IAM Identity Federation

Amazon Web Services

IAM Identity Federation

For federation with Facebook, Google and Amazon, AWS IAM provides integration with OpenID (OIDC). Using this method, you can trade the authentication token you get from the Idp with a temporary credentials in AWS and map it to an IAM role with the required permission to access resources on AWS

You do not need to embed the AWS access keys in the application making the request.

You will need to configure appropriate roles using the **'AssumeRoleWithWebIdentity'** API call.

IAM ACADEMY

IAM Identity Federation

For federation with Active Directory, AWS supports SAML 2.0, an open standard used by many identity providers which enables federated single sign-on (SSO). This feature us used to enable users sign into the AWS Management Console or make programmatic calls to AWS APIs by using assertions from a SAML-compliant identity provider (IdP) like Microsoft Active Directory Federation Services (ADFS). Once you setup ADFS in your environment, you publish a website which would have URL similar to

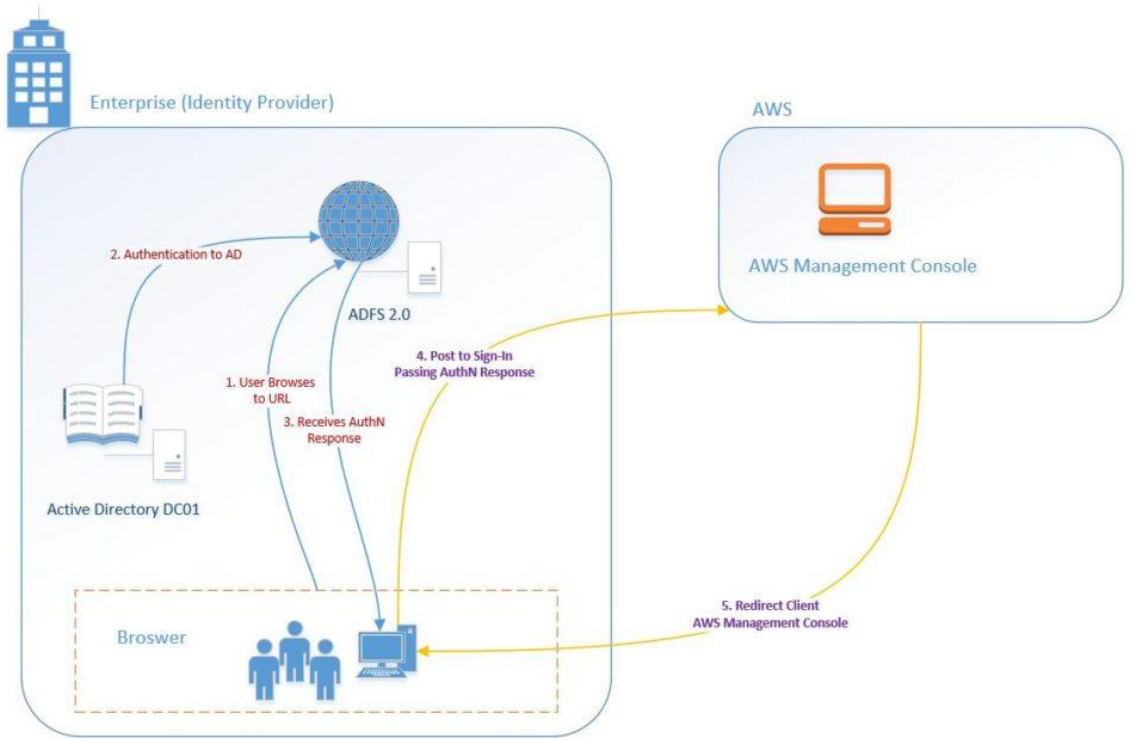
(https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx).

IAMS ACADEMY

IAM Identity Federation with Active Directory

You can use Identity Federation to login onto your AWS Management Console. Key stages involved in enabling SAML 2.0 Federated Users to access the AWS Management Console are:

- You start the sign in process when a user visits the ADFS constructed website (https://*Fully.Qualified.Domain.Name.Here*/adfs/ls/IdpInitiatedSignOn aspx) inside your domain
- This sign in page authenticates the user to the local Corporate Active Directory. The user may be prompted to re-enter his credentials depending on his browser
- The browser will then receive a SAML assertion in the form of an authenticated response from ADFS
- The browser will then post the SAML assertion to the AWS sign-in endpoint (https://signin.aws.amazon.com/saml). The sign-in process uses the **AssumeRoleWithSAML** API to request temporary security credentials and then constructs a sign-in URL for the AWS Management Console.
- The browser then receives the sign-in URL and is redirected to the console.



Exam Tips

- IAM does not apply to specific Regions or Availability Zones – Its affects are universal across your account
- Root Account will have complete administrator access in the AWS Account by default
  - Do not use Root Account for day to day operations
- New Users by default do not have any access and you have to specifically grant them access
  - Always implement the principal of least privileges when you grant access to IAM users
- New Users will have an Access Key ID and Secret Access Key when you first create it. You **must** download and keep these in a safe place as they are only displayed once at the time of user creation. These key are required if you wish to programmatically access services and resources
- It is strongly recommended to create Multifactor Authentication for your root account
- Password Policies can be created to enforce password complexity
- IAM is a free service

Where possible use IAM Roles for programmatic access instead of Access Keys IDs and Secret Access Keys