Identity management service from AWS

Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps

Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.

two main components of Amazon Cognito are

* user pools - provide sign-up and sign-in options for your app users

 user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito, or federate through a third-party identity provider (IdP). Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.

* identity pools - enable you to grant your users access to other AWS services

Support following identity providers that you can use to authenticate users for identity pools:

* Amazon Cognito user pools
* Social sign-in with Facebook, Google, and Login with Amazon
* OpenID Connect (OIDC) providers
* SAML identity providers
* Developer authenticated identities

See the diagram for a common Amazon Cognito scenario. Here the goal is to authenticate your user, and then grant your user access to another AWS service.

1. In the first step your app user signs in through a user pool and receives user pool tokens after a successful authentication.
2. Next, your app exchanges the user pool tokens for AWS credentials through an identity pool.
3. Finally, your app user can then use those AWS credentials to access other AWS services such as Amazon S3 or DynamoDB.

