1)Explain how to create a key pair for accessing your EC2 instance. What is the purpose of

the key pair, and how does it enhance the security of your instance?

→

1. *Login to AWS Management Console* – Go to the EC2 dashboard.

2. *Navigate to Key Pairs* – In the left menu, select *Network & Security → Key Pairs*.

3. *Create a New Key Pair* – Click *Create key pair*, enter a name, choose key type (RSA/ED25519) and file format (.pem for Linux/macOS or .ppk for Windows).

4. *Download the Private Key File* – Save the file securely; it's downloaded only once.

5. *Set Permissions* – For Linux/macOS, run chmod 400 MyKeyPair.pem.

6. *Use It to Connect* – When launching an EC2 instance, select this key pair, then connect using SSH or RDP with the private key.

Purpose:

It authenticates your identity securely without passwords.

Security Benefit:

Only the person with the private key can access the instance, protecting it from unauthorized access.

2)For security reasons, you want to limit SSH access to your EC2 instance to only your office

IP address. How would you modify the inbound rules of your security group to achieve this?

What steps would you follow to ensure that only your office IP address can connect via SSH?

→

1. *Find your office public IP address* – Search "what is my IP" from a system in your office network.

2. *Log in to the AWS Management Console* and open the *EC2 Dashboard*.

3. From the left menu, click *Security Groups* under Network & Security.

4. *Select the security group* attached to your EC2 instance.

5. Click *Edit inbound rules* to modify access permissions.

6. Locate or add a rule for *SSH (Port 22)*.

7. In the *Source* field, enter your office public IP address in CIDR format (e.g., 203.0.113.25/32).

8. *Delete any other SSH rules* allowing open access (like 0.0.0.0/0).

9. Click *Save rules* to apply the changes.

✅ *Result:* Only users connecting from your office IP can access the instance via SSH, enhancing security.