimizer finding

[Opt-in to AWS Compute Optimizer for recommendations.](#)

[| Learn more](#) [↗](#)

Auto Scaling Group name

–

## Expectation for Exercise 5:

- Install nginx & Change the conf to be available on 80 and 443:

```
server {
    listen 80;
    server_name 3.85.11.86
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;

    location / {
        try_files $uri $uri/ =404;
    }
}

server {
    listen 443 ssl;
    server_name 3.85.11.86
    root /var/www/html;
    index index.nginx-debian.html;

    ssl_certificate /etc/ssl/certs/epic-hws.crt;
    ssl_certificate_key /etc/ssl/private/epic-hws.key;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;

    location / {
        try_files $uri $uri/ =404;
    }
}
```

```
ubuntu@ip-10-0-1-162:~$ curl http://3.85.11.86:80
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
ubuntu@ip-10-0-1-162:~$ curl --insecure https://3.85.11.86:443
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
```

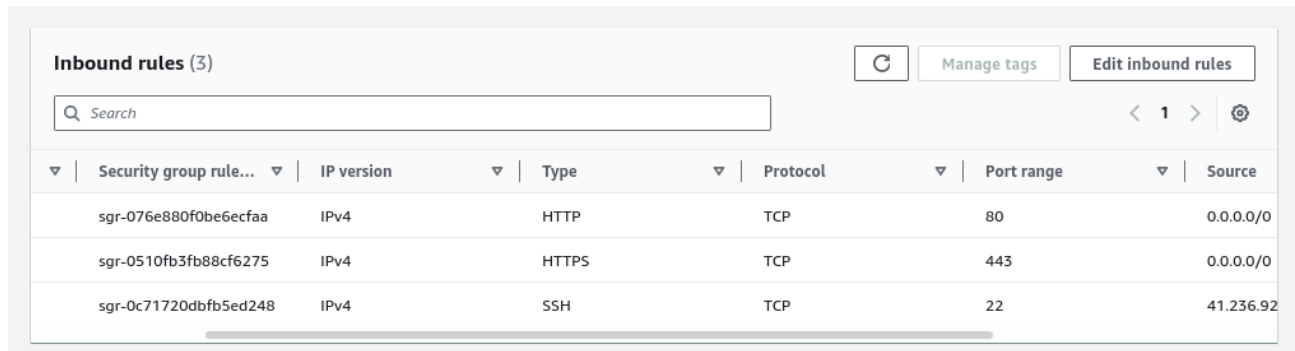
```
ubuntu@ip-10-0-1-162:~$ curl -I http://3.85.11.86:80
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Wed, 15 May 2024 13:29:04 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Tue, 11 Apr 2023 01:45:34 GMT
Connection: keep-alive
ETag: "6434bbbe-267"
Accept-Ranges: bytes

ubuntu@ip-10-0-1-162:~$ curl -I --insecure https://3.85.11.86:443
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Wed, 15 May 2024 13:29:27 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Tue, 11 Apr 2023 01:45:34 GMT
Connection: keep-alive
ETag: "6434bbbe-267"
Accept-Ranges: bytes

ubuntu@ip-10-0-1-162:~$
```

## Expectation for Exercise 6:

- Update your security group and open access on ports 80 and 443:

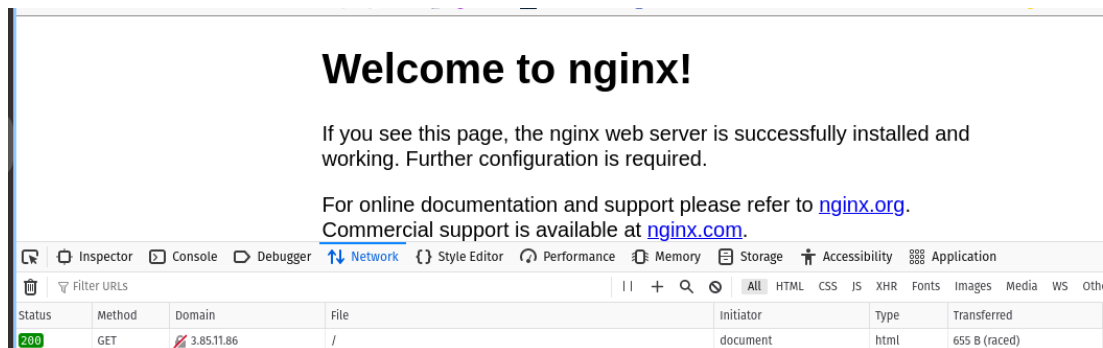


The screenshot shows the 'Inbound rules (3)' section of the AWS IAM console. It features a search bar, a refresh button, and buttons for 'Manage tags' and 'Edit inbound rules'. Below these is a table with three rules. The table has columns for Security group rule ID, IP version, Type, Protocol, Port range, and Source. The rules are: 1) sgr-076e880f0be6ecfaa, IPv4, HTTP, TCP, Port 80, Source 0.0.0.0/0; 2) sgr-0510fb3fb88cf6275, IPv4, HTTPS, TCP, Port 443, Source 0.0.0.0/0; 3) sgr-0c71720dbfb5ed248, IPv4, SSH, TCP, Port 22, Source 41.236.92.

Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-076e880f0be6ecfaa	IPv4	HTTP	TCP	80	0.0.0.0/0
sgr-0510fb3fb88cf6275	IPv4	HTTPS	TCP	443	0.0.0.0/0
sgr-0c71720dbfb5ed248	IPv4	SSH	TCP	22	41.236.92

## Expectation for Exercise 7:

- Try to access EC2 instance public IP:



## Expectation for Exercise 8:

- Create new Role for EC2 :

[IAM](#) > [Roles](#) > epic-hws

### epic-hws Info

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf. Delete

#### Summary Edit

Creation date May 13, 2024, 16:04 (UTC+03:00)	ARN arn:aws:iam::339712893849:role/epic-hws	Instance profile ARN arn:aws:iam::339712893849:instance-profile/epic-hws
Last activity -	Maximum session duration 1 hour	

[EC2](#) > [Instances](#) > [i-021e9533545891d63](#) > Connect to instance

### Connect to instance Info

Connect to your instance i-021e9533545891d63 (Epic-HW4) using any of these options

EC2 Instance Connect | **Session Manager** | SSH client | EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel Connect

Session ID: root-qf2tvjtcdznbkzmg5aoylkjv4

Instance ID: i-021e9533545891d63

Terminate

```
$ bash
ssm-user@ip-10-0-1-162:/var/snap/amazon-ssm-agent/7983$
```

## Expectation for Exercise 9:

- Run one of the scripts you've created in homework 2: [The script's link](#)

```
ssm-user@ip-10-0-1-162:/var/snap/amazon-ssm-agent/7983$ sudo ./myscript.sh
Select an operation:
1) Launch htop on instance
2) Launch tcpdump utility on instance
3) Show EC2 instance metadata
Enter choice: █
```

→ option 1:

```
CPU[|||||] 0.4% Tasks: 32, 52 thr, 77 kthr; 1 running
Mem[|||||] 162M/957M Load average: 0.00 0.02 0.00
Swp[ ] 0K/0K Uptime: 04:50:02

Main I/O
PID USER PRI NI VIRT RES SHR S CPU%MEM+ TIME+ Command
1 root 20 0 22176 13236 9524 S 0.0 1.4 0:04.34 /sbin/init
138 root 20 0 50416 16424 15272 S 0.0 1.7 0:00.47 /usr/lib/systemd/systemd-journald
181 root RT 0 282M 27136 8704 S 0.0 2.8 0:00.19 /sbin/multipathd -d -s
185 root 20 0 26468 8132 5060 S 0.0 0.8 0:00.21 /usr/lib/systemd/systemd-udev
189 root 20 0 282M 27136 8704 S 0.0 2.8 0:00.00 /sbin/multipathd -d -s
```

→ option 2:

```
ssm-user@ip-10-0-1-162:/var/snap/amazon-ssm-agent/7983$ sudo ./myscript.sh
Select an operation:
1) Launch htop on instance
2) Launch tcpdump utility on instance
3) Show EC2 instance metadata
Enter choice: 2
Launching tcpdump...
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enX0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:00:16.930662 IP ip-10-0-1-162.42552 > 67.220.240.135.https: Flags [P.], seq 695958514:695958817, ack 926278664, win 3193, length 303
18:00:16.932271 IP 67.220.240.135.https > ip-10-0-1-162.42552: Flags [.], ack 303, win 20508, length 0
18:00:17.033415 IP ip-10-0-1-162.47308 > 10.0.0.2.domain: 8117+ [1au] PTR? 135.240.220.67.in-addr.arpa. (56)
18:00:17.035515 IP 10.0.0.2.domain > ip-10-0-1-162.47308: 8117 NXDomain 0/1/1 (127)
18:00:17.035977 IP ip-10-0-1-162.38650 > 10.0.0.2.domain: 42788+ [1au] PTR? 162.1.0.10.in-addr.arpa. (52)
```

→ option 3:

```
ssm-user@ip-10-0-1-162:/var/snap/amazon-ssm-agent/7983$ sudo ./myscript.sh
Select an operation:
1) Launch htop on instance
2) Launch tcpdump utility on instance
3) Show EC2 instance metadata
Enter choice: 3
Retrieving instance metadata..
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 56 100 56 0 0 23064 0 --:--:-- --:--:-- --:--:-- 28000
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 325 100 325 0 0 31865 0 --:--:-- --:--:-- --:--:-- 32500
ami-id
```

Student Name: Lama Salah