



LOGICLABS TECHNOLOGIES

www.logiclabstech.com

Amazon Web Services

Roles & Reports

ankitnarula1991@gmail.com

Roles

- A role is a set of permissions that grant access to actions and resources in AWS. These permissions are attached to the role.
- **Features of IAM Roles**
- A role is not uniquely associated with a single person; it can be used by anyone who needs it.
- A role does not have long term security credential, i.e., password or security key.
- We will assign permissions to AWS Services with IAM Roles.
- Up to 10 policies can be assigned to a role

Roles

- Go to IAM Service
- Go to Roles
- Click on Create Role
- Select AWS Service
- Select EC2 & Click on Permissions
- Select the policy we want to attach to our role
- Search S3FullAccess

Roles

- Click on Next
- Click on Next
- Enter the name of the role
- Click on create role
- Create Linux EC2 Machine
- Attach Role to the EC2 Machine

Roles

- Select EC2 Machine



- Select IAM Role
 - Click on save
 - Now connect EC2 Machine using the Putty
 - Create IAM user
- ```
aws iam create-user --user-name <User_Name>
```

# Roles

- Create the S3 Bucket

```
aws s3 mb s3://<Bucket_Name>
```

# Credential Reports

- We can generate and download a credential report that lists all users in our account and the status of their various credentials, including passwords, access keys, and MFA devices.
- Go to IAM Service
- Click on Credential Report
- Click on Download Report



[ankitnarula1991@gmail.com](mailto:ankitnarula1991@gmail.com)