Section 21:) Cognito : cognito user pool, cognito identity pool and cognito sync

**Cognito : give an identity tot users to access application outside the cloud (like mobile application)**

Amazon **Cognito** is a simple user identity and data synchronization service that helps you securely manage and synchronize app data for your users across their mobile devices. ... Amazon **Cognito** is available to all AWS customers

Short Description. **User pools** are for authentication (identify 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).

Or

Machine generated alternative text:
Amazon Cognito 
Amazon Cognito offers user pools and identity pools. User pools are user 
directories that provide sign-up and sign-in options for your app users. Identity 
pools provide AWS credentials to grant your users access to other AWS 
services. 
Manage User Pools 
Manage Identity Pools 

Machine generated alternative text:
Amazon Cognito 
• We want to give our users an identity so that they can interact with our 
application. 
• Cognito User Pools: 
• Sign in functionality for app users 
• Integrate with API Gateway & App •on L Balancer 
• Cognito Identity Pools (Federated I 
• Provide AWS credentials to users— _,an cessAWS resources directly 
• Integrate with Cognito User Pools an identity provider 
• Cognito Sync: 
• Synchronize data from device to Cognito. 
• Is deprecated and replaced by AppSync 
• Cognito vs IAM: "hundreds of users", "mobile users", "authenticate with SAML" 

Cognito User Pools (CUP)

When user login or register to any other website

Machine generated alternative text:
Cognito User Pools (CUP) — User Features 
• Create a serverless database of user for your web & mobile apps 
• Simple login: Username (or email) / password combination 
• Password reset 
• Email & Phone Number Verific i 
• Multi-factor authentication (M 
• Federated Identities: users from Facebook, Google, SAML... 
• Feature: block users if their credentials are compromised elsewhere 
• Login sends back a JSON Web Token (J 

**NOTE :**

CUP has own database of users

Machine generated alternative text:
Cognito User Pools (CUP) 
Returns 
JSON Web Token 
JWT 
Diagram 
Social Identity Provider 
OqenlD 
Federation through 
Third Party Identity Provider (IdP) 
Mobile Applications 
login 
Cognito 
Web Applications 
e 
Database of users 

**Integration of CUP with AWS at high level ( two ways given in diagram)**

Machine generated alternative text:
Cognito User Pools (CUP) - Integrations 
• CUP integrates with API Gateway and Application Load Balancer 
Authenticate 
Retrieve token 
REST API + 
Cognito User Pools 
Evaluate Cognito Token 
Cognito User Pools 
e 
Authenticate 
Application Load Balancer 
+ Listeners & Rules 
Target Group 
flnrfnnri 
Pass Token 
backend 
API Gateway 

**Cognito User Pools hands on**

**Cognito :**

**Customer identities management and aws credential for federated identities**

**Step 1)**

**Search cognito click on manage user pools : database of users to login mobile and web application**

Machine generated alternative text:
Amazon Cognito 
Amazon Cognito offers user pools and identity pools. User pools are user 
directories that provide sign-up and sign-in options for your app users. Identity 
pools provide AWS credentials to grant your users access to other AWS 
services. 
Manage User Pools 
Manage Identity Pools 

Machine generated alternative text:
C eu-west-2.console.aws.amazon.com/cognito/users/?region 
Services v 
Jser Pools Federated Identities 
Your User Pools 
zeu-west-2#/? 
kz5qrtvm 
Click here to create a user pool. 
saurabh @ awsdeveloperleam v 
Paused 
London v Support v 
Create a user pool 
You have no user poo 

Machine generated alternative text:
Services v 
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Pool name 
DemoPoo( 
saurabh @ awsdeveloperleam v 
What do you want to name your user pool? 
Give your user pool a descriptive name so you can easily identify it in the future. 
How do you want to create your user pool? 
London v 
Support v 
Cancel 
Review defaults 
Start by reviewing the defaults and then 
customize as desired 
Step through settings 
Step through each setting to make your 
choices 

Machine generated alternative text:
aws 
Name 
Attributes 
Policies 
Services v 
o 
saurabh @ awsdeveloperleam v 
London v 
Support v 
You can't change the sign-in and attribute options on this page after you've created your user pool. Make sure that you've decided on the settings that you want. 
How do you want your end users to sign in? 
You can choose to have users sign in with an email address, phone number, username or preferred username plus their password. Learn more. 
LJsername - Users can use a username and optionally multiple alternatives to sign up and sign in. 
Aso allow sign in with verified email address 
Aso allow sign in with verified phone number 
Aso allow sign in with preferred username (a username that your users can change) 
Email address or phone number - Users can use an email address or phone number as their "username" to sign up and sign in. 
o 
Allow email addresses 
o 
Allow phone numbers 
o 
Allow both email addresses and phone numbers (users can choose one) 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
You can choose to enable case insensitivity on the username input for the selected sign-in option. For example, when this option is selected, the users can sign in using either "username" or 
"Username". 
(Recommended) Enable case insensitivity for username input 
Which standard attributes do you want to require? 
All of the standard attributes can be used for user profiles, but the attributes you select will be required for sign up. You will not be able to change these requirements after the pool is created. If 
you select an attribute to be an alias, users will be able to sign-in using that value or their username. Learn more about attributes. 
Required 
Attribute 
address 
Required Attribute 
nickname 

**Click next**

Machine generated alternative text:
aws 
Attributes 
Policies 
Services v 
Minimum length 
Require numbers 
Require special character 
Require uppercase letters 
Require lowercase letters 
Amazon recommends requiring passwords with at least 8 characters, lowercase, uppercase, and numbers for greater security_ 
Do you want to allow users to sign themselves up? 
You can choose to only allow administrators to create users or allow users to sign themselves up. Learn more_ 
o 
Only allow administrators to create users 
@ Allow users to sign themselves up 
How quickly should temporary passwords set by administrators expire if not used? 
You can choose for how long until a temporary password set by an administrator expires if the password is not used. This includes accounts created by administrators. 
saurabh @ awsdeveloperleam v 
London v 
Support v 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Days to expire 
7 
Back 
Next step 

Machine generated alternative text:
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Cancel 
Do you want to enable Multi-Factor Authentication (MFA)? 
Multi-Factor Authentication (MFA) increases security for your end users. If you choose 'optional', individual users can have MFA enabled. You can only choose 'required' when initially creating a 
user pool, and if you do, all users must use MFA. Phone numbers must be verified if MFA is enabled. You can configure adaptive authentication on the Advanced security tab to require MFA 
based on risk scoring of user sign in attempts. Learn more about multi-factor authentication_ 
Note: separate charges apply for sending text messages. 
@ Off C) Optional C) 
Required 
How will a user be able to 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 You can choose the preferred way to send codes below. We 
recommend not allowing phone to be used for both password resets and multi-factor authentication (MFA). Learn more. 
o 
o 
o 
C) 
o 
Email if available, othewise phone, but don't allow a user to reset their password via phone if they are also using it for MFA 
Phone if available, otherwise email, but don't allow a user to reset their password via phone if they are also using it for MFA 
Email only 
Phone only, but don't allow a user to reset their password via phone if they are also using it for MFA 
(Not Recommended) Phone if available, othewise email, and do allow a user to reset their password via phone if they are also using it for MFA. 
None — users will have to contact an administrator to reset their passwords 
Which attributes do you want to verify? 
Verification requires users to retrieve a code from their email or phone to confirm ownership. Verification of a phone or email is necessary to automatically confirm users and enable recovery from 
forgotten passwords. Learn more about email and phone verification_ 

**Click next**

Machine generated alternative text:
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Cance 
Do you want to customize your email address? 
You can send emails from an SES verified identity. Learn more about SES verified identities and domains. 
SES Region 
US East (Virginia) 
FROM email address ARN 
Default 
You must verify your email address with Amazon SES before you can select it Verify an SES identity_ 
FROM email address 
e.g. John Smith 
REPLY-TO email address 
Do you want to send emails through your Amazon SES Configuration? 
Select Yes if you require higher daily email limits otherwise select No. Learn more about Cognito daily email limits. If you choose Yes, Cognito will send emails through your Amazon SES 

**Click next ( we can do lot of things with cognito)**

Machine generated alternative text:
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Do you want to add tags for this user pool? 
You can create new tags by entering tag keys and tag values below 
Add tag 
Back 
Next step 

Machine generated alternative text:
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Do you want to remember your user's devices? 
Always 
User Opt In 
No 
Next step 
Back 

Machine generated alternative text:
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Which app clients will have access to this user pool? 
The app clients that you add below will be given a unique ID and an optional secret key to access this user pool. 
Add an app client 
Back 
Next step 

**Click on cancel**

Machine generated alternative text:
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Cancel 
Do you want to customize workflows with triggers? 
You can make advanced customizations with AWS Lambda functions. Pick AWS Lambda functions to trigger with different events if you want to customize workflows and the user experience. 
Visit the AWS Lambda console to create your functions before selecting them below Learn more about triggers. 
Pre sign-up 
This trigger is invoked when a user submits their information to sign up, allowing 
you to perform custom validation to accept or deny the sign up request 
Lambda function 
none 
Custom message 
This trigger is invoked before a verification or MFA message is sent, allowing you to 
customize the message dynamically. Note that static custom messages can be 
edited on the Verifications panel. 
Lambda function 
none 
Pre authentication 
This trigger is invoked when a user submits their information to be authenticated, 
allowing you to perform custom validations to accept or deny the Sign In request 
Lambda function 
none 
Post authentication 
This trigger is invoked after a user is authenticated, allowing you to add custom 
logic, for example for analytics. 
Lambda function 
none 

**=================================================================**

Machine generated alternative text:
User Pools Federated Identities 
Create a user pool 
Name 
Attributes 
Policies 
MFA and verifications 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Review 
Pool name 
DemoPoo( 
Cancel 
What do you want to name your user pool? 
Give your user pool a descriptive name so you can easily identify it in the future. 
How do you want to create your user pool? 
Review defaults 
Start by reviewing the defaults and then 
customize as desired 
Step through settings 
Step through each setting to make your 
choices 

**Userpool created successfully**

Machine generated alternative text:
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
Pool Id 
Pool ARN 
Estimated number of users 
Required attributes 
Alias attributes 
LJsername attributes 
Enable case insensitivity? 
Custom attributes 
Minimum password length 
Password policy 
User sign ups allowed? 
Your user pool was created successfully. 
eu-west-2 7NBXJ2hKp 
arn:aws:cognito-idp:eu-west-2:398678778168:userpool/eu-west-2 7NBXJ2hKp 
email 
none 
none 
Yes 
Choose custom attributes. 
8 
uppercase letters; lowercase letters, special characters, numbers 
Users can sign themselves up 
Delete pool 

**Click on app client**

Machine generated alternative text:
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devi 
p clients 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
Pool Id 
Pool ARN 
Estimated number of users 
Required attributes 
Alias attributes 
LJsername attributes 
Enable case insensitivity? 
Custom attributes 
Minimum password length 
Password policy 
User sign ups allowed? 
Your user pool was created successfully. 
eu-west-2 7NBXJ2hKp 
arn:aws:cognito-idp:eu-west-2:398678778168:userpool/eu-west-2 7NBXJ2hKp 
email 
none 
none 
Yes 
Choose custom attributes. 
8 
uppercase letters; lowercase letters, special characters, numbers 
Users can sign themselves up 
Delete pool 

Machine generated alternative text:
Services v 
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
saurabh @ awsdeveloperleam v 
London v 
Support v 
Which app clients will have access to this user pool? 
The app clients that you add below will be given a unique ID and an optional secret key to access this user pool. 
Add an app client 
Return to pool details 

Machine generated alternative text:
General settings 
Users and groups 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Identity providers 
Attribute mapping 
Which app clients will have access to this user pool? 
The app clients that you add below will be given a unique ID and an optonal secret key to access this user pool. 
App client name 
OemcAppCIi 
Refresh token expiration 
days and O 
Must be bet".een SO minutes and 3650 d&ys 
Access token expiration 
days and 60 
Must be bet".een 5 minutes and I CEnmt be greater th&n refresh token expiÆfion 
ID token expiration 
days and 60 
Must be bet".een 5 minutes and I CEnmt be greater th&n refresh token expiÆfion 
Generate client secret 
Auth Flows Configuration 
Enable username password auth for admin APIs for authentication (ALLOW ADMIN USER PASSWORD_ALITH) 
Enable lambda trigger based custom authenticaton (ALLOW CUSTOM AUTH) Learn more. 
Enable username password based authentication (ALLOW USER PASSWORO_ALJTH) Learn more. 
Enable SRP (secure remote password) protocol based authentication (ALLOW USER SRP AUTH) Learn more. 
Enable refresh token based authentcation (ALLOW REFRESH TOKEN AUTH) Leam more. 
Prevent User Existence Errors Leam more. 
C) Legacy 
@ Enabled (Recommended) 
Set attribute read and write permissions 
CreaÉ dient 
Leam more. 

**Click on app client settings**

Machine generated alternative text:
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App inte ration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
Which app clients will have access to this user pool? 
The app clients that you add below will be given a unique ID and an optional secret key to access this user pool. 
DemoAppClient 
App client id 
30a8r4pq46ngmh9igv40pnOhm9 
Show Details 
Add another app client 
Return to pool details 

**Click on domain name**

Machine generated alternative text:
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
cli 
ettings 
oman name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
Enabled Identity Providers 
Cognito User Pool 
Sign in and sign out URLs 
pp c •en emo pp len 
ID 30a8r4pq46ngmh9i9v40pnOhm9 
Select all 
Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL. 
Callback URL(s) 
https://courses.datacumulus.com/ 
Sign out URL(s) 
OAuth 2.0 
Select the OAuth flows and scopes enabled for this app. Learn more about flows and scopes. 
Allowed OAuth Flows 
Authorization code grant Implicit grant Client credentials 
profile 
Allowed OAuth Scopes 
phone email openid 
Hosted UI 
The hosted UI provides an OAuth 20 authorization server with built-in webpages that can be used to sign up and sign in users using the domain you created. Learn more about the 

Machine generated alternative text:
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
What domain would you like to use? 
Type a domain prefix to use for the sign-up and sign-in pages that are hosted by Amazon Cognito. The prefix must be unique across the selected AWS Regiom Domain names can only contain 
lower-case letters, numbers, and hyphens. Learn more about domain prefixes_ 
This domain is available. 
Amazon Cognito domain 
Prefixed domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes. 
Check availability 
Domain prefix 
https:// sausausau 
Your own domain 
.auth.eu-west-2.amazoncognito.com 
This domain name needs to have an associated certificate in AWS Certificate Manager You also need the ability to add an alias record to the domain's hosted zone after it's 
associated With this user pool. Learn more about using your own domain. 
Use your domain 
Cancel 
Save changes 

**This is the domain I can use to connect with cognito**

Machine generated alternative text:
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
What domain would you like to use? 
Type a domain prefix to use for the sign-up and sign-in pages that are hosted by Amazon Cognito. The prefix must be unique across the selected AWS Regiom Domain names can only contain 
lower-case letters, numbers, and hyphens. Learn more about domain prefixes_ 
This domain is available. 
Amazon Cognito domain 
Prefixed domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes. 
Do 
prefix 
.auth.eu-west-2.amazoncognito.com 
https:// sausausau 
Your own domain 
Check availability 
This domain name needs to have an associated certificate in AWS Certificate Manager You also need the ability to add an alias record to the domain's hosted zone after it's 
associated With this user pool. Learn more about using your own domain. 
Use your domain 
Cancel 
Save changes 

**Click on app client setting**

Machine generated alternative text:
aws 
Services v 
Sign in and sign out URLs 
Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL. 
Callback URL(s) 
https://courses.datacumulus.com/ 
Sign out URL(s) 
OAuth 2.0 
Select the OAuth flows and scopes enabled for this app. Learn more about flows and scopes. 
Allowed OAuth Flows 
Authorization code grant Implicit grant Client credentials 
saurabh @ awsdeveloperleam v 
London v 
Support v 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
profile 
Allowed OAuth Scopes 
phone email openid 
Hosted UI 
The hosted UI provides an OAuth 20 authorization server with built-in webpages that can be used to sign up and sign in users using the domain you created. Learn more about the 
hosted UI 
Launch Hosted UI 

**Click on launch hosted ui**

**Cognito will give login page**

Machine generated alternative text:
sausausau.auth.eu-west-2.amazoncognito.com/login?client 
Sign in with your username and password 
Username 
Username 
Password 
Password 
Forgot your password? 
Sign in 
Need an account? Sign up 
Paused 

Machine generated alternative text:
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
What customizations do you want to make to the end-user experience? 
You can customize the experience to match each of your app's style and branding. If no customizations are made, all default values will be used. Learn more about UI customization_ 
App client to customize 
Defaults for all clients without individual settings 
Logo (optional) 
beach.jpg 
Up to 100 KB in size. 
CSS customizations (optional) 
Labels 
Customize_._ 
Input fields Customize_._ 
Text descriptions 
Customize_._ 
Error messages 
Customize... 
Identity provider buttons 
Customize... 
Identity provider descriptions 
Customize... 

Machine generated alternative text:
Sign in with your username and password 
Username 
Username 
Password 
Password 
Forgot your password? 
Sign in 
Need an account? Sign up 

Machine generated alternative text:
Sign up with a new account 
Username 
saurabh 
Email 
saurabhkesarwani@mailinator.com 
Password 
v' Password must contain a lower case letter 
v' Password must contain an upper case letter 
v' Password must contain a special character 
v' Password must contain a number 
v' Password must contain at least 8 characters 
Sign up 
Already have an account? Sign in 

Machine generated alternative text:
We have sent a code by email to s***@m***.com 
Enter it below to confirm your account. 
Verification Code • 
Confirm Account 
Didn't receive a code? Resend it 

**Now in website means login was successful**

Machine generated alternative text:
C courses.datacumulus.com/?codezabfe38dd-6ceb-4fd6-bdf0-a6a612a90e3c 
AWS Courses 
Kafka Courses 
Data Engineering & API Courses 
Paused 
ailing Li 
Dat'CumuIus 
AWS Certifications 
Trusted by 500,000+ 
pro essionals 
Becdme at e Data & loud ngineer thanks o our courses. You will not be 
disappointe . a 
omes with a 30 days money back guarantee. 

**Click on users and group we will get one user found**

Machine generated alternative text:
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
LJsers 
Groups 
Create user 
User name 
Search for value. 
Phone number verified 
Import users 
LJsername 
saurabh 1987 
saurabh 
Enabled 
Enabled 
Enabled 
Account status 
CONFIRMED 
UNCONFIRMED 
Email verified 
true 
false 
Updated 
Oct 19, 2020 AM 
Oct 19, 2020 AM 
Created 
Oct 19, 2020 AM 
Oct 19, 2020 AM 

**Now all the user details will be here**

**User can sign up or we can define user or we can group user**

**Database of user**

Machine generated alternative text:
user Pools 
DemoPool 
Geneal settings 
Import 
MFA veificatbns 
Advanced sæurity 
Mes—e 
stepYw•e 
App dientS 
App client settings 
Domain name 
COFIRMED 
May 8.2020 PM 
May 8.2020 PM 

**We can set up identity provider**

Machine generated alternative text:
User Pools Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
UI customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
Do you want to allow users to sign in through external federated identity providers? 
Select and configure the external identity providers you want to enable. You will also need to choose which identity providers to enable for each app on the Apps settings tab under App 
integration. Learn more about identity federation With Cognito User Pools. 
O 
Login with Amazon 
O 
Sign in with Apple 
Configure attribute mapping 
O 
Facebook 
O 
SAML 
Go to summary 
O 
Google 
OpenlD Connect 

**Note :**

**Whenever user login or sign up these are the events happening in user pool and we may want**

**To invoke lambda function to react to these events**

**We can set up lambda function with these events**

Machine generated alternative text:
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
p integration 
App client settings 
Domain name 
Lil customization 
Resource servers 
ederation 
Identity providers 
Attribute mapping 
Pre sign-up 
This trigger is invoked when a user submits their information to sign up, allowing 
you to perform custom validation to accept or deny the sign up request 
Lambda function 
none 
Custom message 
This trigger is invoked before a verification or MFA message is sent, allowing you to 
customize the message dynamically. Note that static custom messages can be 
edited on the Verifications panel. 
Lambda function 
none 
Post confirmation 
This trigger is invoked after a user is confirmed, allowing you to send custom 
messages or to add custom logic, tor example tor analytics. 
Lambda function 
none 
Create Auth Challenge 
This trigger is invoked after 'Define Auth Challenge' if a custom challenge has been 
specified as pan ot the 'Define Auth Challenge' trigger. 
Lambda function 
Pre authentication 
This trigger is invoked when a user submits their information to be authenticated, 
allowing you to perform custom validations to accept or deny the Sign in request. 
Lambda function 
none 
Post authentication 
This trigger is invoked after a user is authenticated, allowing you to add custom 
logic, tor example tor analytics. 
Lambda function 
none 
Define Auth Challenge 
This trigger is invoked to initiate the custom authentication flow. 
Lambda function 
none 
Verify Auth Challenge Response 
This trigger is invoked to verity if the response from the end user tor a custom 
authentication challenge is valid or not. 
Lambda function 
none 

**Note : we can use lambda function with cognito user pools**

**Cognito Users pools (others)**

Machine generated alternative text:
Cognito User Pools — Lambda Triggers 
• CUP can invoke a Lambda function synchronously on these triggers: 
user Pool Flow 
Authentication 
Events 
Sign-Up 
Messages 
Token Creation 
Operation 
Pre Authentication Lambda Trigger 
Post Authentication Lambda Trigger 
Pre Token Generation Lambda Trigger 
Pre Sign-up Lambda Trigger 
Post Confirmation Lambda Trigger 
Migrate Vser Lambda Trigger 
Custom Message Lambda Trigger 
Pre Token Generation Lambda Trigger 
Description 
Custom validation to accept or deny the sign-in request 
Event logging for custom analytics 
Augment or suppress token claims 
Custom validation to accept or deny the sign-up 
request 
Custom welcome messages Or event logging for 
custom analytics 
Migrate a user from an existing user directory to user 
pools 
Advanced customization and localization of messages 
Add or remove attributes in Id tokens 

Machine generated alternative text:
Cognito User Pools 
• Cognito has a hosted 
authentication UI that you can 
add to your app to handle sign- 
up and sign-in workflows 
• Using the hosted UI, you have a 
foundation for integration with 
social logins, OIDC or SAML 
• Can customize with a custom 
logo and custom CSS 
Hosted Authentication UI 
CUSTOM 
LOGO 

**Cognito identity Pools**

**Outside users want access to aws environment ( ex dynamodb table or s3)**

**We don’t provide IAM to these users because so many are there and we cant trust them so we allow to access aws through cognito user pool**

Machine generated alternative text:
Cognito Identity Pools (Federated Identities) 
• Get identities for "users" so they obtain temporary AWS credentials 
• Your identity pool (e.g identity source) can include: 
• Public Providers (Login with Amazon Facebook Google, Apple) 
• Users in an Amazon Cognito uset%ool 
• OpenlD Connect Providers & M Providers 
• Developer Authenticated Iden •esl a—co login server) 
• Cognito Identity Pools allow fohgpauthenticated (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 

**AWS Security Token Service** (**AWS STS**) is a web service that enables you to request temporary, limited-privilege credentials for **AWS** Identity and Access Management (IAM) users or for users that you authenticate (federated users).

Machine generated alternative text:
agram 
Cogni 
Web & Mobile 
Applications 
Direct access to AWS 
Private S3 Bucket 
O Stephane Maarek 
I entity ools 
Login and Get Token 
Exchange token Cognito Identity Pools 
Social Identity Provider 
OR?QID 
Cognito 
User Pools 
for temporary 
AWS credentials 
DynamoDB Table 
va da 
STS 
Get temp creds 

Machine generated alternative text:
Web & Mobile 
Applications 
Direct access to AWS 
Private S3 Bucket 
O Stephane Maarek 
Cognito Identity Pools 
Login and Get Token 
Diagram with CUP 
Cognito 
User Pools 
Internal DB 
of users 
Exchange token 
for temporary 
AWS credentials 
DynamoDB Table 
Cognito 
Identity Pools 
validate 
e 
Get temp creds STS 

Machine generated alternative text:
Cognito Identity Pools — IAM Roles 
• Default IAM roles for authenticated and guest users 
• Define rules to choose the role for each user based on the user's ID 
• You can partition your users' accessusi g policy variables 
• IAM credentials are obtained oghlt Identity Pools through STS 
• The roles must have a "trust" po icy-of Cognito Identity Pools 

Machine generated alternative text:
Cognito Identity Pools 
"Version 
"2ø12-1ø-17", 
"Statement" : 
" Action" : 
"s3:GetO jec 
" Effect 
"Resource" : 
"arn:aws:s3::. 
Guest User example 
cket/assets/my_picture. jpg" 

Machine generated alternative text:
Cognito Identity Pools 
"Version 
"2M2-1ø-17", 
"Statement": 
l"s3: ListBucket") , 
"Action": 
Effect" : 
"Al low" , 
"Resource": : , 
"Condition": ("StringLike•• : 
"Action" : 
s3:GetObj , 
PutObj 
Effect" : 
" Al low" , 
"Resource": : :mybucket 
Policy variable on 

Machine generated alternative text:
Cognito Identity Pools 
"Version"; "2Ø12-1ø-17", 
"Statement": I 
"Effect": "AUO•.••, 
"Action": I 
DynamoDB 
"dynandb:Query" , 
"dynamodb:putlte•", "dynZOdb:UpdateIten", , 
"dynamodb : Ba t chWr ite I t—" 
"Resource": t 
"arn : aWS : dynanodb : 123456789ø12 : tab lefHyTab ten 
"Condition": 
"ForAUVa1ues:stri E 
: Le IngKeyS . 
"Slcognito—identity. anazonaws. co': sub) " 
O Stephane Maarek 

**Cognito Identity pool hands on**

**Step1 )**

**Click on federated identities**

Machine generated alternative text:
aws 
User Pool 
Your 
se 
Federated Identities 
r Pools 
DemoPool 
saurabh @ awsdevelopertearn v 
London v Support v 
Create a user pool 

**Take demo pool id and appi id and paste in federated identities**

Machine generated alternative text:
User Pools I Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
Lil customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
POO' Id 
POOI ARN 
Estimated number of users 
Required attributes 
Alias attributes 
username attributes 
Enable case insensitivity? 
Custom attributes 
Minimum password length 
Password policy 
user sign ups allowed? 
FROM email address 
Email Delivery through Amazon SES 
MFA 
Verifications 
eu-west-2 7NBXJ2 
arn:awscognlto-idp:eu-west-2:398678778168userpool/eu-west-2 7NBXJ2hKp 
2 
email 
none 
none 
Yes 
Choose custom attributes.__ 
8 
uppercase letters, lowercase letters, special characters, numbers 
Users can sign themselves up 
Default 
No 
Note: You have chosen to have Cognito send emails on your behalf. Best practices suggest that customers send emails through Amazon SES 
for production user Pools due to a daily email limit. Learn more about email best practices. 
Enable MFA._ 
Email 

Machine generated alternative text:
User Pools I Federated Identities 
DemoPool 
General settings 
Users and groups 
Attributes 
Policies 
MFA and verifications 
Advanced security 
Message customizations 
Tags 
Devices 
App clients 
Triggers 
Analytics 
App integration 
App client settings 
Domain name 
Lil customization 
Resource servers 
Federation 
Identity providers 
Attribute mapping 
What identity providers and OAuth 2.0 settings should be used for your app clients? 
Each ot your app clients can use different identity providers and OAuth 2.0 settings. You must enable at least one identity provider for each app client. Learn more about identity providers. 
Enabled Identity Providers 
Cognito user Pool 
Sign in and sign out URLs 
App client DemoAppClient 
• 30a8r4pq46ngmh9i9v40pnOhm 
Select all 
Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL. 
callback URL(S) 
https://courses.datacumulus.com/ 
Sign out URL(S) 
OAuth 2.0 
Select the OAuth flows and scopes enabled for this app. Learn more about flows and scopes. 
Allowed OAuth Flows 
Authorization code grant Implicit grant Client credentials 
profile 
Allowed OAuth Scopes 
phone email openid 
Hosted UI 
aws.cognito.signin_user.admin 

**This is how we integrate cognito identity provide with congnito user pool**

Machine generated alternative text:
Getting started wizard 
I Step I: Create identity pool 
Step 2: Set permissions 
Create new identity pool 
Identity pools are used to store end user identtes. To declare a new identity pool, enter a unique name. 
Identity pool name' 
Example: My App Name 
unauthenticated identities o 
Amazon Cognito can support unauthenticated identities 
e 
ing a unique identifier and AD'S credentials for users who do not authenticate with an identity provider If your application allows customers to use the applicaton without logging in, you can enable access for unauthenticated identities Leam more about unauthenticated identities. 
Æn AWS typicSty do rot in to application TypicSty. s—iEions fM 
ble access to unauthenticated identities 
Authentication flow settings o 
Auser authenticatngwith Amazon Cognito vill go through a multi-step processto bootstrap their credentials Amazon Cognito has differentlowsfor authentication with public prwiders: enhanced and basic Cognito recommends the use of enhanced authenticaton flovx H cwæver, if you stllwishto use the basic n cnv, you can enable ithere. Learn more about 
authentication flows 
Allcnv Basic (Classic) Flow' 
Authentication providers o 
Amazon Cognito supports the follcnving authentcation methods withAmazon Cognito Sign-In or any public provider. If y:'u al I cm your users to authenticate using any of these publicprwiders, you can specify your application identifiers here Warning: Changing the application ID that your identty pool is linkedtowill prevent existing users from authenticating using 
Amazon Cognito. Learn more about public identity providers. 
Cognito Amazon Apple 
Facebook Google* Twitter / Digits OpenlD 
Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Poo' ID and the App Cient ID. 
User Pool ID 
App client id 
Add 
Required 
3 CE8r4pq4tngmhgigv4C•prÆhrnq 

**Click on create pool**

**These are the roles created for us click on allow**

Machine generated alternative text:
Hide Details 
Role Summary O 
Role Description 
IAM Role 
Role Name 
Oikarinen could you please the changes done 
Your authenticated identities would like access to Cognito. 
Create a new IAM Role 
Cognito_MyDemoIdentityPoolAuth_Role 
Allow 
v Hide Policy Document 
Edit 
"Version": "2012-10-17", 
"Statement": 
"Effect": "Allow", 
"Action": 
"mobileanalytics:PutEvents", 
"cognito-sync: , 
"cognito-identity:*" 
Cancel 

**Two roles created**

Machine generated alternative text:
aws 
Identity and Access 
Management (IAM) 
Identity providers 
settings 
Access reports 
activity 
Control 
Resource Groups 
Create role 
Q Identit 
C.-MO_ 
Global 
Support • 
Showing 2 
Pdiey 
Q Feedback 
English 

**Note : we can attach policy to role**

Machine generated alternative text:
avvS 
Resource Groups 
Add permissions to Cognito_MyDemoldentityPoolAuth 
Attach Permissions 
Filter policies v 
Poucy 
knazonDMSRedshittS3R01e 
knazmS3BeX&yAress 
Role 
Globa • 
7 results 
Perrnissbns p&cy (1) 
Pdiey 
Feedback 
AWS 
AWS man* 
AWS 
Custm'er mmaged 
AWS 
English 

**More option**

Machine generated alternative text:
Identity pool 
Identity browse 
Q&A 
Edit identity pool 
Frorn page you o' a a Of The are With r 
we a to althorize a we to the identity is page when 
COV'itO w"' 
iew 
l&ntity 
ID O 
eu-west-2 ; AR" 
Unauthenticated identities 0 
Authentication flow settings o 
Authentication providers o 
push synchronization 
Cognito Streams 
Announcements 
Notes 

**Cognito user pool vs cognito identity pool**

Machine generated alternative text:
Cognito User Pools vs Identity Pools 
• Cognito User Pools: 
• Database of users for your web and mobile application 
• Allows to federate logins through Public Social, OIDC, SAML.. 
• Can customize the hosted UI for authentication (including the logo)) 
• Has triggers with AWS Lambda during the authentication flow 
• Cognito Identity Pools: 
• Obtain AWS credentials for your users 
• Users can login through Public Social, OIDC, SAML & Cognito User Pools 
• Users can be unauthenticated (guests) 
• Users are mapped to IAM roles & policies, can leverage policy variables 
• CUP + CIP manage user / password + access AWS services 

Machine generated alternative text:
Web & Mobile 
Applications 
Direct access to AWS 
Private S3 Bucket 
O Stephane Maarek 
Cognito Identity Pools 
Login and Get Token 
Diagram with CUP 
Cognito 
User Pools 
Internal DB 
of users 
Exchange token 
for temporary 
AWS credentials 
DynamoDB Table 
Cognito 
Identity Pools 
validate 
e 
Get temp creds STS 

**Cognito Sync**

Machine generated alternative text:
Cognito Sync 
• Deprecated — use AWS AppSync now 
• Store preferences, configuration, state of app 
• Cross device synchronization (any platform — iOS, Android, etc... ) 
• Offine capability (synchronization when back online) 
• Store data in datasets (up to I MB), up to 20 datasets to synchronize 
• Push Sync: silently notify across all devices when identity data changes 
• Cognito Stream: stream data from Cognito into Kinesis 
• Cognito Events: execute Lambda functions in response to events 