What is IAM?

- IAM stands for Identity Access Management.
- IAM allows you to manage users and their level of access to the aws console.
- It is used to set users, permissions and roles. It allows you to grant access to the different parts of the aws platform.
- AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS.
- 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.

Features of IAM

- **Centralised control of your AWS account:** You can control creation, rotation, and cancellation of each user's security credentials. You can also control what data in the aws system users can access and how they can access.
- **Shared Access to your AWS account:** Users can share the resources for the collaborative projects.
- **Granular permissions:** It is used to set a permission that user can use a particular service but not other services.
- **Identity Federation:** An Identity Federation means that we can use Facebook, Active Directory, LinkedIn, etc with IAM. Users can log in to the AWS Console with same username and password as we log in with the Active Directory, Facebook, etc.

- **Multifactor Authentication:** An AWS provides multifactor authentication as we need to enter the username, password, and security check code to log in to the AWS Management Console.
- **Permissions based on Organizational groups:** Users can be restricted to the AWS access based on their job duties, for example, admin, developer, etc.
- **Networking controls:** IAM also ensures that the users can access the AWS resources within the organization's corporate network.
- **Provide temporary access for users/devices and services where necessary:** If you are using a mobile app and storing the data in AWS account, you can do this only when you are using temporary access.
- **Integrates with many different aws services:** IAM is integrated with many different aws services.
- **Supports PCI DSS Compliance:** PCI DSS (Payment Card Industry Data Security Standard) is a compliance framework. If you are taking credit card information, then you need to pay for compliance with the framework.
- **Eventually Consistent:** IAM service is eventually consistent as it achieves high availability by replicating the data across multiple servers within the Amazon's data center around the world.
- **Free to use:** AWS IAM is a feature of AWS account which is offered at no additional charge. You will be charged only when you access other AWS services by using IAM user.

What is SAML?

- SAML stands for Security Assertion Markup language.
- Generally, users need to enter a username and password to login in any application.
- SAML is a technique of achieving **Single Sign-On (SSO)**.
- Security Assertion Markup Language (SAML) is an Xml-based framework that allows the identity providers to provide the authorization credentials to the service provider.
- With SAML, you need to enter one security attribute to log in to the application

- SAML is a link between the authentication of the user's identity and authorization to use a service.
- SAML provides a service known as Single Sign-On means that users have to log in once and can use the same credentials to log in to another service provider.

Why SAML?

- With SAML, both the service provider and identity provider exist separately, but centralizes the user management and provides access to the SaaS solutions.
- SAML authentication is mainly used for verifying the user's credentials from the identity provider.

Advantages of SAML:

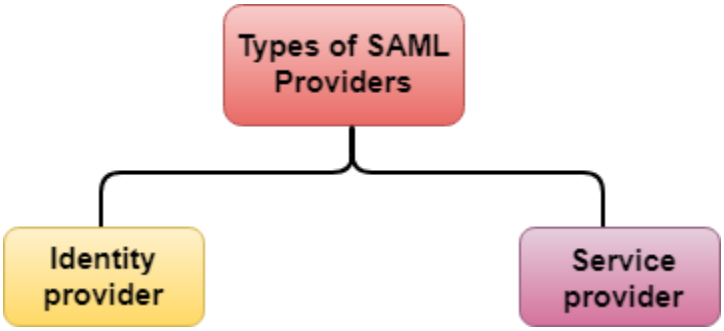
- **SAML SSO (SINGLE SIGN-ON):** SAML provides security by eliminating passwords for an app and replacing them with the security tokens. Since we do not require any passwords for SAML logins, there is no risk of credentials to be stolen by unauthorized users. It provides faster, easier and trusted access to cloud applications.
- **Open Standard SINGLE SIGN-ON:** SAML implementations confirms to the open standard. Therefore, it is not restricted to a single identity provider. This open standard allows you to choose the SAML provider.
- **Strong Security:** SAML uses federated identities and secure tokens to make SAML one of the best secure forms for web-based authentication.
- **Improved online experience for end users:** SAML provides SINGLE SIGN-ON (SSO) to authenticate at an identity provider, and the identity provider sends the authentication to the service provider without additional credentials.
- **Reduced administrative costs for service providers:** Using single authentication multiple times for multiple services can reduce the administrative costs for maintaining the account information.
- **Risk transference:** SAML has put the responsibility of handling the identities to the identity provider.

Types of SAML providers

SAML provider is an entity within a system that helps the user to access the services that he or she wants.

There are two types of SAML providers:

- Service provider
- Identity provider



Service provider

- It is an entity within a system that provides the services to the users for which they are authenticated.
- Service provider requires the authentication from the identity provider that grants the access to the user.
- Salesforce and other CRM are the common service providers.

Identity provider

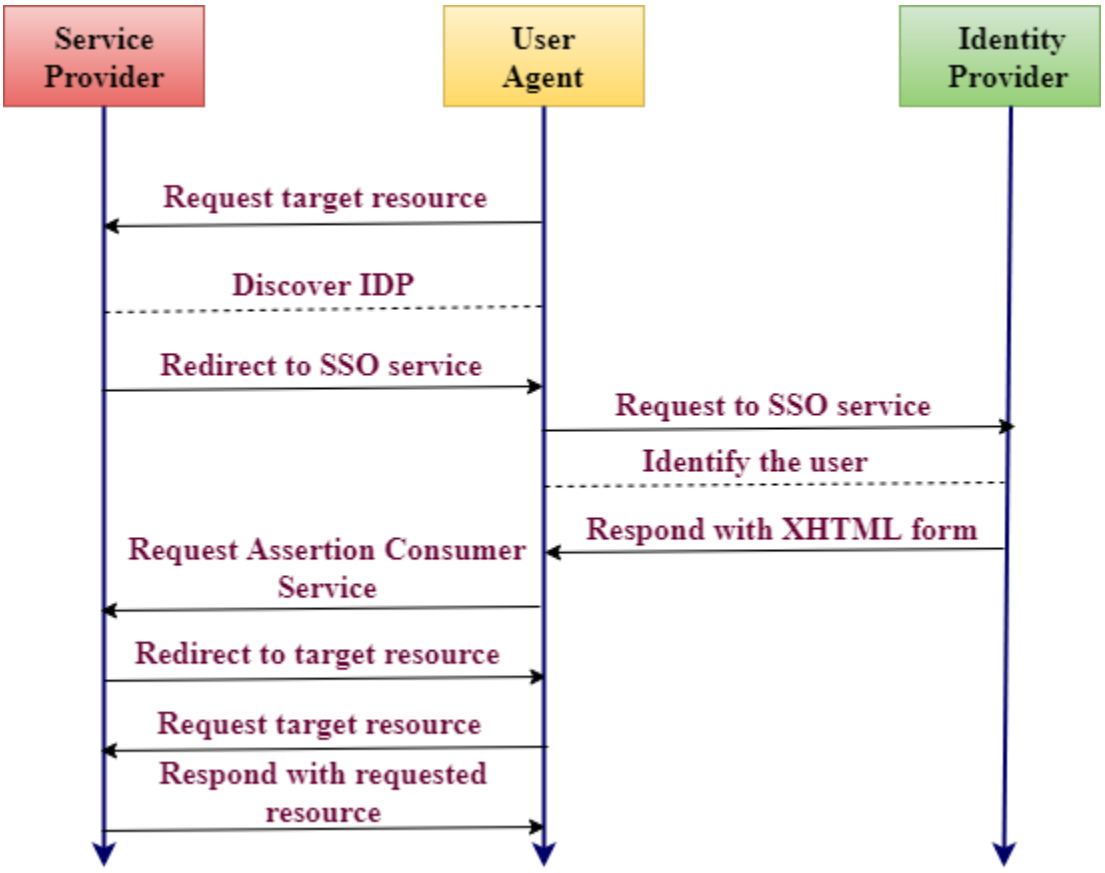
- An identity provider is an entity within a system that sends the authentication to the service provider is about who they are along with the user access rights.
- It maintains a directory of the user and provides an authentication mechanism.
- Microsoft Active Directory and Azure are the common identity providers.

What is a SAML Assertion?

A SAML Assertion is an XML document that the identity provider sends to the service provider containing user authorization.

SAML Assertion is of three types:

- **Authentication**
  - It proves the identification of the user
  - It provides the time at which the user logged in.
  - It also determines which method of authentication has been used.
- **Attribute**
  - An attribute assertion is used to pass the SAML attributes to the service provider where attribute contains a piece of data about the user authentication.
- **Authorization decision**
  - An authorization decision determines whether the user is authorized to use the service or identity provider denied the request due to the password failure.



- If a user tries to access the resource on the server, the service provider checks whether the user is authenticated within the system or not. If you are, you skip to step 7, and if you are not, the service provider starts the authentication process.
- The service provider determines the appropriate identity provider for you and redirects the request to the identity provider.
- An authentication request has been sent to the SSO (SINGLE SIGN-ON) service, and SSO service identifies you.
- The SSO service returns with an XHTML document, which contains authentic information required by the service provider in a SAMLResponse parameter.
- The SAMLResponse parameter is passed to the Assertion Consumer Service (ACS) at the service provider.
- The service provider processes the request and creates a security context; you automatically logged in.
- After login, you can request for a resource that you want.
- Finally, the resource is returned to you.