Cognito

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

Cognito

- Used to give access for users/clients to be able to interact with our applications.
- **Cognito User Pools**:
  - Sign in functionality
  - Integrates with API Gateway and Application Load Balancer
- **Cognito Identity Pools (Federated Identity)**:
  - Provides AWS credentials to users to access AWS resources directly
  - Integrates with Cognito User Pools as an identity provider
- **Cognito Sync**:
  - Synchronize data from devices to Cognito
  - Deprecated: use AppSync
- **Cognito vs IAM**: external user vs internal users

Cognito User Pools (CUP)

- Serverless database for web and mobile applications
- Users can do:
  - Simple login: username/password combination
  - Password reset
  - Email/Phone verification
  - Multi-factor auth (MFA)
  - Federated Identities: users can log in with Facebook, Google, SAML
- User can be blocked if their credential is compromised elsewhere (in case of Federated Identities)
- Login uses JSON Web Token (JWT)
- CUP integrates with API Gateway and ALB

Cognito User Pools - Lambda Triggers

- CUP can invoke Lambda functions synchronously on these triggers:
  - Authentication events:
    - pre auth
    - post auth
    - pre token generation
  - Sign-up
    - pre sign-up
    - post confirmation
    - migrate user
  - Message
    - custom message
  - Toke creation
    - pre token generation

Cognito User Pools - Hosted Authentication UI

- Cognito has a hosted auth UI which can be added to an application to handle sing-up and sign-in workflows
- Using the hosted UI, we can have a foundation for integration with social logins, OIDC or SAML
- We can customize the logo and the CSS of this page

Cognito Identity Pools (Federated Identities)

- Get identities for users to obtain temporary AWS credentials
- The identity pool can include:
  - Public providers (Login with Amazon, Facebook, Google, Apple)

    - Users is an Amazon Cognito pool
    - OpenID Connect Providers and SAML Identity providers
    - Developer authenticated identities (custom login server)
    - Cognito Identity Pools allow for unauthenticated (guest) access
- Users can then access AWS services directly or through API Gateway
    - The IAM policies applied to the credentials are defined in Cognito
    - They can be customized based on the user_id for fine grained control

Cognito Identity Pools - IAM Roles

- We can define default IAM roles for authenticated and guest users
- We can define rules to choose the role for each user based on the userID
- We can partition user access using policy variables
- IAM credentials are obtained by Cognito Identity Pools through STS
- Roles must have a “trust” policy of Cognito Identity Pools

Cognito User Pools vs Identity Pools

User Pools	Identity Pools
Database of users for a web/mobile application	Obtains AWS credentials for the users
Allows to federate logins (Public Social, SAML, etc)	Users can login through Public Social, SAML, CUP
Customize the UI used for auth	User can be guest uses (unauthenticated)
Hast triggers for AWS Lambda during auth flow	Users are mapped to IAM roles/policies
Manage username/password	**Give access to AWS services**

Cognito Sync

- Deprecated - use AppSync instead
- Used to store preferences, configuration, state of app
- Cross device synchronization (any platform - IOS, Android, etc.)
- Offline capability (synchronize when back online)
- Store data in datasets (up to 1MB), up to 20 datasets
- **Push Sync**: silently notify across all devices when identity data changes
- **Cognito Stream**: stream data from Cognito into Kinesis
- **Cognito Events**: execute Lambda function in response to events