Slip2

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

1 Sign in to **AWS Management Console** and open the **EC2 Console** at https://console.aws.amazon.com/ec2/

2 In the navigation pane, click **Instances**.

3 Select the **Windows Server EC2 instance** from the list.

4 Click **Connect** from the top menu.

5 Under the **RDP Client** tab, click **Get Password**.

6 Click **Choose File** and select the **key pair (.pem) file** associated with the instance. Then click **Open**.

7 Click **Decrypt Password** and note down the Administrator password displayed.

8 Click **Download Remote Desktop File** and open the file.

9 If prompted about unknown publisher, click **Connect**.

10 Enter:

- **Username:** Administrator
- **Password:** (from Step 7)

11 If prompted about remote computer identity, click **Yes** to proceed.

12 The **Windows Server Desktop** will appear, indicating a successful connection.

13 After completing tasks, **log off or disconnect** from the instance.

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

- `"Version": "2012-10-17"` – Specifies the policy language version.
- `"Effect": "Allow"` – Grants permissions.
- `"Action"` – List of actions allowed:
    - `ec2:StartInstances` – Start instances.
    - `ec2:StopInstances` – Stop instances.
    - `ec2:DescribeInstances` – View instance details (required to see instances in the console).
- `"Resource": "*"` – Applies to all EC2 instances.

Practical Steps to Create the Policy

1. **Sign in to AWS Management Console** → Go to **IAM**.
2. In the navigation pane, click **Policies** → **Create Policy**.
3. Go to the **JSON** tab and paste the above policy.
4. Click **Next: Tags** (optional) → **Next: Review**.
5. Give the policy a name, e.g., `EC2StartStopPolicy`.
6. Click **Create Policy**.
7. Attach the policy to a user, group, or role.

Slip3

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

   Creating a Custom AMI

1. Sign in to the **AWS Management Console** and go to the **EC2 Console**.
2. In the navigation pane, click **Instances**.
3. Select the configured EC2 instance you want to use.
4. From the **Actions** menu, choose:
   Image and templates → **Create Image**.
5. Enter:
    - **Image Name** and optional **Description**.
6. Choose whether to include:
    - **No Reboot** (optional – skip reboot while creating image).
7. Click **Create Image**.
8. The AMI will appear under **AMIs** in the EC2 console once creation is complete.

Part B – Deleting an AMI

1. Go to the **EC2 Console** → **AMIs**.
2. Select the AMI you want to delete.
3. Choose **Actions** → **Deregister AMI**.

4. Confirm deregistration.
   (This removes the AMI from your account but does not delete snapshots.)
5. Go to **Snapshots** in the EC2 Console.
6. Select the snapshot associated with the AMI and choose **Actions** → **Delete Snapshot**.
7. Confirm deletion to free up storage.

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.

1. Create Two S3 Buckets

1. Sign in to the **AWS Management Console** → Go to **S3**.
2. Click **Create bucket**.
3. Enter a unique **Bucket Name** (e.g., `my-bucket-1`) and choose a region.
4. Keep default settings (or configure as required) → Click **Create bucket**.
5. Repeat steps to create **second bucket** (e.g., `my-bucket-2`).

---

2. Upload Files to First Bucket

1. Open **Bucket 1** (`my-bucket-1`) from the S3 console.
2. Click **Upload** → **Add files** → Select file(s) from local system.
3. Click **Upload** to store files in the bucket.

---

3. Download a Bucket Item

1. Open **Bucket 1** and select the uploaded file.
2. Click **Download**.
3. File will be saved to your local system.

---

4. Copy a Bucket Item to Another Bucket

1. Open **Bucket 1** and select the file.
2. Click **Actions** → **Copy**.
3. Choose **Destination Bucket** (`my-bucket-2`).
4. Click **Copy** to complete.

Slip4) 1)How do you create and manage AWS IAM users and groups?

Create a Group

1. Sign in to **AWS Management Console** → Open **IAM** service.
2. In the navigation pane, click **User groups** → **Create group**.
3. Enter **Group name** (e.g., `DevelopersGroup`).
4. (Optional) Attach policies for required permissions (e.g., `AmazonEC2ReadOnlyAccess`).
5. Click **Create group**.

---

2. Create a User

1. In IAM console, click **Users** → **Create user**.
2. Enter **Username** (e.g., `DevUser1`).
3. Choose access type:
   - **Password** for console access.
   - **Access Key** for programmatic access (CLI/SDK).
4. Attach policies directly or add the user to a group for inherited permissions.
5. Click **Create user**.

---

3. Add User to Group

1. Go to **User groups** → Select the group (e.g., `DevelopersGroup`).
2. Choose **Add users to group**.
3. Select the user(s) and click **Add**.

---

4. Manage Users & Groups

- Modify permissions by attaching/detaching policies.
- Enable **MFA (Multi-Factor Authentication)** for security.
- Rotate access keys regularly.
- Monitor activity with **CloudTrail**.

---

2) 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.

1. Using EBS Snapshots

1. Sign in to **AWS Management Console** → Open **EC2 Console**.
2. In the navigation pane, click **Volumes**.
3. Select the EBS volume attached to the EC2 instance.
4. Click **Actions** → **Create Snapshot**.
5. Enter **Name** and **Description** for the snapshot.
6. Click **Create Snapshot**.
7. (Optional) Use **Data Lifecycle Manager (DLM)** to automate periodic snapshots.

---

2. Using AWS Backup

1. Open **AWS Backup Console**.
2. Click **Create Backup Plan**.
3. Choose **Backup Plan Name** and set schedule (e.g., Daily Backup).
4. Select resources (EC2 instances) to include in the plan.
5. Choose Backup Vault for storage.
6. Confirm and create the backup plan. Backups will occur as per schedule.

Backup of EC2 instance data was successfully performed using **EBS Snapshots** and **AWS Backup**, ensuring data protection and recovery capability.