AWS STS - Security Token Service

If you are studying for AWS Developer Associate Exam, this guide will help you with quick revision before the exam. it can use as study notes for your preparation.

Dashboard Other Certification Notes

AWS STS - Security Token Service

- Allows to grant limited and temporary access to AWS resources (up to 1 hour)
- STS APIs:
  - **AssumeRole**: assume roles within our account or cross account
  - **AssumeRoleWithSAML**: return credentials for user logged in with SAML
  - **AssumeRoleWithWebIdentity**: return credentials for user logged in with an identity provider (Facebook, Google, other OIDC compatible)
    - Deprecated: we should use Cognito Identity Pool instead
  - **GetSessionToken**: used for MFA login with an user or AWS root account
  - **GetFederationToke**: obtain temporary token for federated user
  - **GetCallerIdentity**: returns details about the IAM user or role used in the API call
  - **DecodeAuthorizationMessage**: decode error message when an AWS API is denied

Using STS to Assume a Role

- We should define an IAM Role within our account or in another account in case of cross-account STS
- Define which principals can access this IAM Role
- Use STS API to retrieve credentials and impersonate the IAM Role we want to access (*AssumeRole*)
- Temporary credentials can be valid between 15 minutes to 1 hour

STS with MFA

- We use the **GetSessionToken** API from STS to get a session a token
- We need an appropriate IAM policy using IAM conditions
- In the IAM policy we need to add **aws:MultiFactorAuthPresent:true** condition
- *GetSessionToken* returns:
  - Access ID
  - Secret Key
  - Session Token
  - Expiration Date