AWS IAM Overview

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users.
- IAM is used to control
  - **Identity** – who can use your AWS resources (authentication)
  - **Access** – what resources they can use and in what ways (authorization)
- IAM can also keep your account credentials private.
- With IAM, multiple IAM users can be created under the umbrella of the AWS account or temporary access can be enabled through identity federation with corporate directory.or third party providers
- IAM also enables access to resources across AWS accounts.

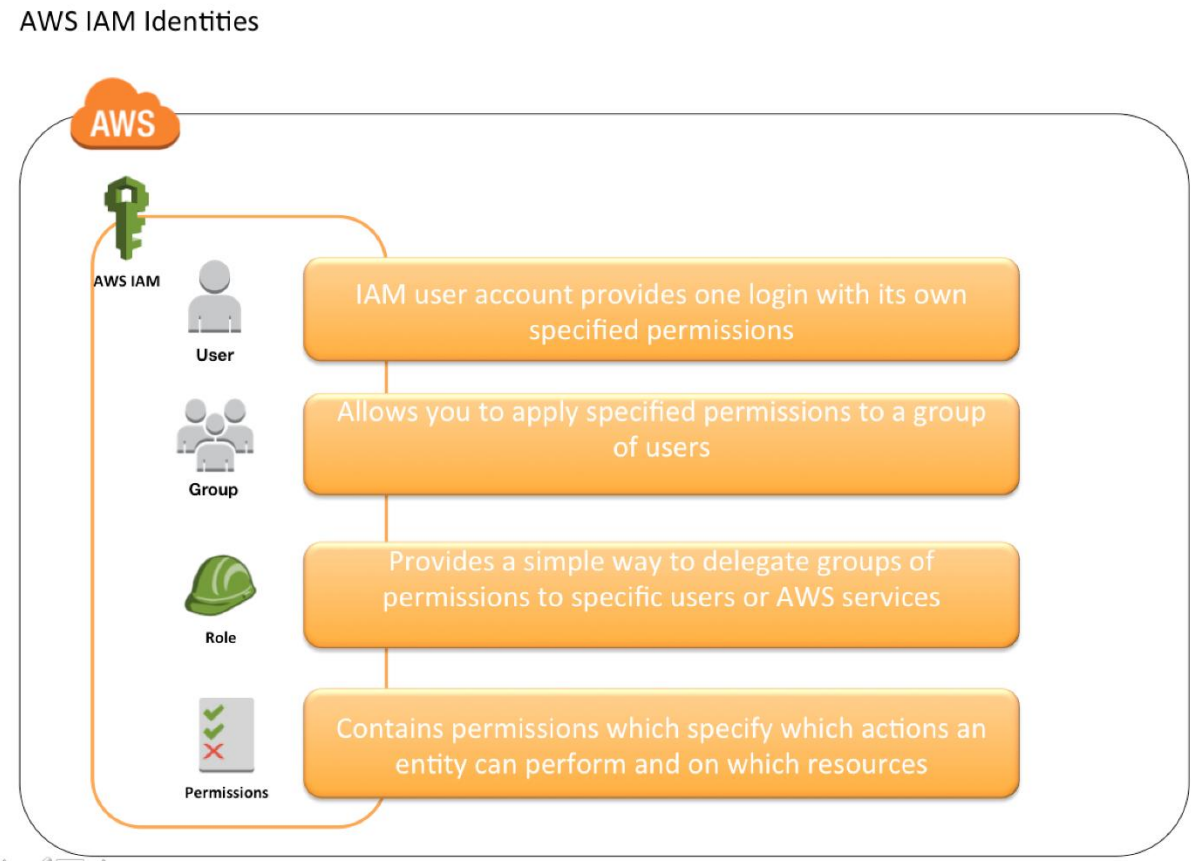
IAM Features

- Shared access to your AWS account
  - Grant other people permission to administer and use resources in your AWS account without having to share your password or access key.
- Granular permissions
  - Each user can be granted with different set granular permissions as required to perform their job
- Secure access to AWS resources for applications that run on EC2
  - IAM can help provide applications running on EC2 instance temporary credentials that they need in order to access other AWS resources
- Identity federation
  - IAM allows users to access AWS resources, without requiring the user to have accounts with AWS, by providing temporary credentials *for e.g. through corporate network or Google or Amazon authentication*
- Identity information for assurance
  - CloudTrail can be used to receive log records that include information about those who made requests for resources in the account.
- PCI DSS Compliance
  - IAM supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being Payment Card Industry Data Security Standard (PCI DSS) compliant
- Integrated with many AWS services
  - IAM integrates with almost all the AWS services
- Eventually Consistent
  - IAM, like many other AWS services, is eventually consistent and achieves high availability by replicating data across multiple servers within Amazon's data centers around the world.
  - Changes made to IAM would be eventually consistent and hence would take some time to reflect
- Free to use

    - IAM is offered at no additional charge and charges are applied only for use of other AWS products by your IAM users.
- AWS Security Token Service
    - IAM provide STS which is an included feature of the AWS account offered at no additional charge.
    - AWS charges only for the use of other AWS services accessed by the AWS STS temporary security credentials.

Identities

IAM identities determine who can access and help to provide authentication for people and processes in your AWS account



Account Root User

- Root Account Credentials are the email address and password with which you sign-in into the AWS account
- Root Credentials has full unrestricted access to AWS account including the account security credentials which include sensitive information
- **IAM Best Practice** – Do not use or share the Root account once the AWS account is created, instead create a separate user with admin privilege

- An Administrator account can be created for all the activities which too has full access to the AWS account except the accounts security credentials, billing information and ability to change password

IAM Users

- IAM user represents the person or service who uses the access to interact with AWS.
- **IAM Best Practice** – Create Individual Users
- User credentials can consist of the following
  - **Password** to access AWS services through AWS Management Console
  - **Access Key/Secret Access Key** to access AWS services through API, CLI or SDK
- IAM user starts with no permissions and is not authorized to perform any AWS actions on any AWS resources and should be granted permissions as per the job function requirement
- **IAM Best Practice** – Grant least Privilege
- Each IAM user is associated with one and only one AWS account.
- IAM User cannot be renamed from AWS management console and has to be done from CLI or SDK tools.
- IAM handles the renaming of user w.r.t unique id, groups, policies where the user was mentioned as a principal. However, you need to handle the renaming in the policies where the user was mentioned as a resource

Credential Type	Use	Description
Passwords	AWS root account or IAM user account login to the AWS Management Console	A string of characters used to log into your AWS account or IAM account. AWS passwords must be a minimum of 6 characters and may be up to 128 characters.
Multi-Factor Authentication (MFA)	AWS root account or IAM user account login to the AWS Management Console	A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account.
Access Keys	Digitally signed requests to AWS APIs (using the AWS SDK, CLI, or REST/Query APIs)	Includes an access key ID and a secret access key. You use access keys to digitally sign programmatic requests that you make to AWS.
Key Pairs	• SSH login to EC2 instances • CloudFront signed URLs	A key pair is required to connect to an EC2 instance launched from a public AMI. The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys. You can have a key pair generated automatically for you when you launch the instance or you can upload your own.
X.509 Certificates	• Digitally signed SOAP requests to AWS APIs • SSL server certificates for HTTPS	X.509 certificates are only used to sign SOAP-based requests (currently used only with Amazon S3). You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the Security Credentials page.

IAM Groups

- IAM group is a collection of IAM users
- IAM groups can be used to specify permissions for a collection of users sharing the same job function making it easier to manage
- **IAM Best Practice** – Use groups to assign permissions to IAM Users
- A group is not truly an identity because it cannot be identified as a Principal in an access policy. It is only a way to attach policies to multiple users at one time
- A group can have multiple users, while a user can belong to multiple groups (10 max)
- Groups cannot be nested and can only have users within it
- AWS does not provide any default group to hold all users in it and if one is required it should be created with all users assigned to it.
- Renaming of a group name or path, IAM handles the renaming w.r.t to policies attached to the group, unique ids, users within the group. However, IAM does not update the policies where the group is mentioned as a resource and must be handled manually
- Deletion of the groups requires you to detach users and managed policies and delete any inline policies before deleting the group. With AWS management console, the deletion and detachment is taken care of.

IAM Roles

Refer to My Blog Post about IAM Role

MultiFactor Authentication (MFA)

- For increased security and to help protect the AWS resources, Multi-Factor authentication can be configured
- **IAM Best Practice** – Enable MFA on Root accounts and privilege users
- Multi-Factor Authentication can be configured using
  - Security token-based
    - AWS Root user or IAM user can be assigned a hardware/virtual MFA device
    - Device generates a six digit numeric code based upon a time-synchronized one-time password algorithm which needs to be provided during authentication
  - SMS text message-based (Preview Mode)

    - IAM user can be configured with the phone number of the user's SMS-compatible mobile device which would receive a 6 digit code from AWS
    - SMS-based MFA is available only for IAM users and does not work for AWS root account
- MFA needs to enabled on the Root user and IAM user separately as they are distinct entities. Enabling MFA on Root does not enable it for all other users
- MFA device can be associated with only one AWS account or IAM user and vice versa
- If the MFA device stops working or is lost, you won't be able to login into the AWS console and would need to reach out to AWS support to deactivate MFA
- MFA protection can be enabled for service api's calls using *"Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}* and is available only if the service supports temporary security credentials.

IAM Access Management

Refer to My Blog Post about IAM Policy and Permissions

Credential Report

- IAM allows you to generate and download a credential report that lists all users in the account and the status of their various credentials, including passwords, access keys, and MFA devices.
- Credential report can be used to assist in auditing and compliance efforts
- Credential report can be used to audit the effects of credential lifecycle requirements, such as password and access key rotation.
- **IAM Best Practice** – Perform Audits and Remove all unused users and credentials
- Credential report is generated as often as once every four hours. If the existing report was generated less than four hours, the same is available for download. If more then four hours, IAM generates and downloads a new report.