Secure the Root User Account

1. **Enable Multi-Factor Authentication (MFA)**:
    - Navigate to **IAM** in the AWS Console.
    - Go to the **Security Credentials** section for the root user and enable MFA using an authenticator app (e.g., Google Authenticator).
2. **Limit Root User Access**:
    - Use the root account only for critical tasks (e.g., billing) and rely on IAM users for daily operations.

---

3. Create an IAM User

1. **Navigate to the IAM Console**:
    - In the AWS Management Console, search for and open the **IAM Service**.
2. **Add a New User**:
    - Click **Users** on the left-hand menu, then click **Add Users**.
    - Enter a username for the new user.
    - Select the type of access:
        - **AWS Management Console Access**: For GUI access.
        - **Programmatic Access**: For API, CLI, or SDK usage.
3. **Assign Permissions**:
    - Choose how to assign permissions:
        - **Add User to a Group**: Recommended for managing multiple users.
        - **Attach Policies Directly**: Attach predefined policies like **AdministratorAccess** or **ReadOnlyAccess**.
        - **Copy Permissions**: Clone another user's permissions.
4. **Review and Create User**:
    - Verify the details and click **Create User**.
5. **Download Credentials**:
    - Save the **Access Key ID** and **Secret Access Key** securely. These are only shown once.

---

4. Organize Permissions with Groups

1. **Create an IAM Group**:
    - Navigate to the **Groups** section in IAM and click **Create Group**.
2. **Assign Permissions**:
    - Attach policies to the group (e.g., **PowerUserAccess**, **EC2ReadOnlyAccess**).
3. **Add Users to the Group**:
    - Add the previously created user to the group to grant them the group's permissions.

---

5. Configure IAM User Security

1. **Enable MFA for IAM Users**:
    - Navigate to the user's security settings and enable MFA.
2. **Set Strong Password Policies**:
    - In the IAM settings, enforce password complexity and rotation policies