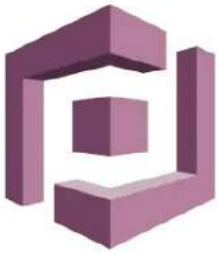
AMAZON COGNITO



AWS Cognito

Amazon Cognito provides sign-up and sign-in options for your app users. and also provides AWS credentials to grant your users access to other AWS services.

Prepared By Shubham

December 2022

What is AWS Cognito?

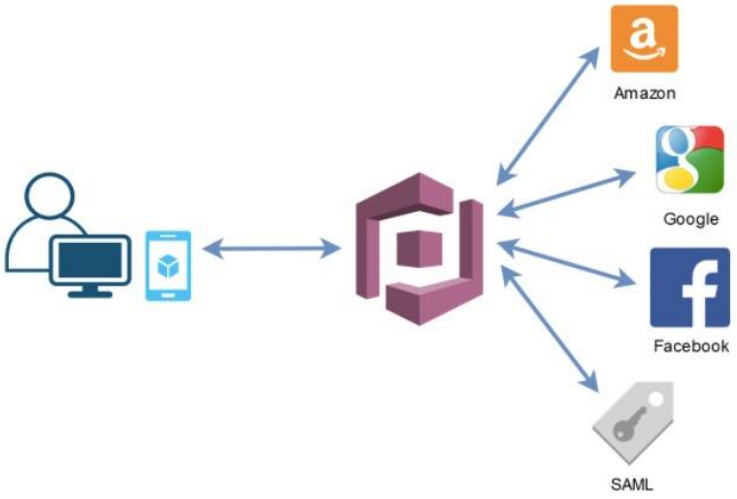
Amazon Cognito lets you easily add user sign-up and authentication to your mobile and web apps. Amazon Cognito also enables you to authenticate users through an external identity provider and provides temporary security credentials to access your app's backend resources in AWS or any service behind Amazon API Gateway.

What is pool in AWS?

A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Google, Facebook, Amazon, or Apple, and through SAML identity providers.

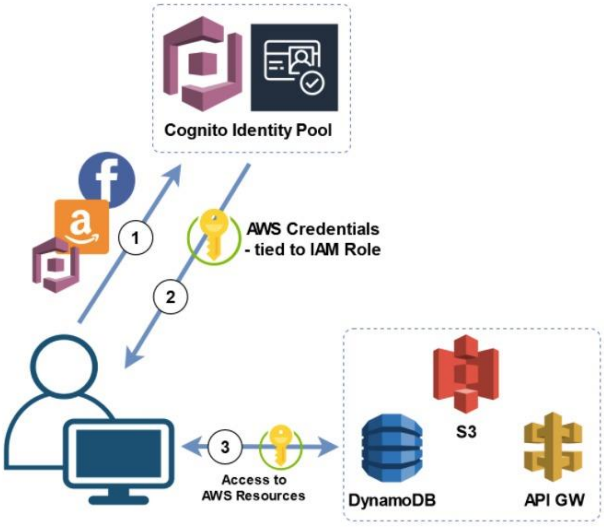
What is AWS User pool?

Amazon Cognito User Pools are used for authentication. To verify your user's identity, you will want to have a way for them to login using username/passwords or federated login using Identity Providers such as Amazon, Facebook, Google, or a SAML supported authentication such as Microsoft Active Directory. You can configure these Identity Providers on Cognito, and it will handle the interactions with these providers so you only have to worry about handling the Authentication tokens on your app. With Cognito User Pools, you can provide sign-up and sign-in functionality for your mobile or web app users. You don't have to build or maintain any server infrastructure on which users will authenticate.



What is AWS Identity pool?

Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.



Short description

User pools are for authentication (identity verification). With a user pool, your app users can sign in through the user pool or federate through a third-party identity provider (IdP). Identity pools are for authorization (access control). You can use identity pools to create unique identities for users and give them access to other AWS services.

What's the difference between user pools and identity pools?

Cognito User Pools	Cognito Identity Pools
Handles the IdP interactions for you	Provides AWS credentials for accessing resources on behalf of users
Provides profiles to manage users	Supports rules to map users to different IAM roles
Provides OpenID Connect and OAuth standard tokens	Free
Priced per monthly active user	

Advanced security features

Cognito has security features that protect your users and their accounts from danger. Cognito can automatically detect unusual sign-in activity, such as sign-in attempts from new locations and devices. It assigns a risk score to the activity and lets you choose to either prompt users for additional verification or straight-up block the sign-in request. It can also notify users of suspicious login attempts. Cognito can also detect credentials that were compromised, prompting users to change their passwords.

Messaging

Cognito can send email messages to verify user email addresses, telling them that they've been invited and notifying them of suspicious sign-in attempts to their accounts. Cognito also sends SMS messages used for Multi-Factor Authentication.

In-built UI

Cognito has an in-built, customizable UI that can be used by users to sign up and sign in. This allows you to quickly develop a basic application or even skip the process of building those elements altogether.

Custom triggers

Cognito allows you to make advanced customization using AWS Lambda functions. For example, you can have your Lambda trigger when a user tries to sign-up to perform some custom validation and accept or deny the sign-up request. More on that later

First section:

Name where you need to enter the name of your user pool in Pool Name. From the first section, you can directly create a user pool with default settings for this you need to click on Review defaults or if you want to go through every step, click on Step through settings. In this tutorial, I will go through Step through settings.

Second section:

Attributes, where you can provide attributes, by using those attributes user will Sign in or sign up.

How do you want your end-users to sign in?

There are two sections 1. Username 2. Email address or Phone number.

1. **Username**

Users can use a username and optionally multiple alternatives to sign up and sign in.

- Sign in with verified email address
- Sign in with verified phone number
- Sign in with preferred username (a username that your users can change).

Here, the meaning of the above is that the user could sign in with username as well as with their email or phone which is provided by user at the sign-up time.

2. **Email address or Phone number**

Users can use an email address or phone number as their “username” to sign up and sign in.

- Email addresses
- Phone numbers
- Both email addresses and phone numbers (users can choose one).

Here mean of above is User could sign in with email or phone number as their username.

Third section:

you can set up different policies like password policy, user can sign up by themselves, etc.

- In What password strength do you want to required?
- In this part, set your password policy according to your requirements.
- In Do you want to allow users to sign themselves up?

If you want only allow admin to add user, then check “Only allow administrators to create users”. Or Allow users to sign up themselves.

In How quickly should temporary password set by administrators expire if not used?

Set no. of days how long until a temporary password set by an administrator expires if the password is not used.

Fourth section:

in this section you can configure MFA, recover of account if user forgot their password, and verification of attributes, and permissions.

- In MFA
- Set Option, if you want to individual users can have MFA enabled.
- Set Require, if you want every user must use MFA.
- In Recover their account

When a user forgets their password, they can have a code sent to their verified email or verified phone to recover their account. Select one option out of five according to your requirement.

In Permission

- Select IAM role to allow send text message.

Fifth section:

this section is regarding messages and text configuration and customization for verification purpose.

- In Do you want to customize your email address
- If you want to send mail from your particular email address for verification mail.
- In Send emails through your Amazon SES Configuration
- If there is need to send mail from SES, enable SES in this part and must add ARN in FROM email address in above section.

In Customize email

You can verify user email through Verification Code or Link, select Code or Link according to your requirement. And you can customize message using HTML tags, but must include {####}.

Sixth section:

add tag as Key and Value to user pool. Sixth section, here you can configure to track and remember user's device. This feature enables developers to remember the devices on which end users sign in to their application. In addition, you can build custom functionality using the notion of remembered devices. For example, with a content distribution application (e.g., video streaming), you can limit the number of devices from which an end user can stream their content. In Do you want to remember your user's devices

There two options:

1. Always

By selecting this option, every device used by your application's users is remembered.

2. Use Opt-In

By selecting this option, your user's device is remembered only if that user opts to remember the device. This configuration option enables your users to decide whether your application should remember the devices they use to sign in, though keep in mind that all devices are tracked regardless.

3. No (default)

- By selecting this option, devices are neither remembered nor tracked.
- Eighth section, this is regarding app client to access user pool.
- In Which app client will have access to this user pool

To create app client, click on Add an app client.

- Enter App client name, according to you require.
- Set Refresh token expiration, Access token expiration, and ID token expiration time as you need. These all tokens mean, Cognito will give token to your application to access aws resources.
- If you use JavaScript SDK with Cognito to authenticate, at that time must uncheck "Generate Client Secret" because JavaScript SDK does not support client secret. Otherwise leave it to default.
- Under Auth Flow Configuration leaves, it to default or Check or Uncheck as your requirement.
- In Security Configuration leave it to default.

To set which attributes of Cognito will be read or write by your application, click on Set attribute read and write permission Check and Uncheck attributes under Readable Attributes and Writeable attributes according to your requirements.

Nine sections:

you can configure some Lambda functions on different events. This is optional. Click on Save Changes to review all configurations of the Amazon Cognito User Pool. On the Review tab click on Create Pool.