Declaration	
Questions in this exercise are intentionally complex and could be convoluted or confusing. This is by design and to simulate real life situations where customers seldom give crystal clear requirements and ask unambiguous questions.	

I have read the above statement and agree to these conditions	
I AGREE	Pratibha Dixit
	<Enter your name above this line to indicate that you are in agreement>

Step 5: Answer the following questions

Answer the following questions

Q1 What is the default setting for DNS hostnames when a new VPC is created?

a) Enabled

b) Disabled

c) Can be set during VPC creation

d) Depends on the region used

Enter your answer here — b) Disabled

Q2 What is the term used for the machine when we use it to log into the database server?

a) Bastion Host

b) NAT Gateway

c) Tunnel Interface

d) SSH Gateway

Enter your answer here — a) Bastion Host

Q3 The database server security group in this exercise has to keep port 3306 open. Which protocol uses this port to communicate?

a) HTTPS

b) RDP

c) TCP

d) SCP

Enter your answer here | c) TCP

Q4 Which port is being used by Mattermost to communicate with the client application

a) 8080

b) 80

c) 443

d) 8065

Enter your answer here | d) 8065

Q5 Which of the following is a reason why we cannot set the CIDR block for the public subnet to 10.0.2.0/16, assuming the values for the other CIDR blocks are the same as mentioned in the instructions?

a) CIDR block overlaps with existing block

b) CIDR block is not a valid CIDR

c) CIDR block does not fall within the VPC

d) There is no reason, this is a perfectly valid CIDR

Enter your answer here | c) CIDR block does not fall within the VPC

Q6 Assume that you have been asked to create 3 EC2 instances - application server, the database server and NAT instance. Each of these instances have their own security groups with a set of ports to be kept open. One of those ports is entirely unnecessary for the given architecture to function. Which of the ports given in the option below could it be?

a) Port 22 on the NAT instances

b) Port 3306 on the database server

c) Port 443 on the NAT instance

d) Port 22 on the application server

Enter your answer here |

Enter your answer here

a) Port 22 on the NAT instances

Q7 Describe the steps you would take to increase security of the servers you have deployed so that they are not reachable from external sources

Security is an important thing when deploying servers on AWS infrastructure. Here are some of the important things to protect our servers in the cloud.

1) Use VPCs - Our servers already connected to the Project 1 VPC and this provide a more secure connection among resources because the network's interfaces are inaccessible from the public internet. Using a VPC we can create private clouds within the public cloud and it isolates from other customers in the private cloud.

2) Establish and Use a Secure Connection - When connecting to a remote server, it is essential to establish a secure connection for communication. We used the SSH Protocol to establish a protected connection. SSH access encrypts all data transmitted in the cloud.

3) Always use SSH Keys - SSH keys use encryption to provide a secure way of logging into our server. We used the popular RSA 2048-bit encryption, which is equivalent to a 617- digit password.

4) Use Security groups and Network ACLs - Security Groups act as a virtual firewall, allowing us to control inbound and outbound traffic. We use security groups to limit access to administrative services (SSH, RDP, etc.) as well as databases. NACLs work in conjunction with security groups, and can allow or deny traffic even before it reaches the security group

5) Use Firewalls - A properly configured firewall will ensure that only services that should be publicly available can be reached from outside our servers or network. Use Web application firewalls (WAF) and Next-Gen firewalls to prevent denial of service attacks. Using host-based firewalls to control access to each instance.

6) Create NAT instance to restrict access to a data base server (private network) from an external network. Bastion Host and NAT instance both help secure our servers by limiting access to our instances over cloud. In order to access the database server we used SSH from application server. if we want to go out to the internet from the database server, we can use the NAT instance to give access to

the internet without allowing inbound access to it.

7) Assign the SSH port to known IP address (custom / corporate) When creating the NAT instance, application server and database server, we have set the port 22 open to "Anywhere", create rules that allow public access to our servers. This is not a good practice in general. It would be recommended to assign the SSH to known IP addresses (custom /corporate) to prevent hackers from reaching our servers.

8) We opened port 3306 for the database security, which don't allow access to the internet.

9) Close any unnecessary system ports. In order to get maximum security, it is recommended to close any unwanted open ports.

10) Assign IAM Roles to EC2 Instances and IAM policies to control access.

Q8 Describe the steps required to deploy the given application in an autoscaling environment

For an Auto Scaling Environment to function effectively, it is better to add Elastic Load Balancers to automatically distribute incoming application traffic across all EC2 instances within our Auto Scaling groups. So I am adding Load balancer first.

Step 1 - Create and configure Application Load Balancer (ALB)
a) In the wizard, also create Target group but do not add any instances now.
b) Create a Launch Template – Enable Auto Scaling guidance to select our server instance.

Step 2 - Create an Auto Scaling group Using the Auto Scaling wizard, create an Auto Scaling group specifying a name, size, and network for our Auto Scaling group. Network would be Project 1 VPC

Step 3 - Select subnet in all desired availability zones.

Step 4 - Configure scaling policies for our Auto Scaling group Example - Scale Minimum size 2, Maximum size 4, Desired 2.

Step 5- Associate Target group with Autoscaling group. Confirm email subscription.

Step 6 -Associate ELB health check

Step 7 - Set auto scaling policy on Average CPU> 20%. Configure email notification and email subscription.

Step 8 - Wait for instances to be running.

Now we can access the mattermost (application server) using load balancer DNS.

Grades distribution	
MCQs	6 (1 mark each)
Subjective questions	20 marks (10+10)
Implementation screenshots	24 marks (1 marks each)
Total	50 marks