**IDENTITY AND ACCESS MANAGEMENT**

**IAM Service:**

* Stands for Identity Access Management
* Comes under Security Engineering
* Is a web service that helps you securely control access to AWS resources.
* With IAM, you can centrally manage permissions that control which AWS resources users can access.
* A global service
* You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
* When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account
* After creating IAM user, you can sign in as IAM user, with the Account ID, username and password and work in the environment among the services that are permitted by the IAM admin

**IAM Features:**

* Shared access to your AWS account
* Granular permissions
* Secure access to AWS resources for applications that run on Amazon EC2
* Multi-factor authentication
* Identity information for assurance
* Integrated with many AWS services
* Eventually consistent
* Free to use

**Components of IAM:**

**Users**

* An IAM user is an identity with an associated credential and permissions attached to it
* With IAM, you can securely manage access to AWS services by creating an IAM user name for each employee in your organization
* Each IAM user is associated with only one AWS account
* By default, a newly created user is not authorized to perform any action in AWS
* The advantage of having one-to-one user specification is that you can individually assign permissions to each user.

**How to create a IAM user?**

* Go to services -> Security, Identity, & Compliance -> Users -> Add user

**Step 1**

* Enter the user name
* Select “Provide user access to the AWS Management console”
* Select “I want to create an IAM user”
* Create password either by autogenerating or custom password
* Select “Users must create a new password at next sign-in”, if needed
* Click on next

**Step 2**

**Permission options:**

* Select attach policies directly
* In permission policies, add the policies to attach to new user

Example: AmazonEC2FullAccess, AmazonEC2ReadOnlyAccess, AmazonS3FullAccess

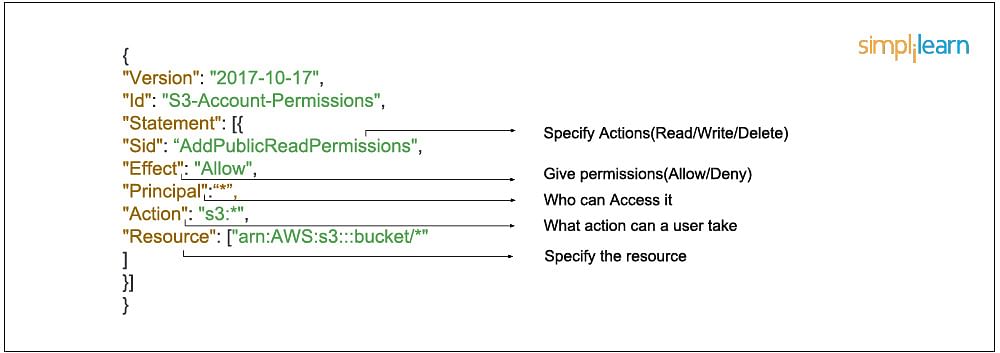
* Add tags to help identify, organize, or search for resources, if needed
* Click create user

**User groups**

* A collection of IAM users is an IAM group.
* You can use IAM groups to specify permissions for multiple users so that any permissions applied to the group are applied to the individual users in that group as well
* Managing groups is quite easy
* You set permissions for the group, and those permissions are automatically applied to all the users in the group
* If you add another user to the group, the new user will automatically inherit all the policies and the permissions already assigned to that group

**Policies**

* An IAM policy sets permission and controls access to AWS resources
* Policies are stored in AWS as JSON documents
* Permissions specify who has access to the resources and what actions they can perform. For example, a policy could allow an IAM user to access one of the buckets in [Amazon S3](https://www.simplilearn.com/tutorials/aws-tutorial/aws-s3)
* The policy would contain the following information:
  + Who can access it
  + What actions that user can take
  + Which AWS resources that user can access
  + When they can be accessed



**Types of Policies:**

* P

**Roles**

Service to Service access

Example: EC2-S3 (Permission)

With Role

Without Role

**MFA**

How to create MFA

How to remove MFA

**Accessing IAM:**

**By using AWS GUI :**

AWS console access

Credentials:

Account ID

Username

Password

**How to create policy:**

* Create a user group
* Enter name of the group
* Go to policies
  + Choose service
  + Choose actions
* Create next
* Click review
  + Enter name
  + Create policy

**By using CLI:**

* Go to User -> Security credentials -> Access keys **->** Create access key **->** Command line interface
* Create access key
* An access key and a secret access key will be created. Download the .csv file
* Launch a Linux instance
* In the terminal, enter the following:
  + sudo su –
  + aws configure
  + Enter aws access key
  + Enter aws secret access key
  + Enter region (say ‘us-east-1’)
  + Enter output format: json
  + aws s3 ls

To list out all the buckets

* Now, all the buckets in the s3 will be displayed
* Similarly we can use various commands