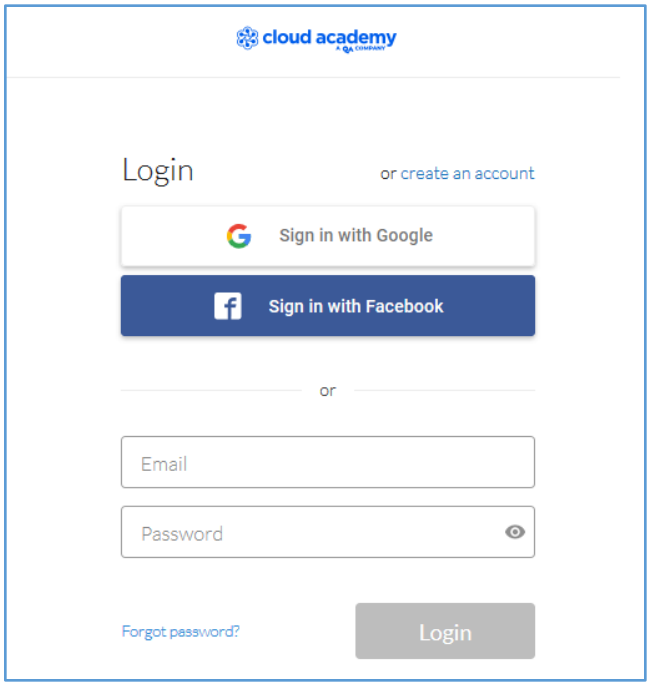
Amazon Cognito

Web applications usually allow a valid username and password combination for successful sign in to the application. Modern authentication flows incorporate more approaches to ensure user authentication. When using AWS, this is no exception, thanks to the abilities and features offered by AWS Cognito. Amazon Cognito service is designed to provide APIs and infrastructure for key features in user management space such as authentication, authorization, and managing user repository with different operations for your web and mobile apps

Modern authentication flows

You might have come across some of the methods as mentioned below

- Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address as part of multi-factor authentication.
- Login challenges are meant to be answering more security questions to prevent access where there is mistrust.
- In some websites, you could sign in through your Google account or Facebook account as well. Cloud academy login page also provides such flexibility in sign in.
- Nowadays once we login to a corporate network we don't need to log in again to access internal applications. We are able to access internal applications without re-login.
- You might have noticed that once you login to any of the google applications such as Gmail, google drive you would be able to access other google applications too without providing user credentials again.



Cloud Academy Login Page

In today's world, we might be wondering how we are going to build essential features with respect to user management, authentication, and authorization in our web applications and mobile applications efficiently. It requires a significant amount of development activities, testing activities, adherence to security compliance standards and exposure to authentication standards.

Amazon Cognito

Payment Gateways

Let me recall how other specific requirements are managed in web applications. For example, many web applications have pages for payment. These payment pages provide flexible options to pay using credit cards, net banking, etc. In a typical web application, they integrate API services from any of the third-party payment gateways to fulfill all requirements in a simple manner.

Payment gateways facilitate payment transactions between customers and banks. These payment gateways also take care of the security of the transactions and adherence to standards such as PCI DSS(Payment Card Industry Data Security Standard). Hence the product teams can focus on core functionalities of their web and mobile applications without putting too much focus on handling payment transactions.

Can we apply the same approach for signup, sign-in, and user management features especially in AWS cloud? Yes. It's a good approach to leverage third-party service provider solutions for authentication as well. Luckily we have got Amazon Cognito to help us to manage things better.

Amazon Cognito

This service allows users to log in directly with their user credentials that are maintained in Amazon Cognito on behalf of of your web and mobile applications. It also allows sign-in through a third party social networking application such as Facebook, Amazon, Google or Apple, and other Identity providers.

Amazon Cognito provides important features to achieve different use cases in user management and authentication in web applications and mobile applications.

Let us have a quick look at Amazon Cognito features before we move on to key components of the AWS Cognito service and overall architecture.

- Managing user directory - Amazon user pools are used as user directories to store user's personal data such as login id, password, etc. This information will be used during sign-in for validation. As this is a cloud service from AWS, We need not worry about managing infrastructure, setup and scaling the service. We could store even millions of user details if required.

- Integrate with social network logins and federated identity providers - Amazon Cognito accepts and allows sign in for users who have an account in social networking sites such as Facebook, Google, PayPal without the need to create a new account in Amazon Cognito. This feature is also available if a user sign-in through an external identity provider(IdP) that is compatible to OpenID Connect and SAML 2.0.

- Standards-based authentication- OpenID Connect, OAuth 2.0, and SAML 2.0.

- Security for your apps and users - HIPAA eligible and PCI DSS, SOC, and ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.

Amazon Cognito

- Simple integration with your app - Amazon Cognito provides software development kit(SDK) for Android, iOS and JavaScript to call APIs that implement user sign-up and sign-in functionality. In addition to providing simple APIs, Amazon Cognito also comes with a default and customizable UI page for user sign-up and sign-in.

- Role based access control for AWS resources - An AWS IAM role has specific permissions to access AWS resources. You could use identity pools to map users to specific roles and authorize their access to AWS resources.

Key components of AWS Cognito
In general, any user management and identity management services are built upon two key functions namely authentication and authorization.

Authentication is the process of validating your claims on identity. For example, You could prove your identity with a passport for security check-in airport.

Authorization is the process to provide confirmation on your access rights to other AWS resources and services. For example, you could show a boarding pass to get into the flight.

User pool and identity pool are two main components in Amazon Cognito. User pools are nothing but a repository where user profile details are kept. When new users signup using your web or mobile applications this user pool will be updated. As a result when users sign-in, their credentials would be authenticated against data in the user pool.

Identity pools simplify authenticated user access to other AWS resources. Identity pool issues temporary AWS credentials to your user's so that they could access other AWS resources without re-entering their credentials. Amazon Cognito is flexible enough to allow usage of user pools and identity pools separately. They can be used together as well.

In the enterprise intranet network, users sign in using user id and password. If the user id and password are validated successfully they can enter the network. This function is called authentication and performed by user pool.

If they want to access some internal services or resources they don’t need to re-enter their login credentials. They will be authorized to use the service based on policies and rules configured. This authorization is enabled by some service that provides either login credentials of the user or issues temporary access tokens to access other servers or resources. This function is called authorization and performed by the identity pool.

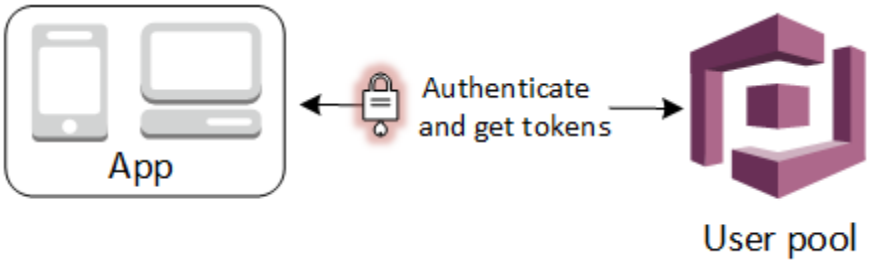
In simple words, the authentication function is performed before the authorization is done. OpenID Connect is one of the references for authentication whereas OAuth 2.0 is one of the references for authorization.

Now we shall see how user pools and identity pools perform authentication and authorization in AWS.

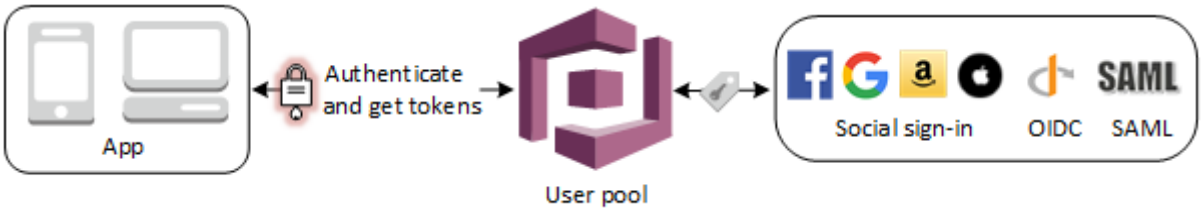
Amazon Cognito

Amazon Cognito user pool overview

A user pool is a user directory in Amazon Cognito. This component takes care of providing authentication to users who sign in through your web or mobile application. Once a user is authenticated, Amazon Cognito returns user pool tokens to your application. It also allows social sign in from Google etc and sign-in with SAML identity providers.

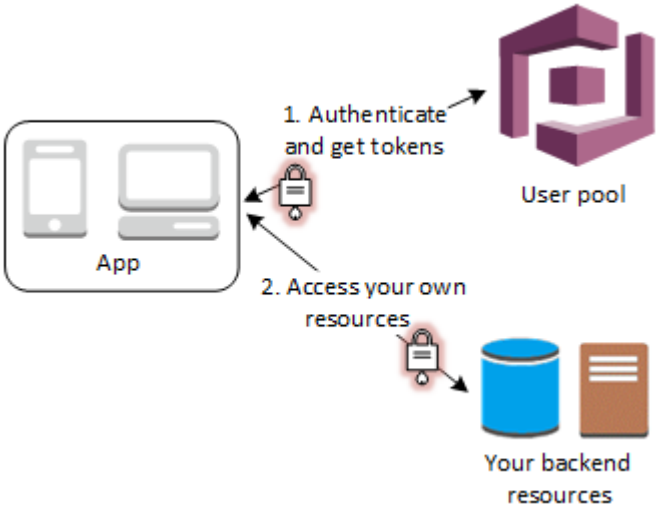


Source: *https://docs.aws.amazon.com/cognito/latest/developerguide/amazon-cognito-user-pools-using-tokens-with-identity-providers.html*



These tokens can be classified into ID token and access token. Your users could perform the following activities by using these tokens.

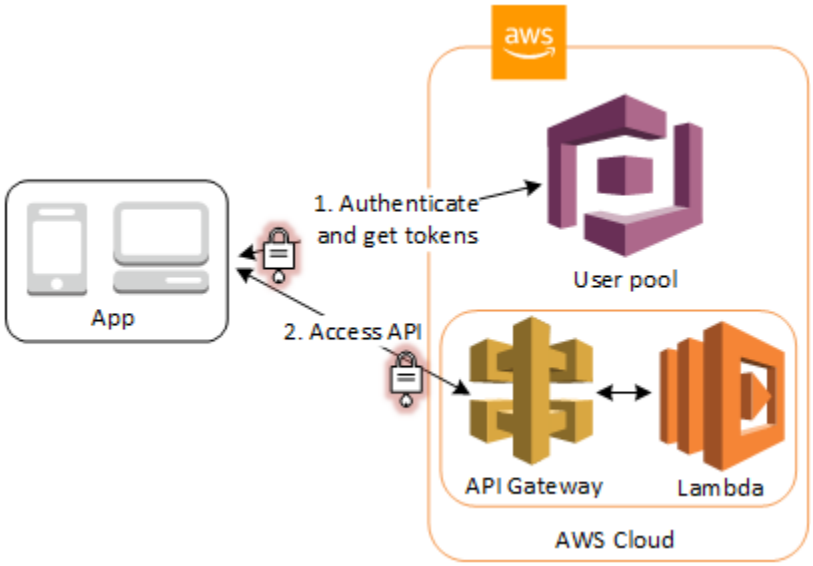
Your client web and mobile applications can access your own server-side components such as a database.



Source: https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-scenarios.html

Amazon Cognito

Your client applications can exchange these tokens for temporary AWS credentials to access other AWS services from the identity pool of Amazon Cognito.



Source: https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-scenarios.html

You could refresh tokens as well as they expire one hour after authentication. We could also revoke these tokens if required.

User pool also provides the following features.

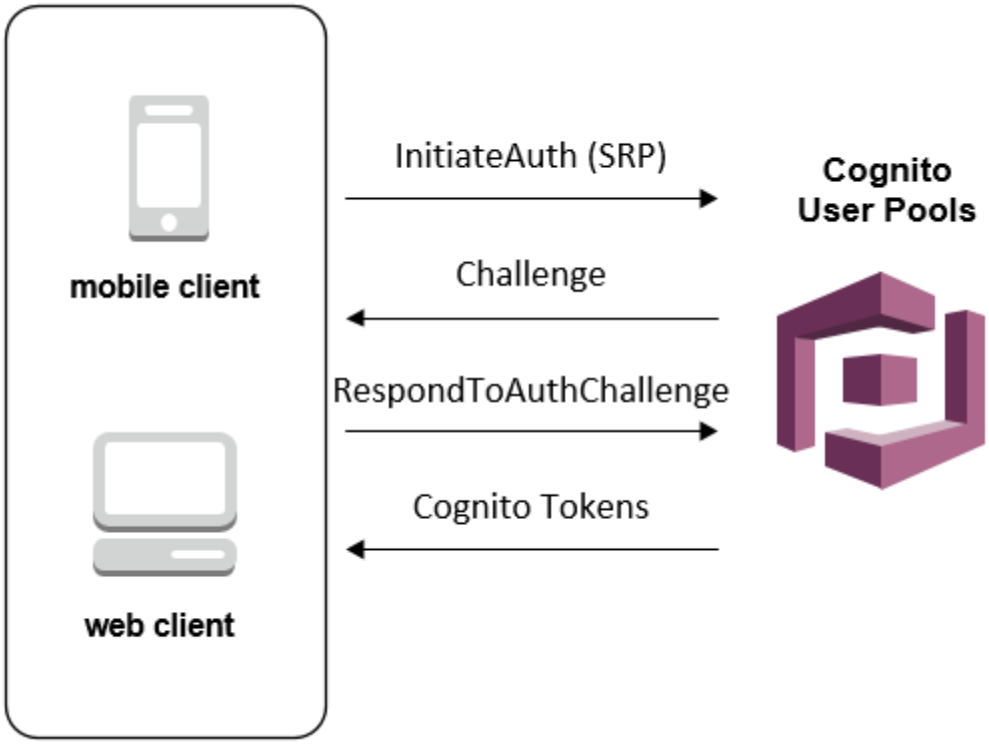
- Import CSV file contents into the user pool where the CSV file contains existing user's credentials.
- User pool comes with sign-up and sign-in features and a ready-made, customizable web UI to sign in users.
- User directory management and user profiles.
- It supports various security features such as multi-factor authentication (MFA) and checks for compromised credentials.
- It provides features such as account takeover protection, and verification through phone and email.
- It helps us to create customized workflows and support user migration through AWS Lambda triggers.

Amazon Cognito

Amazon Cognito API for developers - User pool

If you are from software development background you would be interested to know about user authentication flow.

We could configure different authentication workflows by configuring a set of challenges in the user pool. Based on authentication flow, the user needs to answer further challenges until authentication either fails or the user assigned tokens. There is a sequence of request and response API calls shown below. The following APIs are used: InitiateAuth and RespondToAuthChallenge. RespondToAuthChallenge can be repeated to include different challenges so that we can support any custom authentication flow.



Source: https://docs.aws.amazon.com/cognito/latest/developerguide/amazon-cognito-user-pools-authentication-flow.html

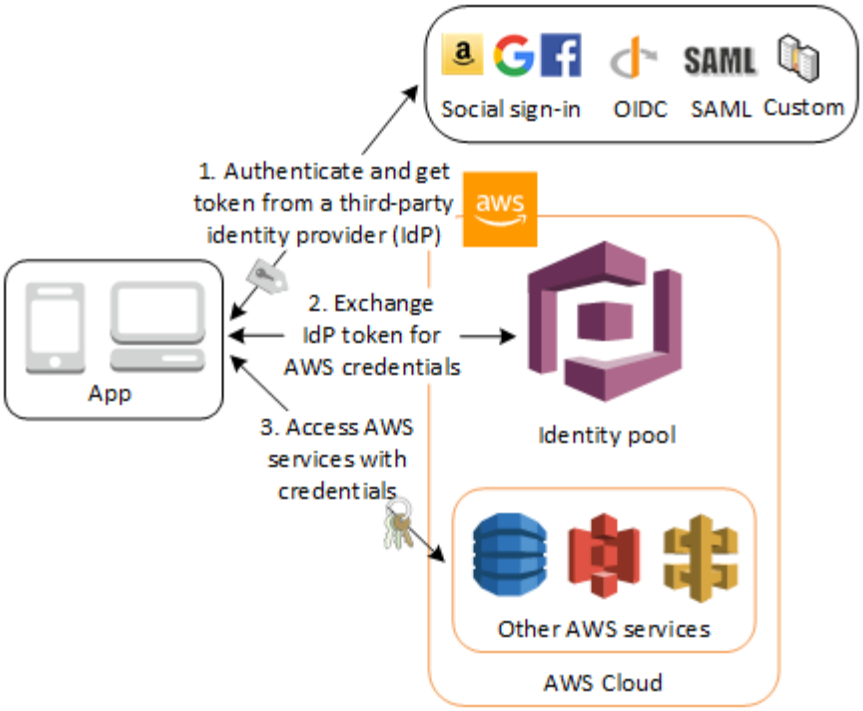
Amazon Cognito

Amazon Cognito Identity pool

Identity pool authorizes users to access other AWS services without further user authentication. Identity pool help to create identities for users and assign permissions for them using IAM roles. Using the Identity pool, users can get access to other AWS services based on their identity information.

An identity pool can include:

- Users from Amazon Cognito user pool
- Users from who can authenticate from external identity providers such as Facebook, Google
- Users authenticated from user own authentication process



Source: https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-scenarios.html

Identity pools also support unauthenticated users such as guest user access as well.

There are only **four steps** in involved with an identity pool.

- Authenticate user from Amazon User pool or external identity providers or your identity provider
- Create an identity for them in Amazon Cognito after authenticating the user
- Get OpenID token from Amazon Cognito
- Get temporary AWS credentials tokens from Amazon Cognito once they share the OpenID token. Using temporary AWS credentials tokens, the user can access any AWS service or resource based on assigned IAM roles for their identities as long as access token is not expired.

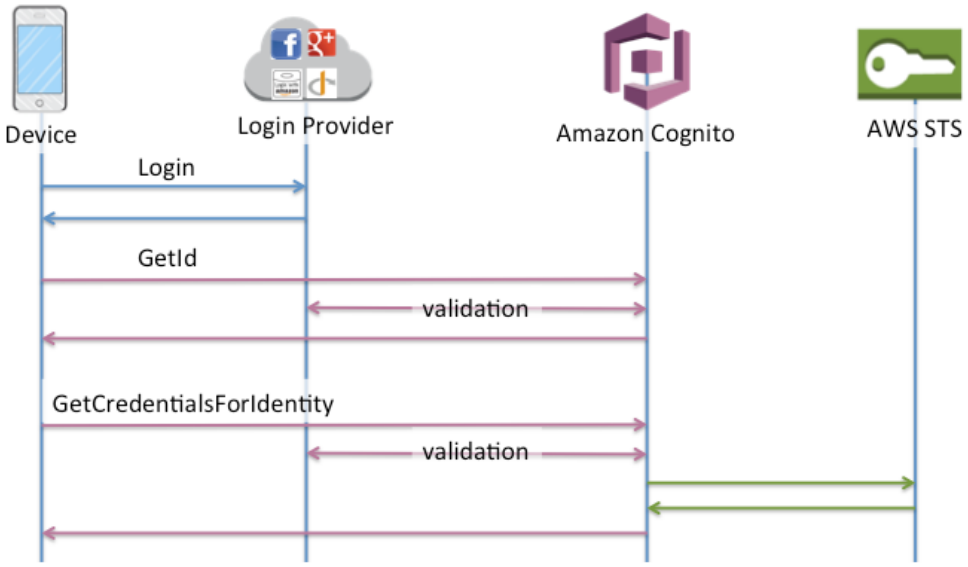
Amazon Cognito API for developers - Identity pool

Amazon Cognito supports multiple flows such as basic flow and enhanced flow. Let us a look at the enhanced flow. In the below diagram, GetId creates an identity in Amazon Cognito.

GetCredntialsForIdentity gets a valid OpenID Connect token and it exchanges this token with AWS STS. By this step, your application gets temporary credentials to access other AWS resources.

Enhanced (Simplified) Authflow

1. `GetId`
2. `GetCredentialsForIdentity`



Source: https://docs.aws.amazon.com/cognito/latest/developerguide/authentication-flow.html

So far we have seen the usage of Amazon Cognito User pool for authentication purposes. Then we saw four steps in Amazon Cognito Identity pool to access other AWS services for authenticated users. We also covered one scenario where both user pool and identity pool used together as part of the authentication workflow.

As a recap, let us list a few scenarios that could use Amazon Cognito.

- Users can be authenticated with a user pool in AWS Cognito
- Users can be authenticated to use server-side resources
- Users are authorized to use resources with API Gateway and Lambda
- Users are allowed to use other AWS resources without re-login by combined usage of user pool and identity pool.
- Integrating support for authentication from third-party Identity providers and social logins.

Amazon Cognito

Here is a list of few more suggested use cases from Amazon Cognito in alignment with what we covered above.

Amazon Cognito User pool use cases

Web and mobile application developers can use a user pool when you need to:

- Embed a default sign-up and sign-in page in your client-side applications
- To avail typical user management features as a proven readily available module
- To monitor trends in usage and reconstruct sign-in request flows from the perspective of security based on the user device, location, and IP address.
- To build a custom authentication flow based on your specific user management requirements.

Amazon Cognito Identity pool use cases

Web and mobile application developers can use an identity pool when you need to:

- Grant permitted access to your authenticated users to access other AWS resources such an Amazon Simple Storage Service (Amazon S3) bucket or an Amazon DynamoDB table.
- Grant temporary default access to guest users who are not authenticated.

Needless to say, it also enables us to give better user experience as mentioned below.

- Reduce password fatigue from maintaining different username and password combinations
- Eliminate time spent re-entering passwords for the same identity
- Lower IT costs due to less number of IT help desk calls about passwords
- Mitigate risk for access to 3rd-party sites where profile data is not managed and stored securely
- Gain better control over your online user credentials and identity
- To speed up Sign Up Process at your favorite web applications and services

I hope you have got an introduction to Amazon Cognito with an overview of major components such as user pool and identity pool with architecture to support various use cases.

It would be very useful to you if you put more effort into this service so that it would give one more useful option to implement user management services in your web or mobile applications, especially in AWS context.

Author: Vijayakumar Athithan

Vijay is an independent technical consultant in the network security R&D domain. He teaches classes on various subjects especially on programming, Linux, cloud, and network security in the capacity of guest faculty at BITS Pilani (India). Prior to that, he gained a decade of experience in different roles in reputed IT service companies across the globe. He has earned the following certifications: SCJP, SCBCD, PMP, ITIL, Exin-Cloud, and CEH.