

EE4221 Lab 3 - Build your VPC and Launch a Web Server

Checkpoints and Lab Assignments

This worksheet supplements the lab activities and provides additional checkpoints to verify your learning outcomes. Extended tasks are provided to guide students to explore more in-depth knowledge. Follow the instructions below to complete each checkpoint and explain your results in the lab report.

Part A – ACF Lab 2: Task 1 to 4

Checkpoint 1:

(Task 1) Show the **Route Table ID** of the two route tables in your VPC. Explain which one is for the *Public Subnet 1* and *Private Subnet 1* respectively.

Checkpoint 2:

(Task 2) Show the **Subnet IDs** that are associated with the *Private Route Table* and *Public Route Table* respectively. Explain the difference of these two route tables.

Checkpoint 3:

(Task 3 to 4) Show the web page displaying the AWS logo and instance meta-data. Explain the number of available IP addresses in the four subnets (250 and 251 respectively).

☐	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4 Addresses
☐	Public subnet 1	subnet-09785...	available	vpc-06f2192c4...	10.0.0.0/24	250
☐	Private subnet 1	subnet-0ac5e...	available	vpc-06f2192c4...	10.0.1.0/24	251
☐	Public subnet 2	subnet-02085...	available	vpc-06f2192c4...	10.0.2.0/24	250
☐	Private subnet 2	subnet-0218a...	available	vpc-06f2192c4...	10.0.3.0/24	251

Part B – Extended Tasks

Checkpoint 4:

The private subnets can be seen as an intranet where access is restricted from the VPC. Now launch another web server with the same setting as **Web Server 1** but deploy it to the **Private Subnet 2**. Tag this server with the name **Private Web Server**.

Demonstrate and explain how you verify the following configurations:

- The *Private Web Server* has access to internet.
- The web page on *Private Web Server* cannot be viewed from internet.
- The web page on *Private Web Server* can be viewed from *Web Server 1*.

(Hints: modify the **Web Security Group** to permit inbound SSH traffic)

Checkpoint 5:

If **Web Server 1** is compromised, it can be a security threat to the applications running in private subnets. Create a Network ACL that blocks all traffic from **Public Subnet 2** but allows the SSH traffic from **Web Server 1** and then associate it to the two private subnets. The web page on *Private Web Server* will be unviewable from *Web Server 1*. Explain your Network ACL settings and how you verify the results.