AWS IAM

Topics to be covered--IAM

1) IAM Introduction

2) Users

3) Creating users with different policies

4) Password types

5) MFA

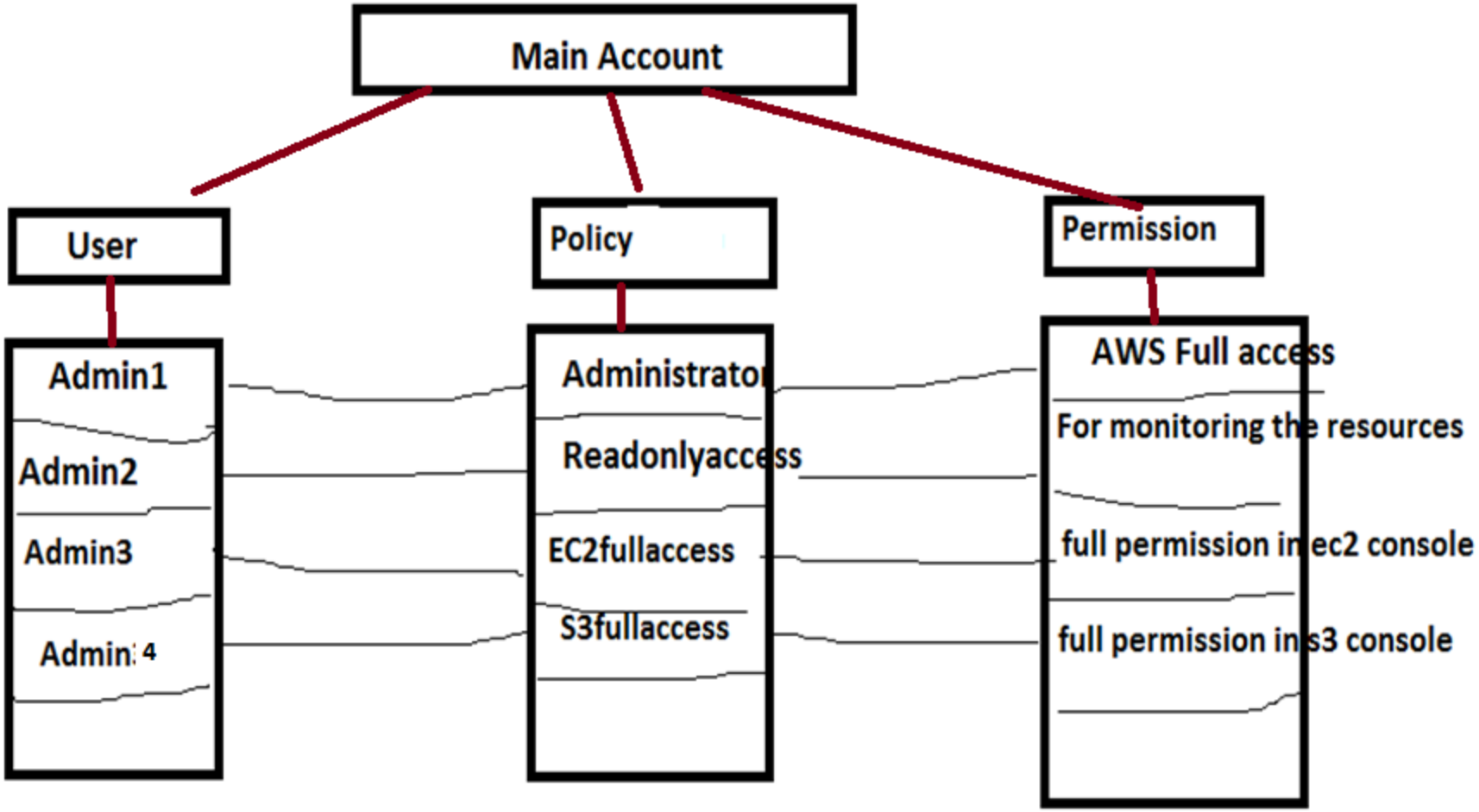
6) Policies –default and custom

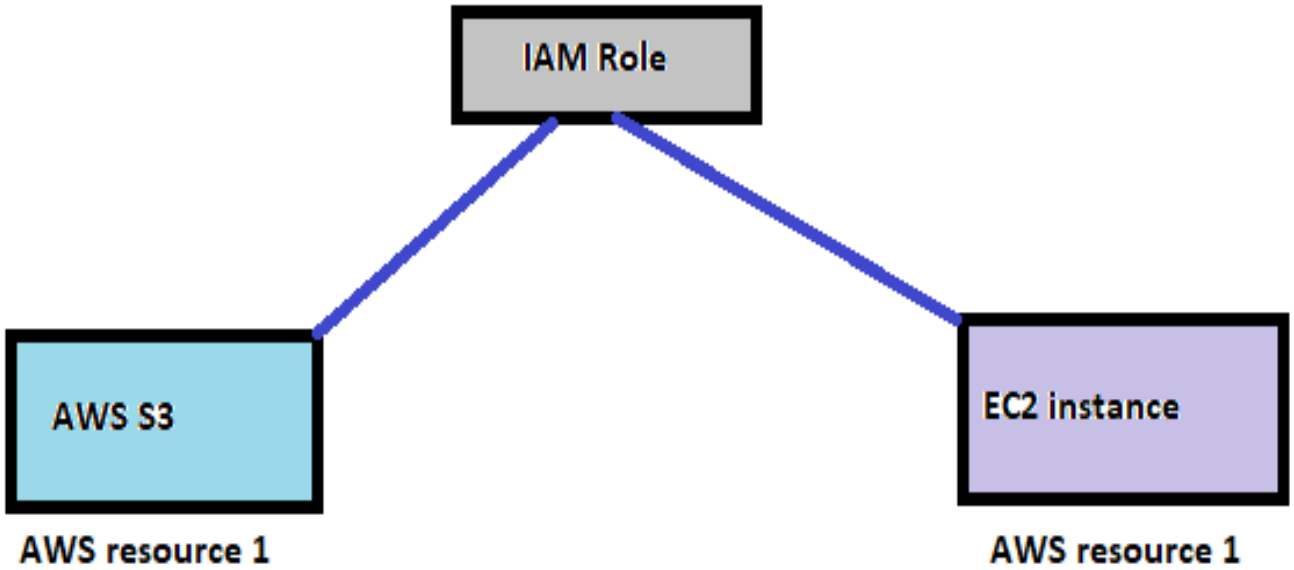
7) Role – default and custom

8) Group

AWS IAM Hands on

1) Create an IAM user and assign full access in aws console
2) Create an IAM user and assign full access in ec2 console only
3) Create an IAM user and assign full access in S3 console only
4) Create an IAM user and assign read only access in aws console
5) How to add multiple permission to an user
6) Create group –add user—assign policy
7) Configure custom policy
8) Creating Roles
10) Autogenerated password
10) Configure MFA – 2 step authentication for user aws console login
11) Sync S3 bucket with EC2 instance


Main Account
User
Policy
Permission
Admin1
Admin2
Admin3
Admin 4
Administrator
Readonlyaccess
EC2fullaccess
S3fullaccess
AWS Full access
For monitoring the resources
full permission in ec2 console
full permission in s3 console



IAM Role help to interact two different reource in aws

IAM

- IAM stands for Identity Access Management.
- It is used to set users, permissions and roles. It allows you to grant access to the different parts of the aws platform.
- With IAM, Organizations can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.
- Without IAM, Organizations with multiple users must either create multiple user accounts, each with its own billing and subscriptions to AWS products or share an account with a single security credential. Without IAM, you also don't have control about the tasks that the users can do.
- IAM enables the organization to create multiple users, each with its own security credentials, controlled and billed to a single aws account. IAM allows the user to do only what they need to do as a part of the user's job.

AWS Root User

- When you first create an AWS account, you create an account as a root user identity which is used to sign in to AWS.
- You can sign to the AWS Management Console by entering your email address and password. The combination of email address and password is known as **root user credentials**.
- When you sign in to AWS account as a root user, you have unrestricted access to all the resources in AWS account.
- The Root user can also access the billing information as well as can change the password also.

IAM Roles

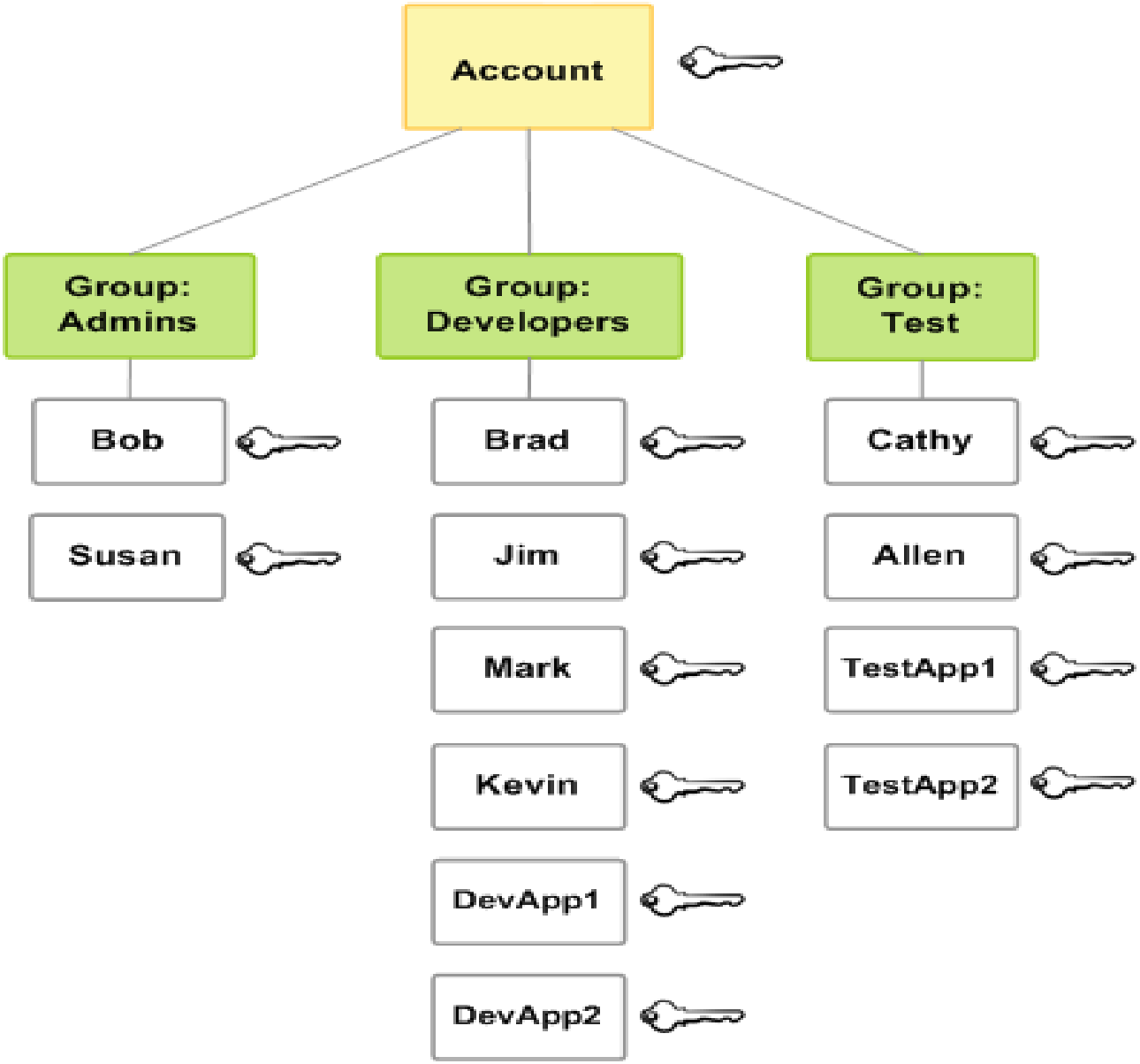
- A role is a set of permissions that grant access to actions and resources in AWS. These permissions are attached to the role, not to an IAM User or a group.
- An IAM User can use a role in the same AWS account or a different account.
- You can use the roles to delegate access to users, applications or services that generally do not have access to your AWS resources.

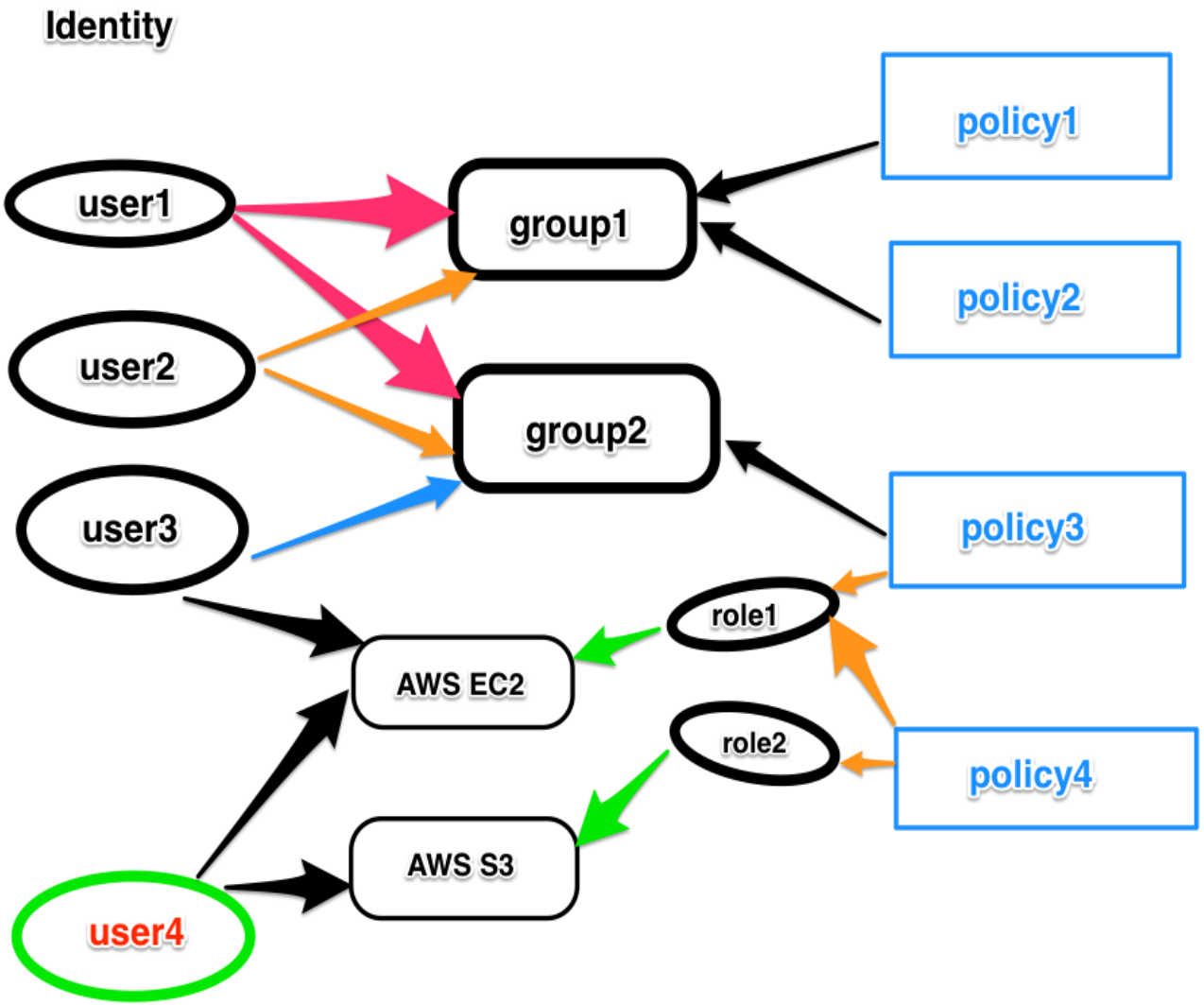
- A role is not uniquely associated with a single person; it can be used by anyone who needs it

IAM Components

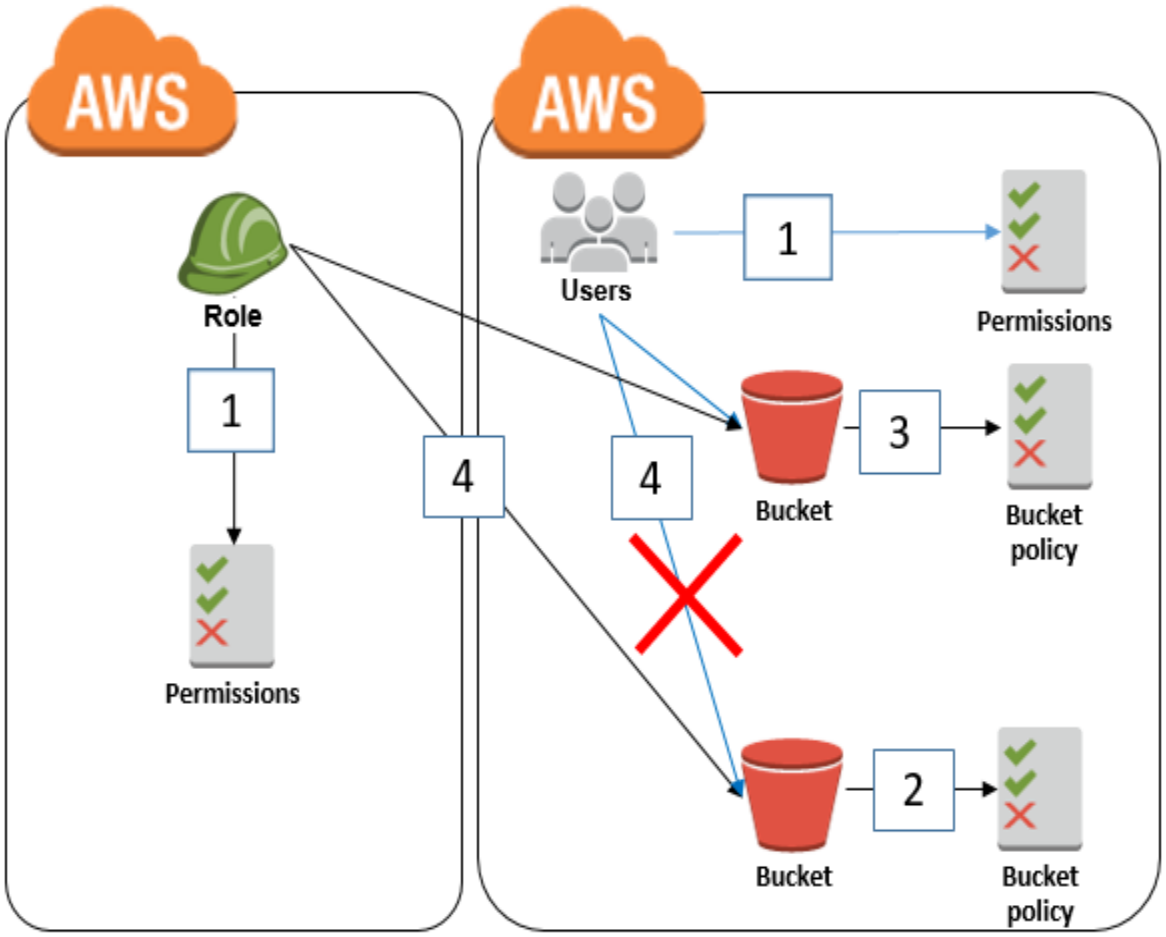
1) Users –Entity to manage different aws resource
2) Group –set of users
3) Policy --permission
4) Role –set of policy
5) Password

- ✓ AWS Console Management password
- ✓ Auto generated password
- ✓ Multi factor Authentication(MFA)

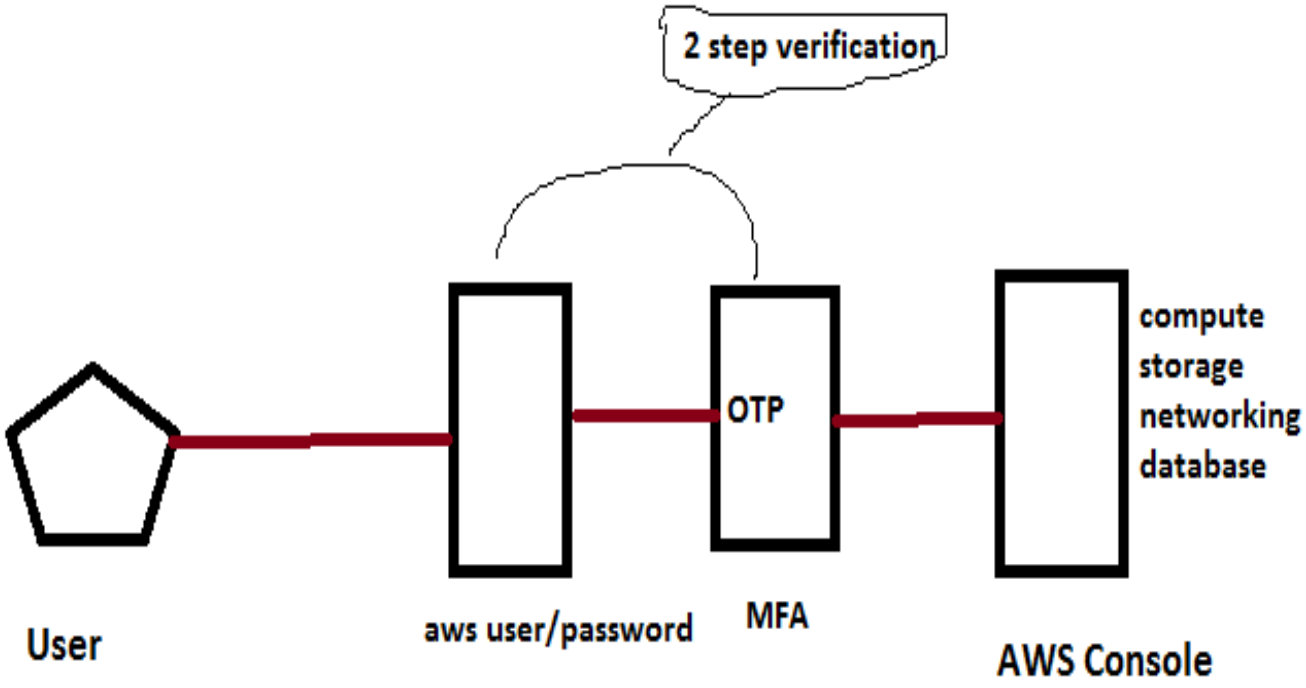

Account
Group: Admins
Group: Developers
Group: Test
Bob
Susan
Brad
Jim
Mark
Kevin
DevApp1
DevApp2
Cathy
Allen
TestApp1
TestApp2


Identity
policy1
user1
group1
policy2
user2
group2
user3
policy3
role1
AWS EC2
role2
policy4
AWS S3
user4

Roles and policies

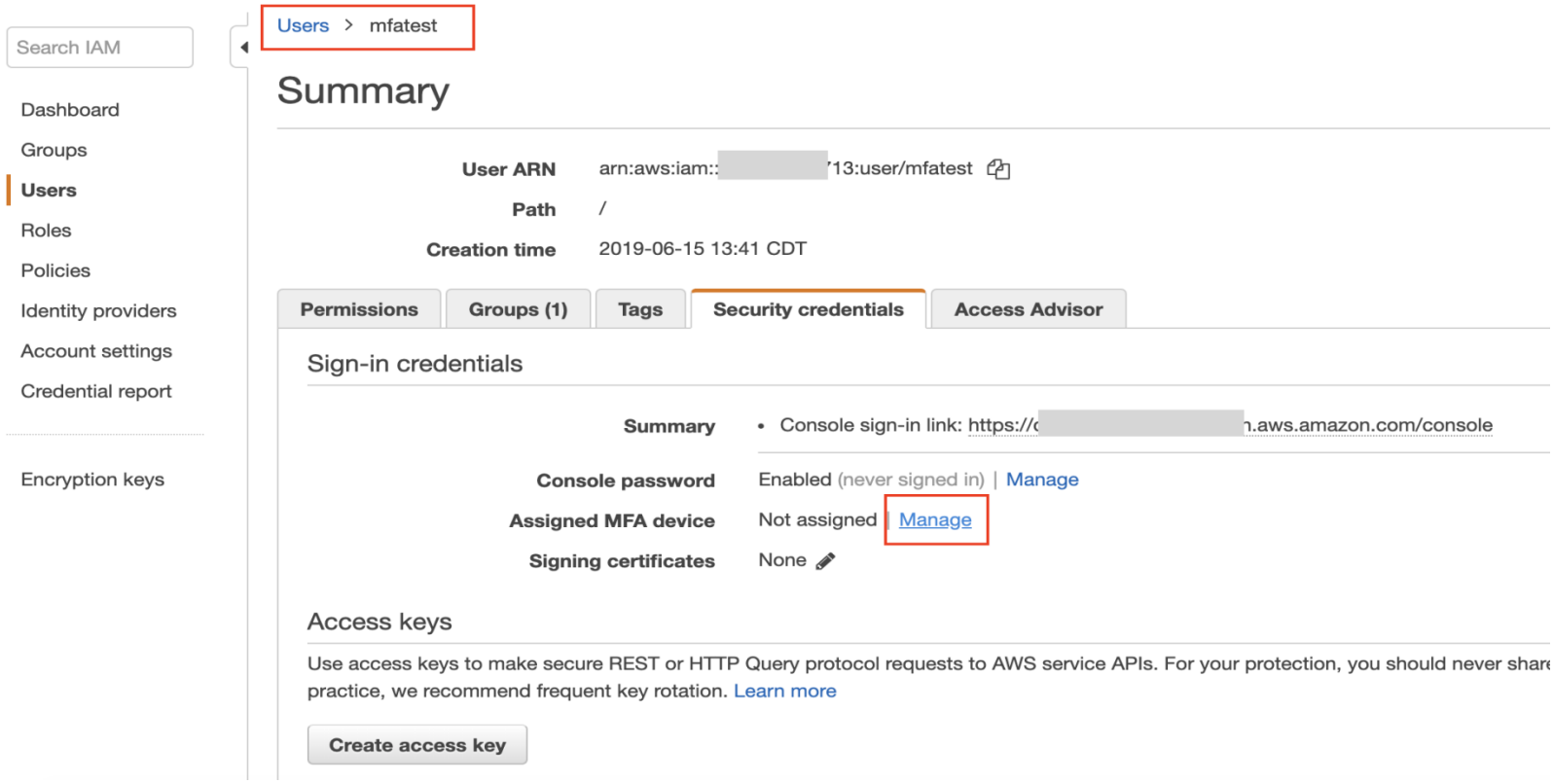


MFA -Muti Factor Authentication



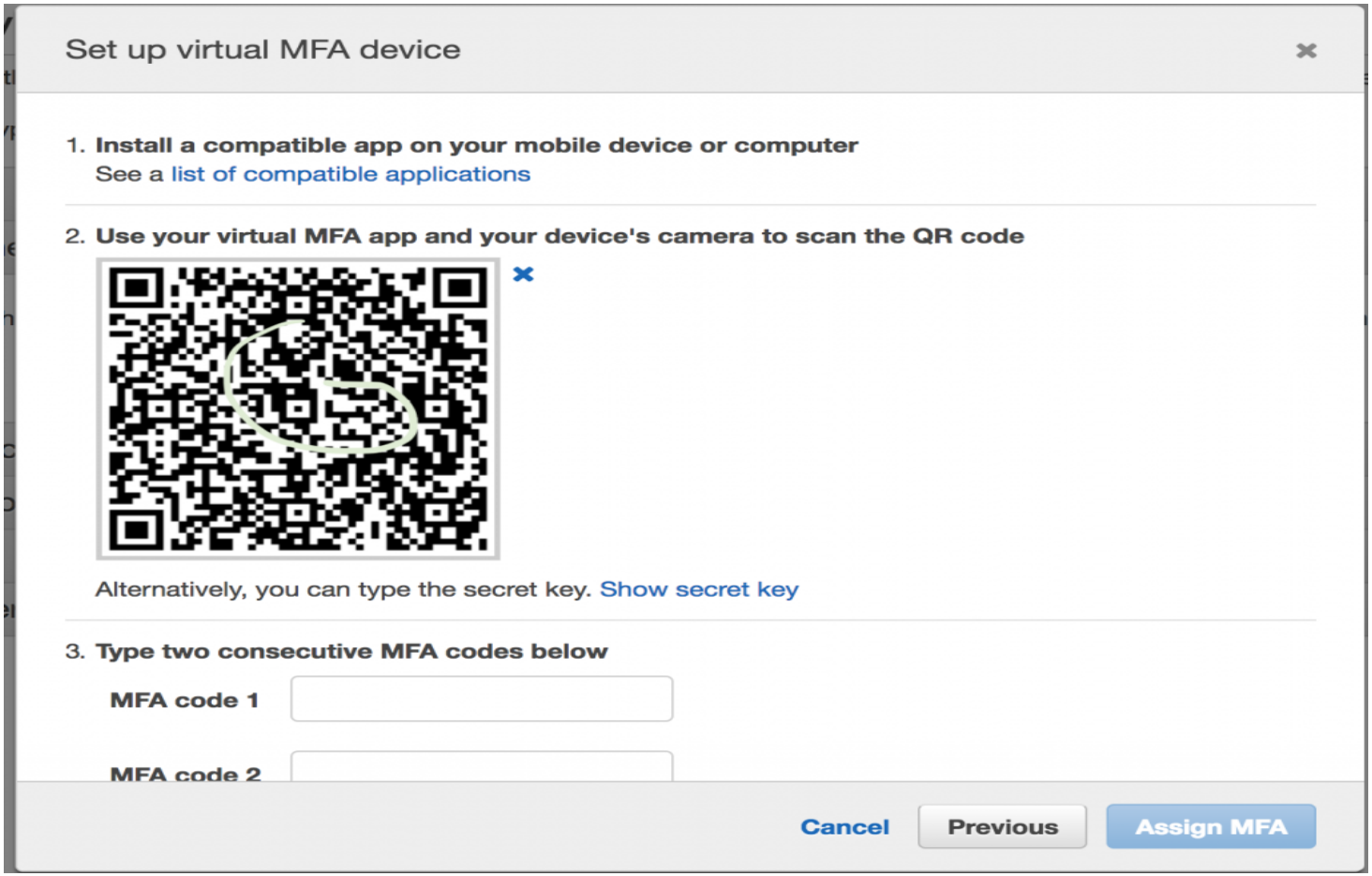
Lab: Configure MFA

1) This is two step authentication
2) Create an user in IAM
3) After creating --Open it – security credential –Assign MFA– Manage--



Lab: Configure MFA

Now select Virtual MFA– Download google authenticator from play store in android mbile –open and scan this code –one by one two code will displayed there—put these code here--- Assign MFA



us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algori

aws

Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

575909

Submit

Cancel

Policy examples

1) Create policy to start and stop instance and add with user to check with specific instance.

2) Create policy to create bucket and upload(put) files in any bucket and add with any user.

3) Create bucket policy to access it from specific IP address only.

4) S3 bucket Access control list (ACL)