Slip 1

Q1. **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?**

Ans:- 1.create a key pair

2. Lunch the ec2 enstance while lunching the instance connect —> selected the created key pair

3 select your instance —-> connect —-> connect

How It Enhances Security

1. Passwordless Access:

You don't need to type a password to log in.

Only the person who has the private key file can access the EC2 instance.

This reduces the risk of someone guessing or stealing your password.

---

2. Encryption-Based Security:

When you connect to your EC2 instance, all the data (like login details) is **encrypted** — or hidden — using strong mathematical codes.

This means even if a hacker tries to watch your network, they can't read or understand the data being sent.

---

3. Unique and Private:

Every key pair is different for each user.

AWS keeps only the **public key**, while you keep the **private key** safely on your computer.

Since AWS doesn't store your private key, no one else can use it to access your instance.

---

4. Protection from Brute-Force Attacks:

Brute-force attacks happen when hackers try many password combinations to break in.

With key-based login, there's no password to guess — so such attacks won't work.

This makes your EC2 instance much more secure.

Purpose of the Key Pair

The purpose of a key pair is to provide **secure login (authentication)** to an EC2 instance without using a password.

A key pair has two parts:

- **Public Key:** It is stored in AWS and attached to the EC2 instance. It acts like a lock for the server.

- **Private Key (.pem or .ppk):** It is downloaded and kept by the user. It acts like a key to open the lock and is used while connecting to the instance through SSH or PuTTY.

Q2.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?

ANS:- to select your security group —> select our above question instance then scroll down —>click networking —> scroll right side then see name of security group

- To Find security group go on security group list
- Click on security group name —-> edit inbound rule —> source —>change custom to my ip —> save rule

 # Steps to Modify Inbound Rules:

1.Open AWS Management Console

Go to the **EC2 Dashboard** and click on **Security Groups** from the left menu.

2.**Select the Security Group**

Choose the security group that is attached to your EC2 instance.

3.**Edit Inbound Rules**

Click on **Edit inbound rules**.

4.**Set SSH Rule**

In the Type field, select **SSH**.

In the Port range, it will automatically show **22**.

In the Source field, select **My IP** or enter your **office IP address** (for example, `203.0.113.25/32`).

5.**Save the Rule**

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

Slip 2

Q1. Launch a Windows Server Amazon EC2 instance and connect using Windows Remote Desktop.

—> 1. Lunch the ec2 while lunching the instance select windows then lunch instance

2. Then click on the running instance —-> connect —>see option of RDP —-->

Download the remote desktop file —-> click Get password —-> uplod .pem file —> decrypt it —> see password copy that —>go on downloaded file windows.edp —> connect —> yes —-> paste password

Q2. How do you create an IAM policy that grants full access to EC2 instances but only allows starting and stopping instances?

Ans:- Search IAM —> polices —> create policy —> select service ec2 —--> in action allowed go in write and select stop and start instance —> resources click all →click on next → give name ,discription —> click on create policy

Slip 3:

Q1. Create a custom AMI from your configured EC2 instance. What steps would you take to delete an AMI?

Ans:- lunch ec2 instance —> click Action —> click image and templates —> create image

In image tab click on IAM → lunch instance from AMI —> give name —> create new key pair —> create security group → click on create instance —> click on action —> deregistered

Q2. Create a two S3 bucket in AWS and perform the following operation. Upload files to an S3 bucket Download a bucket item. Copy a bucket item to another bucket.

Ans:- create two s3 bucket —->click on first bucket —> add file upload any file —-> go on first bucket click on uploaded file —> in right side you see object action —> click on copy —> give destination of second bucket —> scroll down and click on copy

Slip 4

Q1. How do you create and manage AWS IAM users and groups?

Ans:- 1. Login to AWS Console

Go to https://aws.amazon.com/console → open IAM (Identity and Access Management) service.

2. Create a Group

Click User Groups → Create Group.
Give a name (e.g., DevelopersGroup).
Attach required policies (e.g., AmazonS3ReadOnlyAccess).
Click Create Group.

3. Create a User

Click Users → Add Users.
Enter username (e.g., ManasiUser).

Select Access type:

AWS Management Console access, or

Set password if console access is selected.

4. Add User to Group

In the same wizard, Add user to existing group (e.g., DevelopersGroup).

Click Next → Create User.

5. Verify User Creation

User is listed under IAM → Users tab.

Note Access Key ID and Secret Key (if programmatic access given).

6. Manage Users and Groups

You can later add/remove users, change permissions, or attach new policies anytime.

Result:

Successfully created and managed IAM users and groups in AWS for secure access contr**ol.**

Q2. You want to ensure that your EC2 instance's data is backed up regularly. What methods would you use to back up data from your EC2 instance? Discuss options such as creating snapshots of EBS volumes and using AWS Backup.

ANS:- create volume —> click on create volume green msg →action → create snapshot —> go on AWS backup (sear in search bar) open it —> click on backup plan —> choose template —> 35 or any one —> backup rule —> create plan —> in assign resources in General assign name ec2 —> click on assign resources

Slip 6

Q1. How can you create an IAM policy that allows only read access to S3 buckets?

ANS:- 1. Login to AWS Console

Open https://aws.amazon.com/console and go to IAM service.

2. Go to Policies → Create Policy

3. Choose Service

Select S3 under the list of services.

4. Select Actions

Under Read, check the boxes like:

GetObject

Under list,check the boxes like:

ListBucket

(These actions allow read-only access.)

5. Select Resources

Choose All resources or specify the S3 bucket ARN.

6. Add Conditions (optional)

Example: allow access only from specific IP or require MFA.

7. Review and Create Policy

Give name: S3ReadOnlyPolicy

Click Create Policy.

8. Attach Policy

Go to Users → Permissions → Add Permissions → Attach Policy
and attach this new S3ReadOnlyPolicy.

IAM Policy created successfully that allows only read access to S3 buckets.

Q2 Create multiple key-pair and use same key-pair for multiple instances.

ANS:- create multiple instance and use same key pair for them

Slip 7

Q1 2 How do you configure Network Access to an instance using Security groups?

Ans:- create a security group → inbound ssh → then lunch the ec2 instance —> select existing group select our created security group .

Q2 You have a web server EC2 instance that needs to be secured from unauthorized access while allowing necessary traffic. How would you configure security groups to secure your EC2 instance? Describe the process for creating and applying security group rules to allow only HTTP and SSH traffic while restricting all other access

ANS:-

Lunch ec2 instance with name web server —> select security group→ edit inbound rules —> ssh (my ip) and http (custome ip)

Slip 8

Q1 If you have a custom AMI that you want to use to launch new EC2 instances. What are the steps to launch an EC2 instance using your custom AMI? Include details about choosing the AMI, selecting instance types, and configuring the instance settings

Ans:- lunch ec2 instance —> click Action —> click image and templates —> create image

In image tab click on IAM → lunch instance from AMI —> give name —> create new key pair —> create security group → click on create instance —> click on action —> then open terminal —> cd Download —> ls → find our key name .pem → type cat and key paire name → copy that name —> example command in ssh client of AWS copy and paste on teminal

Q2 How do you configure AWS S3 versioning and lifecycle policies?

Ans:- search amazon s3 —> go in buckets or create buckets

After this select bucket you created —> properties —> in bucket versioning click on edit —> click on enable → save changes —> then go in management —> in lifecycle rules click on lifecycle rule —> give name —> choose a rule scope select apply to all objects in the bucket —> in life cycle rule action select first two option —> scroll

down —> in choose storage class transition select glacier deep same for next option —> create rule

Slip 10

Q1 How do you add tags to an existing EC2 instance?

Ans:

Step-by-step Answer:

1. Login to AWS Management Console
   Go to https://aws.amazon.com/console/ and sign in to your AWS account.
2. Open EC2 Dashboard
   From the AWS console, select EC2 under “Compute” services.
3. Select Instances
   In the left panel, click on Instances → Instances.
4. Choose the Instance
   Select the EC2 instance you want to add tags to.
5. Open Tags Tab
   Scroll down and click the Tags tab in the lower section.
6. Add/Edit Tags
   Click Manage tags or Add/Edit tags.
7. Enter Tag Key and Value

Example:

   Key: Name
   Value: WebServer-Instance

8. Save Changes
   Click Save to apply tags to your instance.

Purpose of Tags:

Helps in resource identification.

Useful for billing, automation, and management.

Q2. How do you configure AWS IAM policies for data access control?

Steps:

1. Login to AWS Console → Go to IAM (Identity and Access Management) service.
2. Create or Select a User/Group/Role → Choose who you want to assign the access control policy to.
3. Create a Policy
   In the IAM sidebar, click Policies → Create Policy.
4. Choose a Service
   Example: Select S3 (for controlling access to S3 buckets).
5. Set Permissions
   Choose Actions (e.g., GetObject, PutObject, ListBucket).
   Specify Resources (e.g., a specific bucket or all buckets).
7. Review and Create
   Give a name (e.g., S3ReadOnlyPolicy) and description, then Create Policy.

8. Attach the Policy
Go to Users → Permissions → Add permissions → Attach policies directly and select the policy.

Slip 11
Q1. How do you add an SSH public key to an existing EC2 instance using the AWS Management Console?
Ans;-

Q2 How does an IAM user goes towards enabling Multi-Factor Authentication (MFA)?
Ans:- 1. Go to IAM service in AWS Console.
2. In the left panel, click Users.
3. Select your IAM user (e.g., mansi).
4. In the user details page, open the Security credentials tab.
5. Find the Multi-Factor Authentication (MFA) section.
6. Click Assign MFA device.
7. Choose MFA device type:
Either Authenticator app (like Google Authenticator)
Or Passkey/Security key (Windows Hello or USB key)
8. Click Next.
9. Follow the on-screen steps:
If Authenticator app → scan the QR code and enter two 6-digit codes.
If Passkey → confirm using your device PIN, fingerprint, or key.
10. When it shows ✅ “MFA device successfully assigned”, you’re done!

Slip 12
Q1 How can you create an IAM policy that allows only read access to S3 buckets?
Ans:- create IAM user —-> go in policies —> create policy → select a services s3 —> action allow select read —> select read choose get object —--> in resources select all → then click on next
Policy details —> give policy name —> create policy
Then search your policy —>click on it —> then go in entities attach → click on attached —> select user then attached policy

Q2 How would you create a security group to ensure your EC2 instance is accessible only through necessary ports (e.g., HTTP and SSH)? What inbound and outbound rules would you configure, and why?

ANS:- create security group → configure inbound rules —> allow ssh and http with my ip —> default outbound rule —> create security group
Use this security group when time of lunch instance

Slip 15
Q1. You want to protect your EC2 instances from common security vulnerabilities and attacks. What steps would you take to secure EC2 instances against common vulnerabilities such as unauthorized access, misconfigurations, and software vulnerabilities? Discuss strategies such as patch management, configuration hardening, and access control.
Ans:- search ec2 —> lunch ec2 —>create new security group select —> lunch instance
Then view all instance → click our instance —->scroll down—> networking —> scroll right side —> see security group click on the security group —->inboun rule
Add rule —> ssh —> my ip
Add rule —> http —> my ip
Add rule —-> https —>my ip —> save rule
Go no key pair —>

Q2. How can you automate the process of adding or removing SSH public keys to EC2 instances using AWS Systems Manager?

Slip 17
Q1 How do you restrict HTTP traffic to only a specific IP address or range in a Security Group?
ANS:- create a security group —> click inbound rule —> edit inbound rule
2 Add http rule —> my ip
3.save the rule

Steps:- open AWS Management Console
Go to the **EC2 Dashboard** and select **Security Groups**.
Select the Security Group
Choose the security group attached to your EC2 instance.
Edit Inbound Rules
Click on **Edit inbound rules**.
Add HTTP Rule
Set **Type** to **HTTP**.
The **Port range** will be automatically set to **80**.
In the **Source** field, enter the **specific IP address** (e.g., `203.0.113.25/32`) or an **IP range** (e.g., `203.0.113.0/24`).
Save Rules
Click **Save rules** to apply the changes.

Q2. How do you attach a policy to an IAM user using the AWS Management Console?

Ans:- search IAM —>create user → attach policy directly —> scroll down in permission policy —-> search amazons3readonlyacces —> select —> next—-> create user

Slip 18

Q1. How do you add an outbound rule to a Network ACL to block all traffic to the internet?

Ans: To block all outbound traffic to the Internet using a Network ACL (NACL) in AWS, follow these steps:

Step-by-Step Procedure:

1. Open AWS Management Console → Go to VPC service.
2. From the sidebar, select Network ACLs.
3. Choose the Network ACL associated with your subnet.
4. Click on the Outbound Rules tab.
5. Click Edit outbound rules → Add new rule.
6. Enter details as follows:

Field	Value
Rule Number	100
Type	All Traffic
Protocol	All
Port Range	All
Destination	0.0.0.0/0
Action	Deny

7. Click Save changes.

Result:

All outbound traffic from instances in the subnet is blocked.

No data can leave the subnet to the internet.

Explanation:

Network ACLs are stateless firewalls at the subnet level.

By setting the outbound rule to Deny all traffic (0.0.0.0/0), you effectively stop all communication from your VPC subnet to the Internet.

Q2. How do you create an IAM policy that denies all access to a specific S3 bucket?

To deny all access to a specific Amazon S3 bucket, you can create a custom IAM policy.

Steps:

1. Open AWS Management Console → IAM service.
2. Go to Policies → Create policy.
3. Select the JSON tab and paste the following code:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::my-example-bucket",
        "arn:aws:s3:::my-example-bucket/*"
      ]
    }
  ]
}
```

> Replace my-example-bucket with the actual bucket name.

4. Click Next → Review.
5. Enter:

Policy name: DenyAllAccessToBucket
Description: Denies all S3 actions on a specific bucket.

6. Click Create policy.
7. Attach the policy to any IAM user, group, or role you want to restrict

.

Slip 19

Q1. How do you implement a Network ACL that allows only HTTPS traffic on port 443 and denies all other traffic?

Ans:-

Let's break it into easy VPC steps you can actually do in AWS.

STEP 1 — Create a VPC

1. Open AWS Management Console → VPC service
2. Click Create VPC
3. Choose VPC only (not with subnets)
4. Enter:

Name tag: MyVPC
IPv4 CIDR block: 10.0.0.0/16
Leave rest as default

5. Click Create VPC

You now have a private network to apply the ACL on.

STEP 2 — Create a Subnet

1. Inside your VPC, click Subnets → Create subnet
2. Choose VPC: MyVPC
3. Add:

Subnet name: MySubnet
Availability Zone: Choose any (like ap-south-1a)
IPv4 CIDR block: 10.0.1.0/24

4. Click Create subnet

This subnet will use your Network ACL.

STEP 3 — Create an Internet Gateway (for Internet access)
1. Go to Internet Gateways → Create internet gateway
Name: MyInternetGateway
2. Click Create internet gateway
3. Then Attach to VPC → Select MyVPC
This connects your VPC to the Internet.
STEP 4 — Create a Route Table
1. Go to Route Tables → Create route table
Name: MyRouteTable
VPC: MyVPC
2. Click Create route table
3. Select it → Routes → Edit routes → Add route
Destination: 0.0.0.0/0
Target: MyInternetGateway
4. Click Save changes
5. Then go to Subnet associations → Edit subnet associations → Select MySubne
Your subnet now has internet access.
STEP 5 — Create and Configure Network ACL
1. Go to Network ACLs → Create network ACL
Name: MyNACL
VPC: MyVPC
2. Click Create network ACL
3. Go to Inbound Rules → Edit inbound rules → Add rules
    Rule #100 → Allow HTTPS (port 443)
    Type: HTTPS
    Protocol: TCP
    Port range: 443
    Source: 0.0.0.0/0
    Allow
    Rule #200 → Deny all
    Type: All Traffic
    Protocol: All
    Port range: All
    Source: 0.0.0.0/0
    Deny
4. Go to Outbound Rules → Edit outbound rules → Add rules
    Rule #100 → Allow HTTPS (port 443)
    Destination: 0.0.0.0/0
    Allow
    Rule #200 → Deny all traffic
    Deny
5. Click Save changes
Now only HTTPS (port 443) is allowed; everything else is blocked.
STEP 6 — Associate NACL with your Subnet

1. In your Network ACL → Subnet associations → Edit subnet associations
2. Select your subnet (MySubnet)
3. Click Save associations
The ACL now controls inbound and outbound traffic for that subnet.
(Optional) STEP 7 — Launch EC2 Instance
You can launch an instance in your VPC to test:
Go to EC2 → Launch Instance
In Network Settings, choose:
VPC: MyVPC
Subnet: MySubnet
Launch instance and test HTTPS connectivity.

Q2. How do you grant read access to a specific S3 bucket for an IAM user?
Ans: Answer:
To grant read-only access to a specific Amazon S3 bucket for an IAM user:
1. Login to AWS Console → Go to IAM → Users.
2. Select the IAM user who needs access.
3. Go to the Permissions tab → Click Add permissions.
4. Choose Attach policies directly → Click Create policy.
5. Use the JSON tab and add the following policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::my-example-bucket",
        "arn:aws:s3:::my-example-bucket/*"
      ]
    }
  ]
}
```

6. Replace my-example-bucket with your bucket name.
7. Click Next → Review → Create policy.
8. Attach the policy to the IAM user.
Result:
The user can view and download objects (read-only) from that specific S3 bucket only.

Slip 20

Q1. How do you allow only traffic from other EC2 instances in the same security group?

Lunch ec2 instance the security group will automatically create
Use this security group

Select our instance then scroll down —>click networking —> scroll right side then see name of security group

- To Find security group go on security group list
- Click on security group name —-> edit inbound rule —> source —>change custom to my ip
- Then add rules —>keep default costume tcp —>give port range 22 —> add our security group —> save rule

Steps:

Open AWS Management Console

Go to the EC2 Dashboard and click Security Groups.

Select the Security Group

Choose the security group used by your EC2 instances.

Edit Inbound Rules

Click Edit inbound rules.

Add a Rule

Select the Type of traffic you want to allow (for example, All traffic or Custom TCP).

In the Source field, choose Custom and then select the same security group ID (for example, `sg-0123456789abcdef`).

Save Rules

Click Save rules to apply the changes.

Q2. How can you set up an S3 bucket to be publicly accessible?

1. Go to AWS Console → S3 → Create Bucket.
2. Enter a unique bucket name and region.
3. Uncheck “Block all public access.”
4. Confirm the warning → Create the bucket.
5. After creation, click on s3 bucket name → go to the Permissions tab → edit →Bucket Policy
6. At the top of the page, click “Policy Generator” (blue link).

In the new window:

Select Type of Policy: → S3 Bucket Policy
Effect: → Allow
Principal: → * (it mention that any one can access the policy)

Actions: → GetObject
ARN: → Paste your bucket ARN (add /* at the end) (e.g., arn:aws:s3:::slip20bucket/*)(form previous window)

7.Click “Add Statement”, then “Generate Policy.”
8. Copy generated json code
9.paste it on a bucket policy page
10.Click Save.

or

Edit Bucket Policy → Add a JSON policy like:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": "*",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::your-bucket-name/*"
  }]
}
```