AWS Cognito

CS516 – Cloud Computing

Computer Science Department

Maharishi International University

Maharishi International University - Fairfield, Iowa

Content

- Amazon Cognito and its benefits
- JWT token
- OAuth, SAML
- Amazon Cognito User pool
- App client
- Cognito Sync

Amazon Cognito

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and enterprise identity providers, such as Microsoft Active Directory.

With Amazon Cognito user pools groups, you can manage your users and their access to resources by mapping IAM roles to groups.

Amazon Benefits

Scalable user directory – Scales to hundreds of millions of users. No server or infrastructure to manage.

Social and enterprise identity federation – Supports identity and access management standards, such as OAuth 2.0, SAML 2.0.

Security for your apps and users – Multi-factor authentication and encryption of data-at-rest and in-transit.

Access control for AWS resources – You can define roles and map users to different roles so your app can access only the resources that are authorized for each user.

Easy integration with your app – With a built-in UI and easy configuration. You can add your branding.

Amazon Cognito user pools

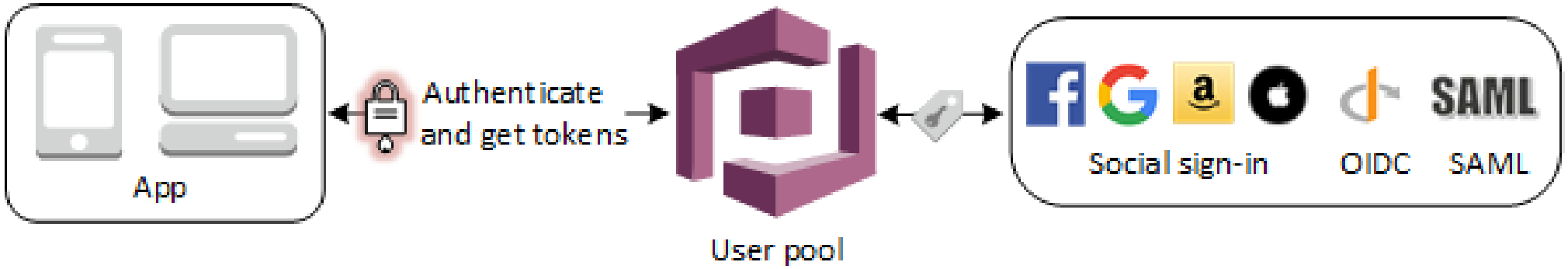
A user pool is a user directory in Amazon Cognito.

User pools provide:

- Sign-up and sign-in services.
- A built-in, customizable web UI to sign in users.
- Social sign-in with Facebook, Google, Amazon, Apple, as well as sign-in with SAML identity providers from your user pool.
- User directory management and user profiles.
- Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
- Customized workflows and user migration through AWS Lambda triggers.

JWT token

After successfully authenticating a user, Amazon Cognito issues JSON web tokens (JWT) that you can use to secure and authorize access to your own APIs, or exchange for AWS credentials.



JWT token

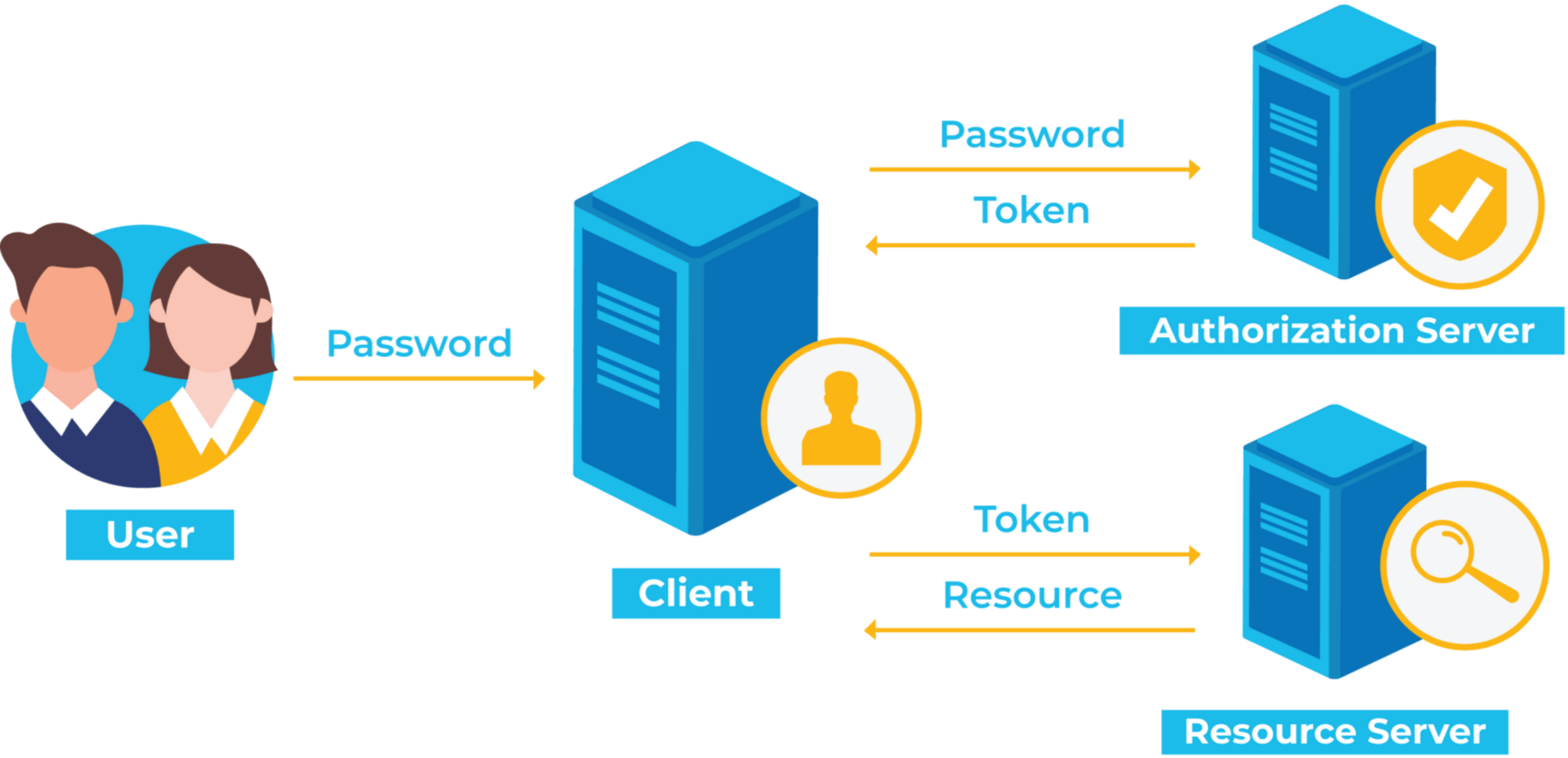
A JWT is a structured security token format used to encode JSON data.

Using a JWT allows the token to be validated locally, without making an HTTP request back to the IdP, thereby increasing your application's performance.

Applications can make use of data inside the token, further reducing expensive HTTP calls and database lookups.

JWT can be stored in a shared caching server so applications can scale out easily as servers don't need to store user session.

Even if the hackers compromised the token, it is temporary.


Password
Token
Authorization Server
Password
User
Client
Token
Resource
Resource Server

JWT token stores user data

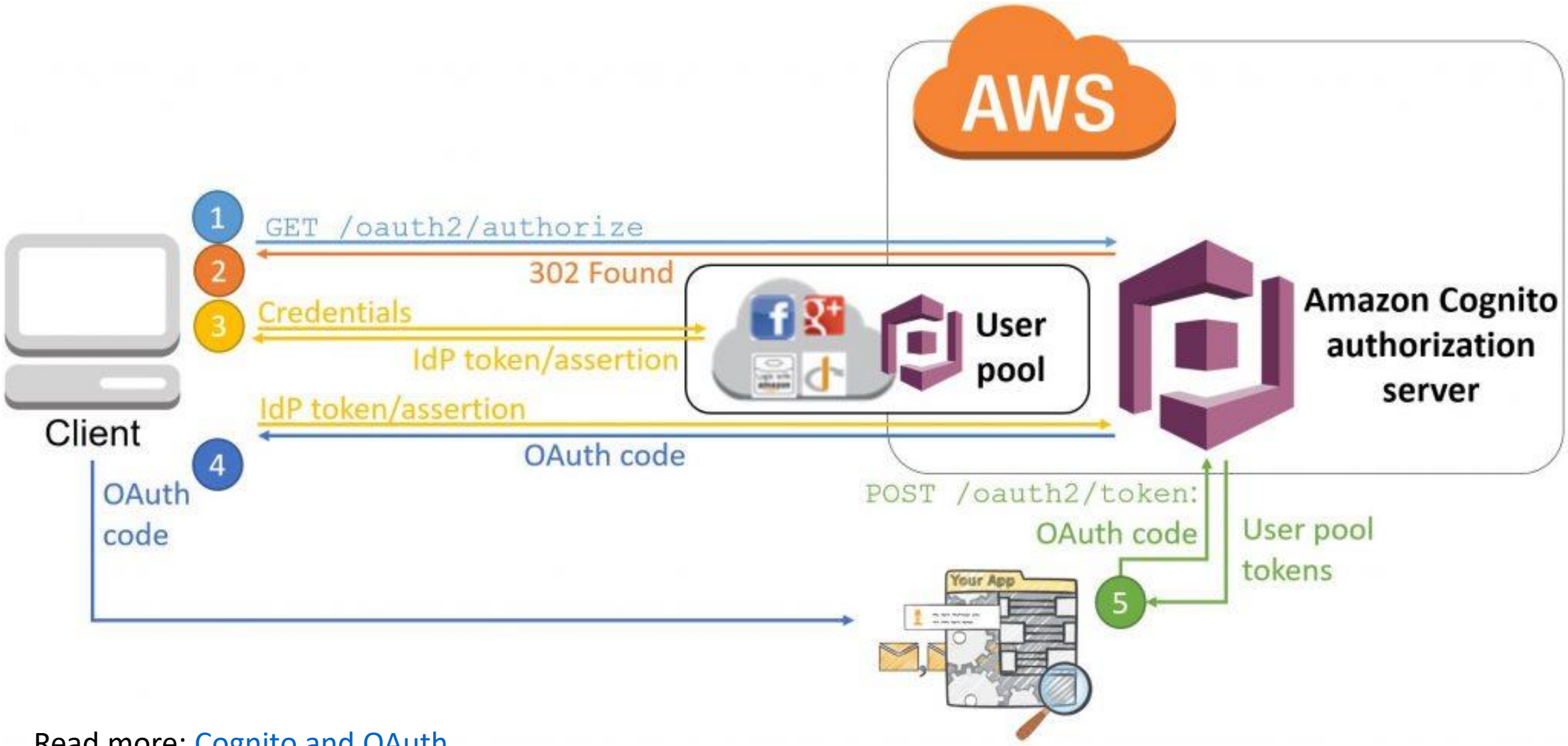

```
{
  "sub": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "device_key": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "cognito:groups": [
    "admin"
  ],
  "token_use": "access",
  "scope": "aws.cognito.signin.user.admin",
  "auth_time": 1562190524,
  "iss": "https://cognito-idp.us-west-2.amazonaws.com/us-west-2_example",
  "exp": 1562194124,
  "iat": 1562190524,
  "jti": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "client_id": "57cbishk4j24pabc1234567890",
  "username": "janedoe@example.com"
}
```

OAuth 2.0

OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.

This mechanism is used by companies such as Amazon, Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third party applications or websites.

Accessing AWS via OAuth



Read more: [Cognito and OAuth]

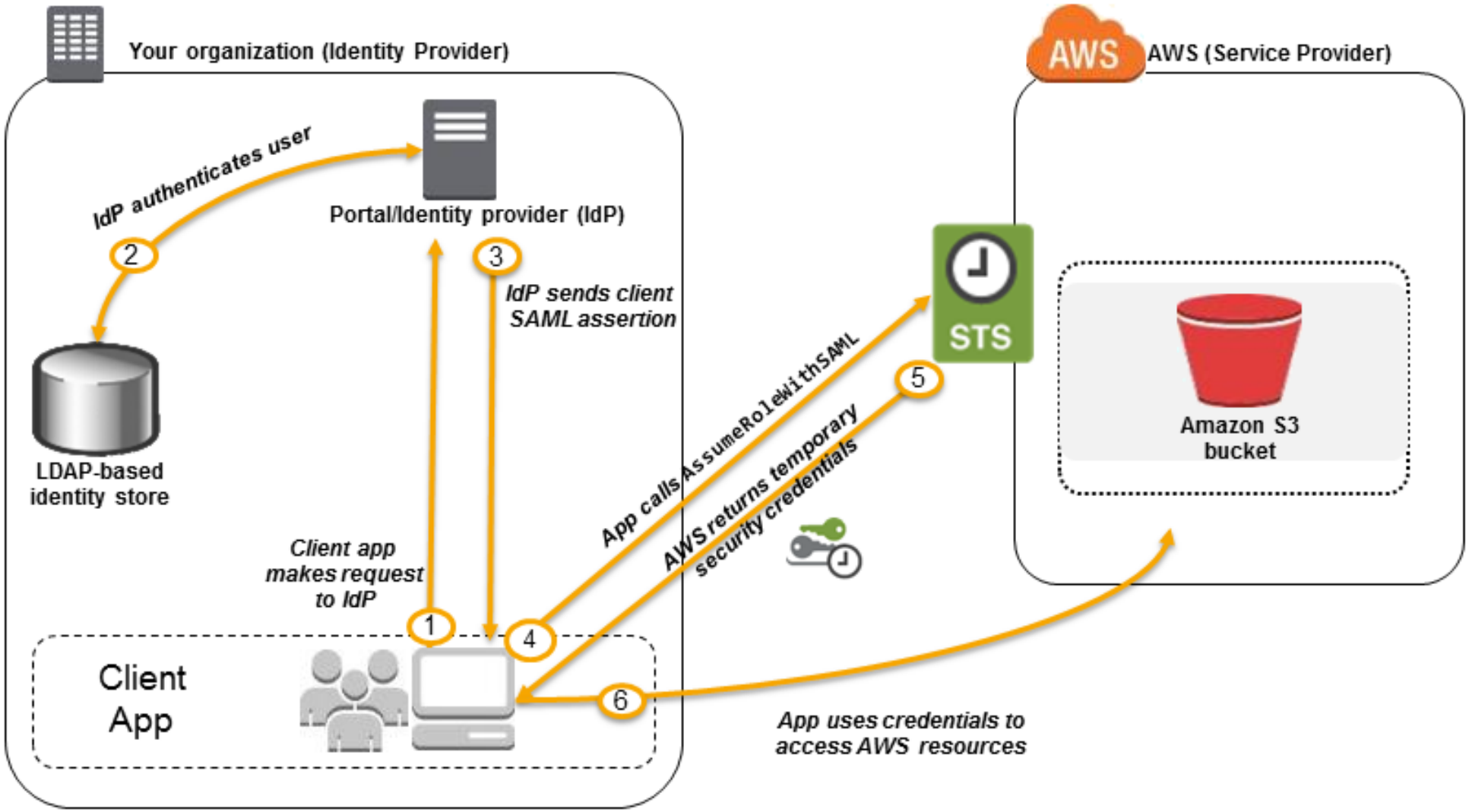
SAML 2.0

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

SAML is an XML-based markup language for **security assertions**. Used commonly for **enterprise users**.

AWS supports identity federation with SAML 2.0 that enables federated single sign-on (**SSO**), so users can log into the AWS Management Console or call the AWS API operations without you having to create an IAM user for everyone in your organization.

Accessing AWS via SAML



User Pool App Client

You can configure an app client for accessing Amazon Cognito from your application through SDK.

You can also generate the **client secret** that is used by only application and authentication server (or another app), not communication between application and user! Never issue a client secret for public front-end apps like React. Instead, use only when authenticating microservice to microservice communication.

User Pool App Client Token types

There are 3 tokens in user pool app client:

- **Refresh token** - Refresh Tokens are credentials used to obtain access tokens
- **ID token** - The ID Token is a security token granted by the OpenID Provider that contains information about an End-User. This information tells your client application that the user **is authenticated**, and can also give you information like their username or locale.
- **Access token (Authorization)** - Access tokens, on the other hand, are not intended to carry information about the user. They simply allow access to certain defined server resources.

App client name

my-app-client

Refresh token expiration

30 days and 0 minutes

Must be between 60 minutes and 3650 days

Access token expiration

0 days and 60 minutes

Must be between 5 minutes and 1 day. Cannot be greater than refresh token expiration

ID token expiration

0 days and 60 minutes

Must be between 5 minutes and 1 day. Cannot be greater than refresh token expiration

☐ Generate client secret

Auth Flows Configuration

☐ Enable username password auth for admin APIs for authentication (ALLOW_ADMIN_USER_PASSWORD_AUTH) Learn more.

☐ Enable lambda trigger based custom authentication (ALLOW_CUSTOM_AUTH) Learn more.

☑ Enable username password based authentication (ALLOW_USER_PASSWORD_AUTH) Learn more.

☑ Enable SRP (secure remote password) protocol based authentication (ALLOW_USER_SRP_AUTH) Learn more.

☑ Enable refresh token based authentication (ALLOW_REFRESH_TOKEN_AUTH) Learn more.

Amazon Cognito Sync

Amazon Cognito Sync is an AWS service and client library that enables cross-device syncing of application-related user data. You can use it to synchronize user profile data across mobile devices and the web without requiring your own backend.

The client libraries cache data locally so your app can read and write data regardless of device connectivity status. When the device is online, you can synchronize data.

Pricing

Pricing Tier (MAUs)	Price per MAU
First 50,000	Free
Next 50,000	$0.00550
Next 900,000	$0.00460
Next 9,000,000	$0.00325
Greater than 10,000,000	$0.00250