sts security token services

AWS STS – Security Token Service

- Allows to grant limited and temporary access to AWS resources.
- Token is valid for up to one hour (must be refreshed)
- Cross Account Access
  - Allows users from one AWS account access resources in another
- Federation (Active Directory)
  - Provides a non-AWS user with temporary AWS access by linking users Active Directory credentials
  - Uses SAML (Security Assertion markup language)
  - Allows Single Sign On (SSO) which enables users to log in to AWS console without assigning IAM credentials
- Federation with third party providers / Cognito
  - Used mainly in web and mobile applications
  - Makes use of Facebook/Google/Amazon etc to federate them

Cross Account Access

- Define an IAM Role for another account to access
- Define which accounts can access this IAM Role
- Use AWS STS (Security Token Service) to retrieve credentials and impersonate the IAM Role you have access to (AssumeRole API)
- Temporary credentials can be valid between 15 minutes to 1 hour