AWS ROLES AND POLICIES

Example Scenario :

AMAZON S3 BUCKET

EC2 INSTANCE

IAM USER

POLICY

AWS CLI

Create EC2 Instance

* Go to <https://aws.amazon.com>.
* Sign into console then click on EC2 instance.
* The page is open after that click on launch instance.

1. Name : appserver
2. AMI : amazon linux
3. Key pair : appkey@

* Then click on launch instance.

Create S3 bucket

* Go to console then click on S3.

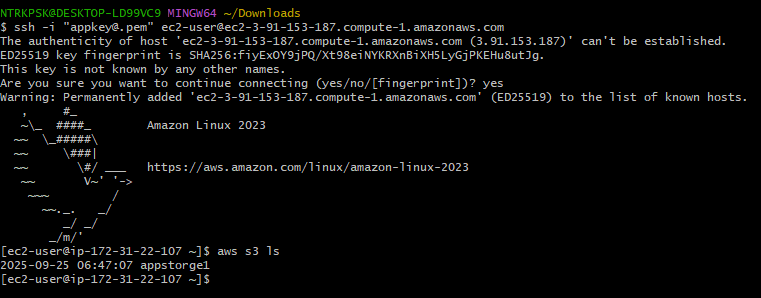
1. Name : app storage 1

Create IAM role

* Go to IAM then click on roles.

1. Trusted Entity type : AWS service
2. Service Usecase : EC2
3. Permission policies : Amazon S3 full access

* Then click on create role.
* Again go to appserver instance then click on instance Id.
* The page is open then click on connect and the connect page is open click on ssh client.
* Copy that command.
* Go to downloads open that appkey@ in git bash paste that command and click on enter.
* Next enter this command aws s3 ls.



* Go to appserver instance click on actions.
* Then click on security after that modify that IAM role.
* Choose that role and update it.

Let us create Customized Policies

* Go to policy then click on create policy.
* Select your policy editor Json or manual
* Select which service you want.
* Give permissions for that service.
* Then click on create.

AWS Organizations : AWS Organizations is a free account management service that allows you to centrally manage and govern multiple AWS accounts.