IAM

- What is IAM
- IAM features
- IAM Terms
- Root User
- IAM user
- IAM group
- IAM Roles

IAM - Identity and Access Management

- AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely.
- Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources
- IAM is used to control
  - Identity – who can use your AWS resources (authentication)
  - Access – what resources they can use and in what ways (authorization)
- Using IAM, multiple IAM users, groups, roles can be created in an AWS account.

IAM features

- Shared access to your AWS account
  - You can grant other people permission to administer and use resources in your AWS account without having to share your credentials (password or access key)
- Granular permissions
  - You can grant different permissions to different people for different resources.
- Secure access to AWS resources for applications that run on AWS Amazon
- Multi-factor authentication (MFA)
  - You can add two-factor authentication to your account and to individual users for extra security.
- Identity federation
  - You can allow users who already have passwords elsewhere—for example, in your corporate network or with an internet identity provider—to get temporary access to your AWS account.

IAM features

- 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 compliant with Payment Card Industry (PCI) Data Security Standard (DSS).
- Integrated with many AWS services
- Most services can integrate with IAM
- Eventually Consistent
  - IAM, like many other AWS services, is eventually consistent.
  - IAM achieves high availability by replicating data across multiple servers within Amazon's data centers around the world.
- Free to use
  - AWS Identity and Access Management (IAM) and AWS Security Token Service (AWS STS) are features of your AWS account offered at no additional charge.

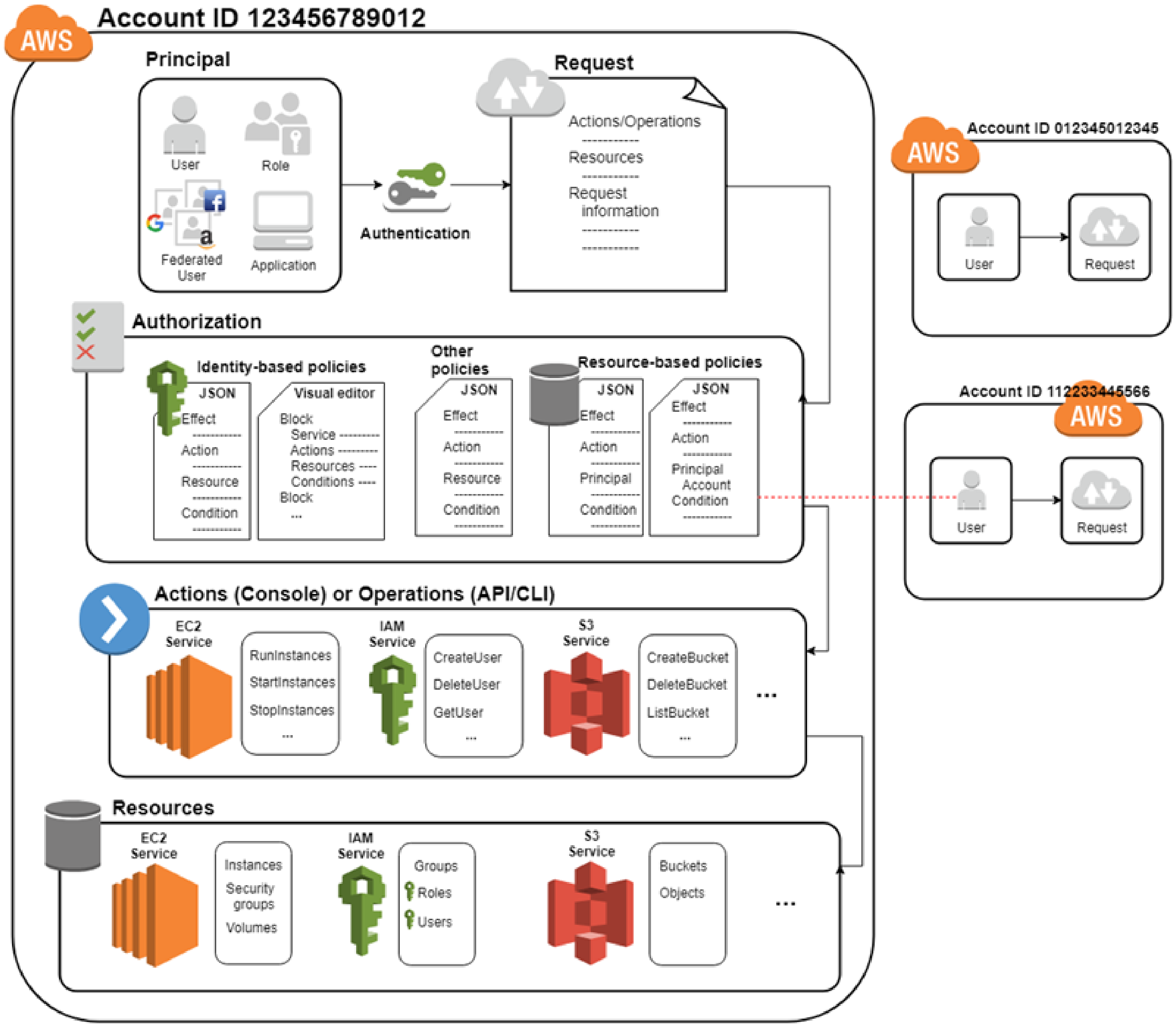
IAM Terms

- IAM Resources
  - The user, group, role, policy, and identity provider objects that are stored in IAM.
- IAM Identities
  - The IAM resource objects that are used to identify and group. You can attach a policy to an IAM identity. These include users, groups, and roles.
- IAM Entities
  - The IAM resource objects that AWS uses for authentication. These include IAM users and roles.
- Principals
  - A person or application that uses the AWS account root user, an IAM user, or an IAM role to sign in and make requests to AWS. Principals include federated users and assumed roles.

IAM Terms

- Authentication
  - Who can use your AWS resources
  - A principal must be authenticated using their credentials.
  - Amazon S3 and AWS STS, allow a few requests from anonymous users. However, they are the exception to the rule.
- Authorization
  - What resources you can use and in which ways
  - AWS check attached policies that apply to the request.
  - It determines whether to allow or deny the request.
  - Policies are stored in AWS as JSON documents format

How IAM works…



Root User

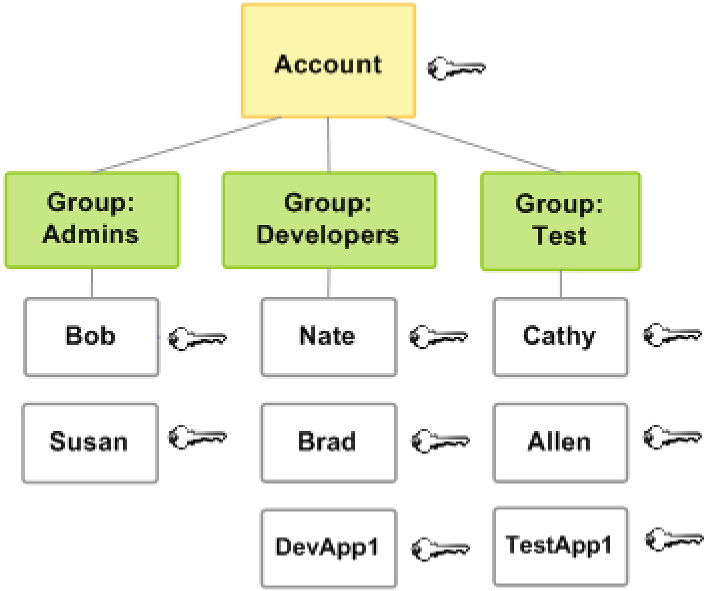
- When you create an AWS account, you create an AWS account root user.
- Root Account Credentials are the email address and password with which you sign-in into the AWS account
- Root Credentials has full unrestricted access to AWS account including the account security credentials which include sensitive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

IAM user

- IAM user represents the person or service who uses the access the AWS account.
- User credentials can consist of the following
  - User name, password to access 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
- Each IAM user is associated with one and only one AWS account.

IAM group

- 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
- A group is 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)
- 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.



IAM Roles

- An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS
- IAM role is not intended to be uniquely associated with a particular user, group or service and is intended to be assumable by anyone who needs it.
- Role does not have any credentials associated with it
- Role helps in access delegation to grant permissions to someone that allows access to resources that you control
- Roles can help to prevent accidental access to or modification of sensitive resources
- Modification of a Role can be done anytime and the changes are reflected across all the entities associated with the Role immediately

Roles for Amazon EC2

- If you run applications on Amazon EC2 instances and those applications need access to AWS resources, you can provide temporary security credentials to your instances when you launch them.
- These temporary security credentials are available to **all applications** that run on the instance