IAM - Roles

Creating IAM Role - Another AWS Account

- Sign in to the AWS Management Console.
- Open the **IAM** page using the **Services** tab from the menu bar.
- Click the **Roles** link from the menu on the left.
- Click the **Create Role** tab.
- Choose **Another AWS account** option that will use this role.
- For **Account ID**, type the AWS account ID to which you want to grant access to your resources.
- If you are granting permissions to users from an account that you do not control, and the users will assume this role programmatically, then select **Require external ID**. The external ID can be any word or number that is agreed upon between you and the administrator of the third-party account. This option automatically adds a condition to the trust policy that allows the user to assume the role only if the request includes the correct ID.
- If you want to restrict the role to users who sign in with multi-factor authentication (MFA), select **Require MFA**. This adds a condition to the role's trust policy that checks for an MFA sign-in.
- Click **Next: Permissions** tab.
- If possible, select the policy to use as the permission policy or choose **Create policy** to open a new browser tab and create a new policy from scratch.
- Let's select AmazonS3FullAccess policy via the search bar for this example.
- This policy will allow another AWS accounts to access all S3 resources when EC2 assumes this role.
- Then click **Next: Tags** tab.
- Optionally, type a tag or tags as key-value pairs.
- Click Next: Review tab.
- Type a **name** for your role. Role names must be **unique** within your AWS account.
- Use a maximum of 64 **alphanumerics** and **'+=,.@-_' characters**.
- Click **Create role** tab.
- The role would be created successfully.

- Choose **Another AWS account** option that will use this role.
- For **Account ID**, type the AWS account ID to which you want to grant access to your resources.
- If you are granting permissions to users from an account that you do not control, and the users will assume this role programmatically, then select **Require external ID**. The external ID can be any word or number that is agreed upon between you and the administrator of the third-party account. This option automatically adds a condition to the trust policy that allows the user to assume the role only if the request includes the correct ID.
- If you want to restrict the role to users who sign in with multi-factor authentication (MFA), select **Require MFA**. This adds a condition to the role's trust policy that checks for an MFA sign-in.
- Click **Next: Permissions** tab.