



**LOGICLABS TECHNOLOGIES**

[www.logiclabstech.com](http://www.logiclabstech.com)

# **Amazon Web Services**

---

## **Groups & Attach Policies**

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

# Groups & Attach Policies

- An IAM Group is a collection of users. Group specifies the permission for a collection of users, and it also makes it possible to manage the permissions easily for those users.
- Following are some important characteristics of user groups:
  - A user group can contain many users, and a user can belong to multiple user groups.
  - User groups can't be nested; they can contain only users, not other user groups.
  - There is no default user group that automatically includes all users in the AWS account. If you want to have a user group like that, you must create it and assign each new user to it.
  - Default Quota is 300 Groups For an AWS Account & Max quota is 500 Groups

# Groups & Attach Policies

- Go to IAM
- Click on User groups
- Click on Create Group
- Enter the name of the group
- Attach Permission policies
- Search S3Full Access
- Click on Create Group

# Groups & Attach Policies

- Create new user with Group
- Select AWS Access Type
- Enter password
- Click on Next: Permissions
- Select Add user to group
- Click on Add: Tags
- Click on Create User
- Login with User
- Check the S3 Bucket

# Groups & Attach Policies

- **Remove User & Add User in Group**
- Create One more Group
- Attach Permissions Policies
- Search EC2 Read only
- Create Group
- Open First Group
- Select the user

# Groups & Attach Policies

- Click on Remove users
- Open Second Group
- Click on Add Users
- Select the user & Click on Add users
- Now check group



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