



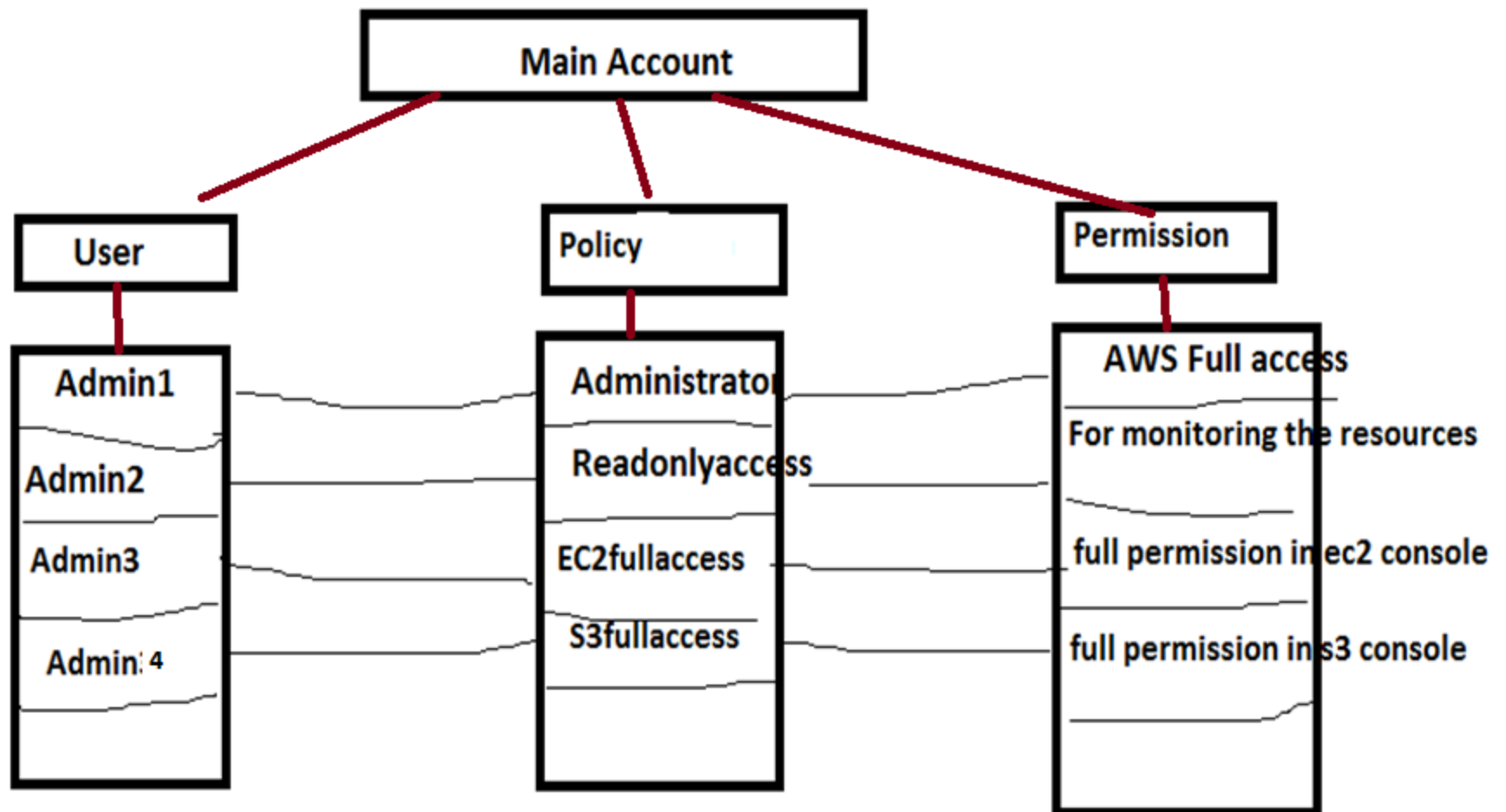
AWS IAM

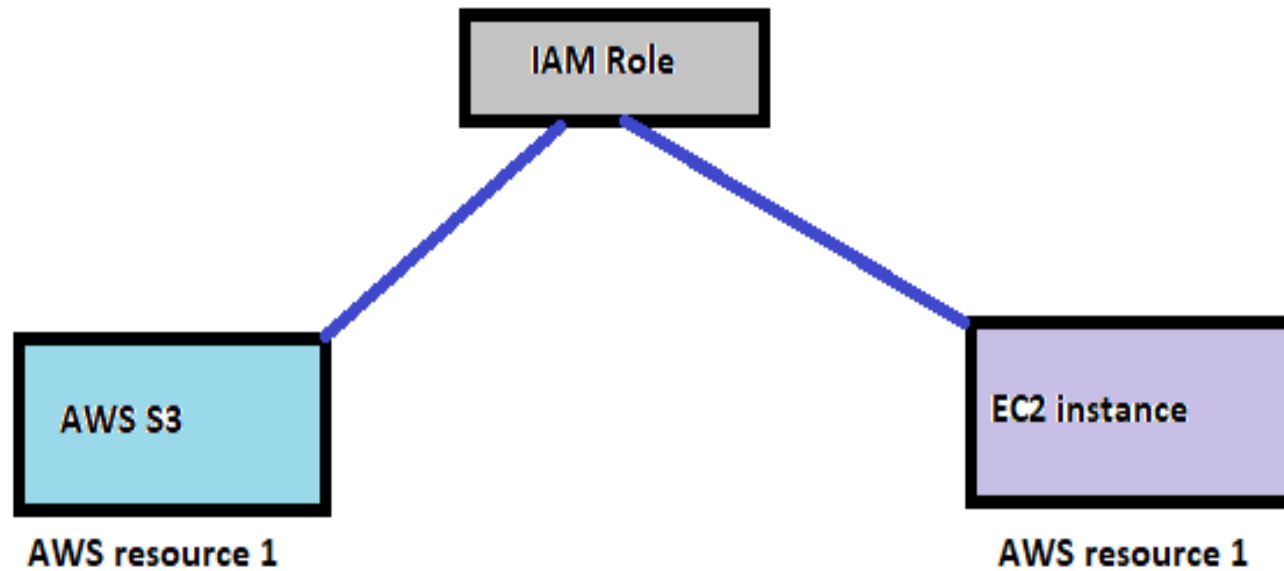
Topics to be covered--IAM

- 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





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

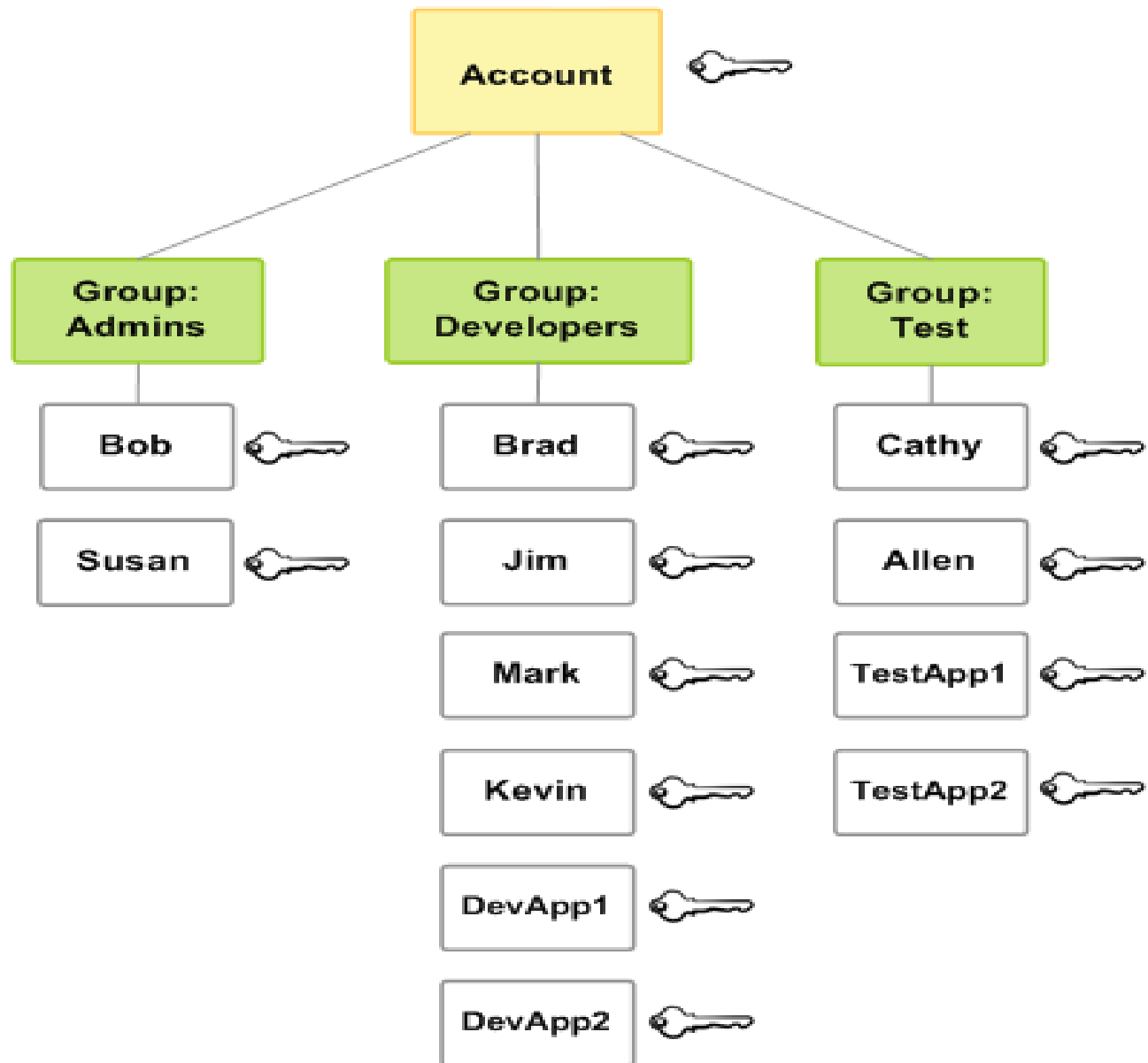
- When you first create an AWS account, you create an account as a root user identity which is used to sign in to AWS.
- You can sign to the AWS Management Console by entering your email address and password. The combination of email address and password is known as **root user credentials**.
- When 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

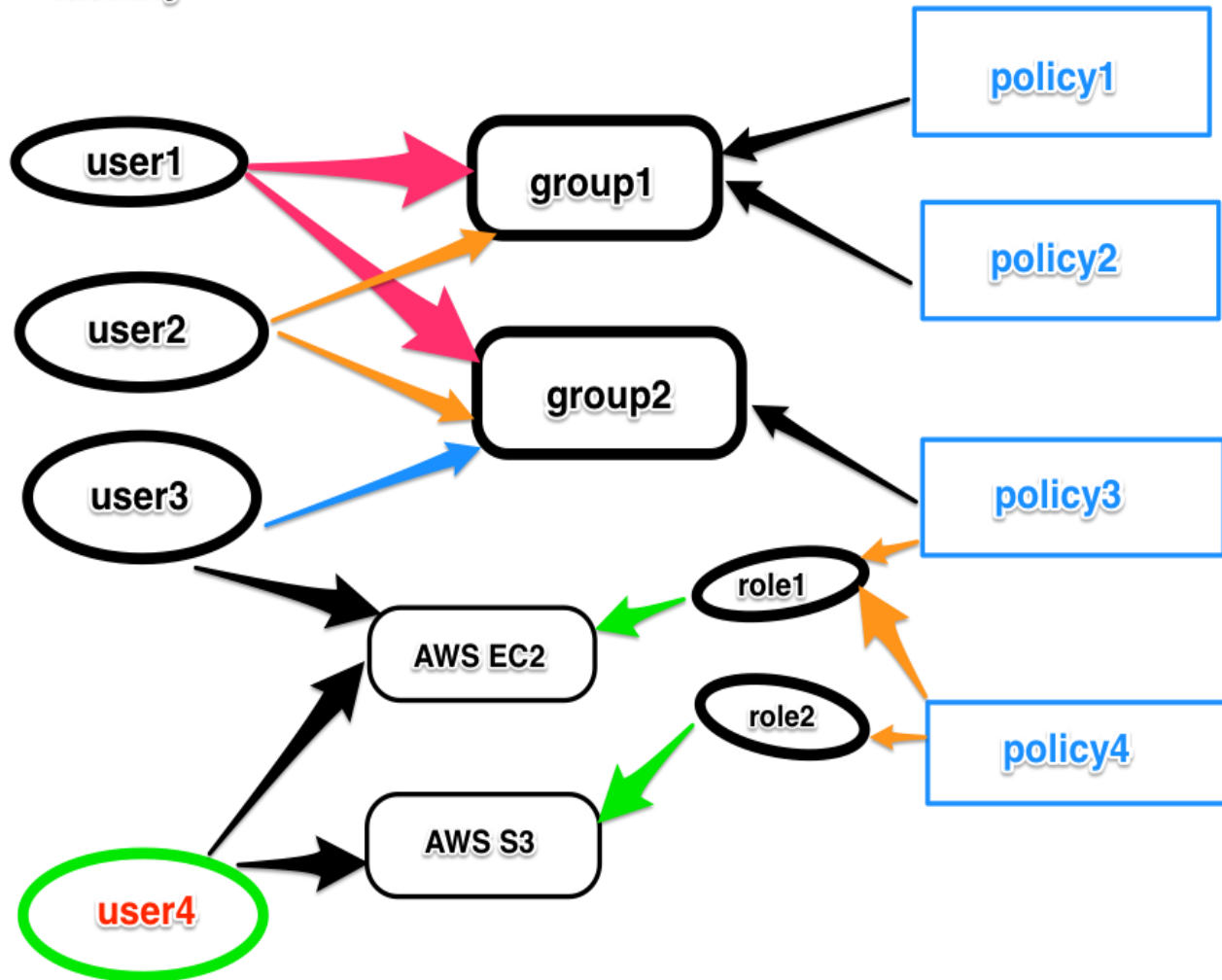
- A role is a set of permissions that grant access to actions and resources in AWS. These permissions are attached to the role, not to an IAM User or a group.
- An IAM User can use a role in the same AWS account or a different account.
- You can use the roles to delegate access to users, applications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

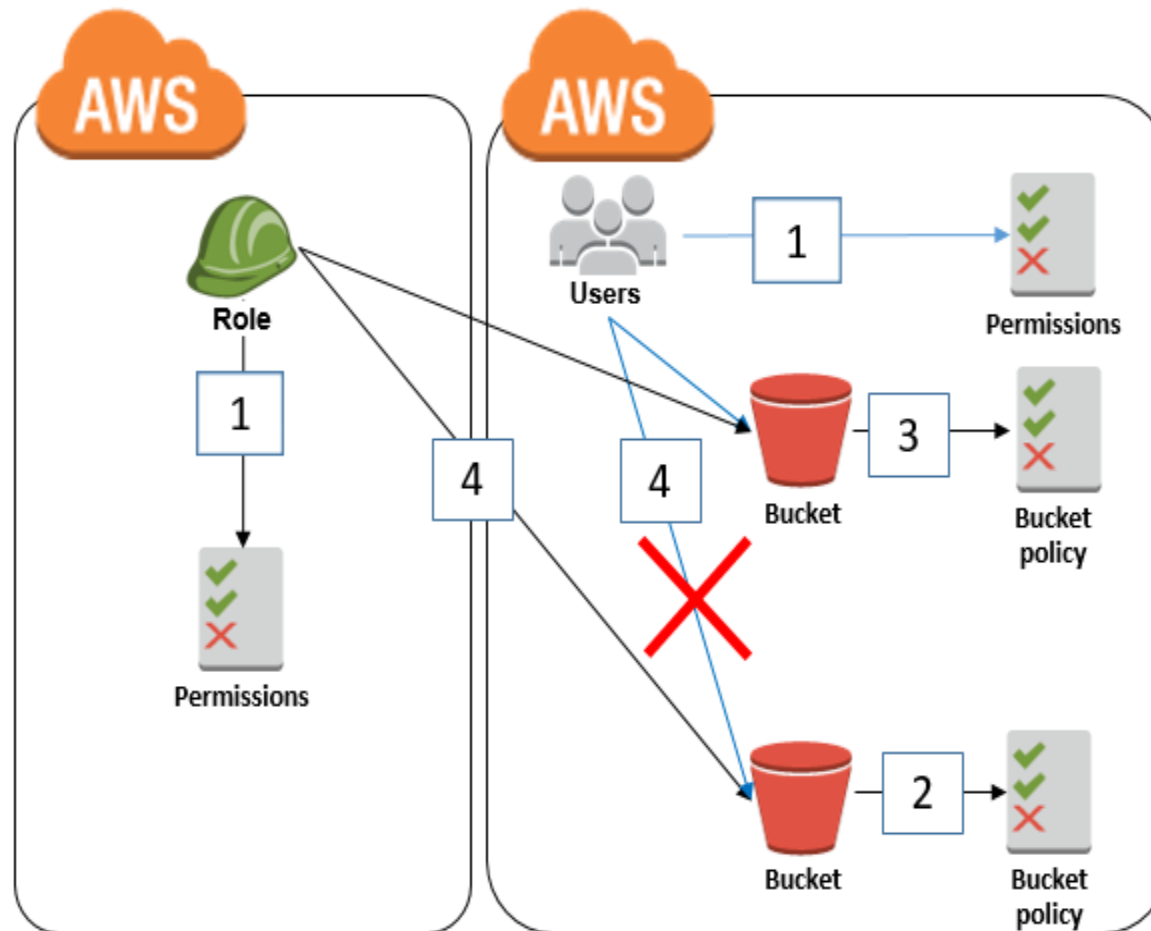
- 1) Users –Entity to manage different aws resource
- 2) Group –set of users
- 3) Policy --permission
- 4) Role –set of policy
- 5) Password
 - ✓ AWS Console Management password
 - ✓ Auto generated password
 - ✓ Multi factor Authentication(MFA)



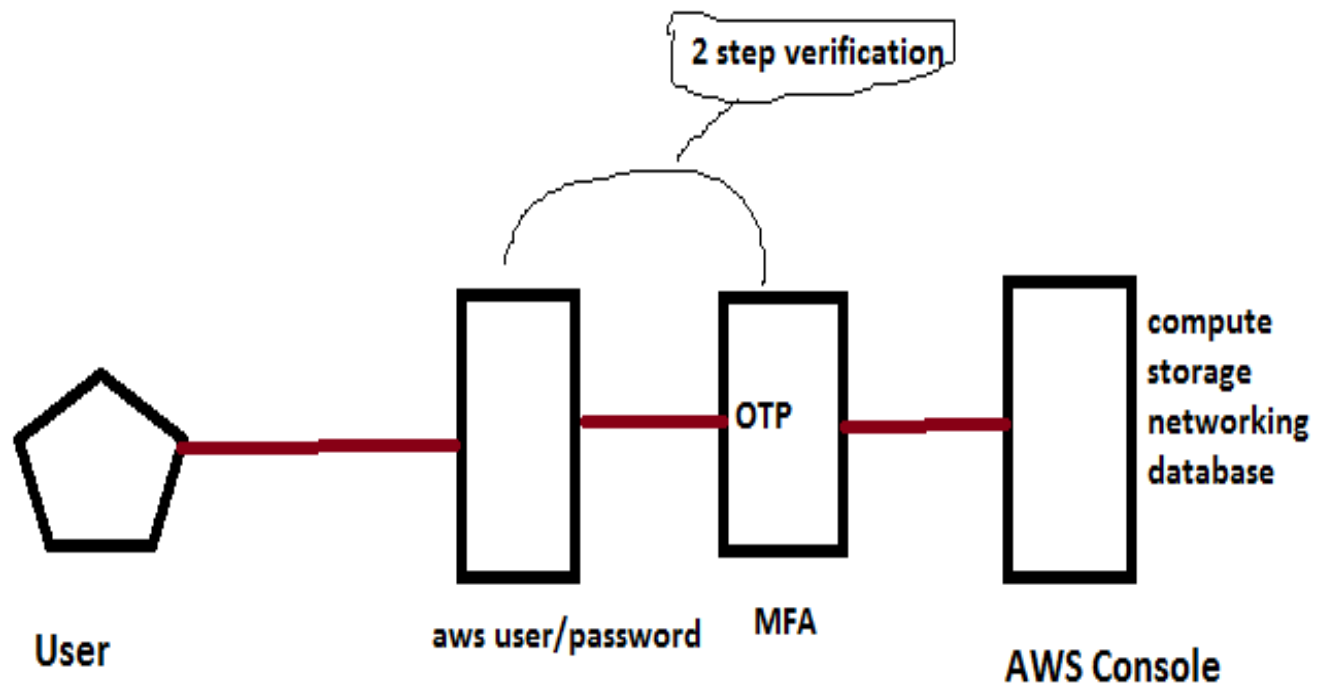
Identity



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--

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with links to Search IAM, Dashboard, Groups, Users (highlighted), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area shows the 'Users > mfatest' path. The 'Summary' tab is active, displaying the User ARN, Path, and Creation time. Below this, the 'Security credentials' tab is selected, showing the 'Sign-in credentials' section. This section includes a 'Summary' row with a console sign-in link, a 'Console password' row (Enabled), an 'Assigned MFA device' row (Not assigned), and a 'Signing certificates' row (None). The 'Manage' link next to 'Assigned MFA device' is highlighted with a red box. At the bottom, there is an 'Access keys' section with a 'Create access key' button.

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Users > mfatest

Summary

User ARN arn:aws:iam::[redacted]:user/mfatest

Path /

Creation time 2019-06-15 13:41 CDT

Permissions **Groups (1)** **Tags** **Security credentials** **Access Advisor**

Sign-in credentials

Summary

- Console sign-in link: [https://\[redacted\].aws.amazon.com/console](https://[redacted].aws.amazon.com/console)

Console password Enabled (never signed in) | [Manage](#)

Assigned MFA device Not assigned | [Manage](#)

Signing certificates None

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share practice, we recommend frequent key rotation. [Learn more](#)

[Create access key](#)


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

Set up virtual MFA device

1. Install a compatible app on your mobile device or computer
See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

MFA code 2

Cancel

Previous

Assign MFA



Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

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)