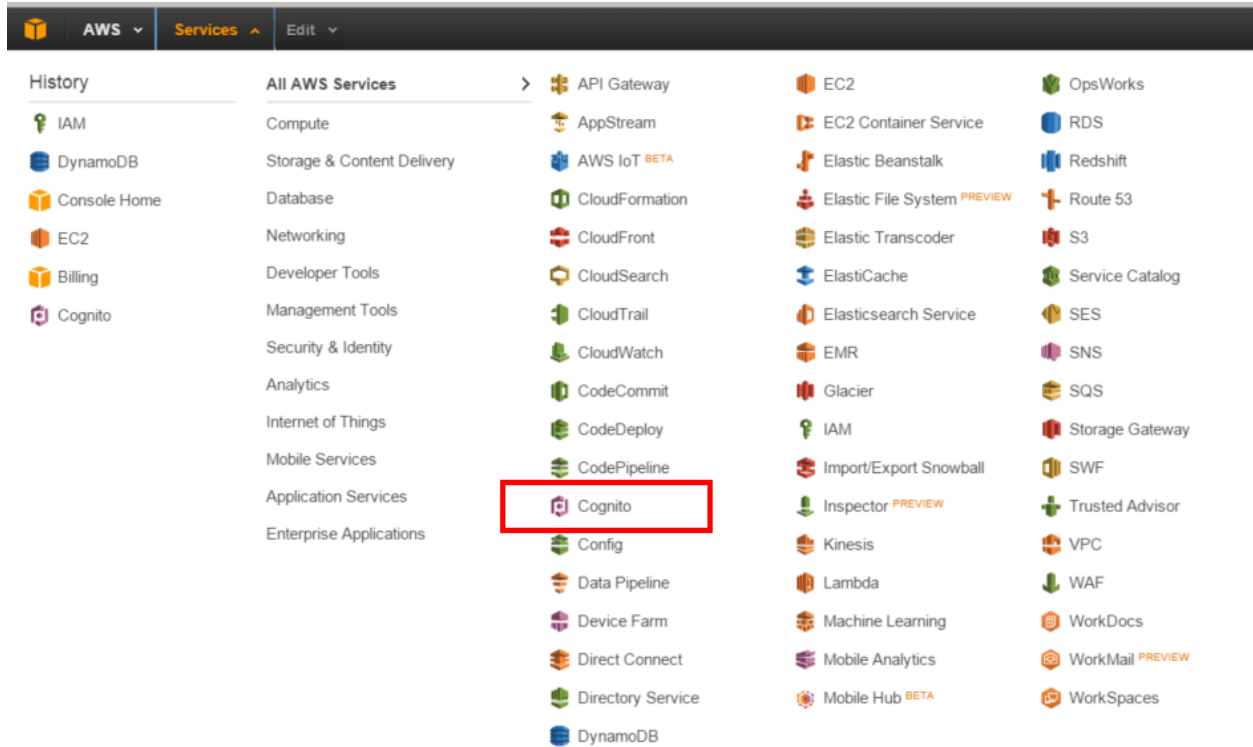
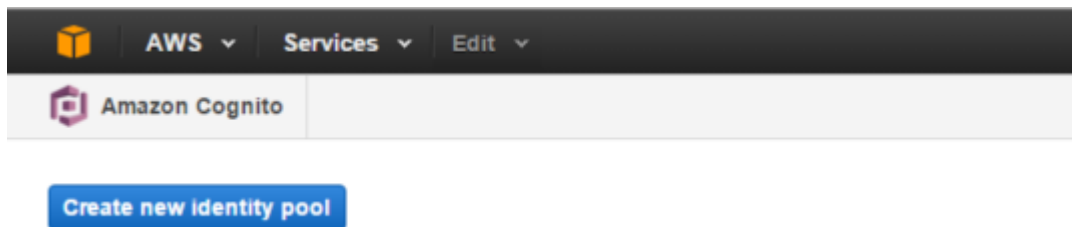


AWS Cognito Setup Primer

1. Log into AWS console, select 'Cognito' from service tab



2. Create new Identity Pool with some name relating to your game



3. IMPORTANT: If you are not going to create / use a custom provider (which DDBHelper does not currently support, but if you know what you're doing shouldn't too hard to add since you have all the source code) you MUST allow Unauthenticated identities access. Anything that is not from Facebook, Google+, Amazon, etc. is unauthenticated.

Getting started wizard

Step 1: Create identity pool

Step 2: Set permissions

Create new identity pool

Identity pools are used to store end user identities. To declare a new identity pool, enter a unique name.

Identity pool name*

RelevantAppRelatedName



Example: My App Name

Unauthenticated identities

Amazon Cognito can support unauthenticated identities by providing a unique identifier and AWS credentials for users who do not authenticate with an identity provider. If your application allows users who do not log in, you can enable access for unauthenticated identities. [Learn more about unauthenticated identities.](#)



Enable access to unauthenticated identities

Authentication providers

Amazon Cognito recognizes tokens from these public identity providers. If you allow your users to authenticate using any of these providers, you can specify your application identifiers here. Warning: Changing the application id your identity pool is linked to will prevent existing users from authenticating with Amazon Cognito. [Learn more about public identity providers.](#)

Amazon

Facebook

Google+

Twitter

OpenID

Custom

Amazon App ID

Optional

Example: amzn1.application.188a56d827a7d6555a8b67a5d

* Required

Cancel

Create Pool

- The next page is creating your IAM roles, which later you will provide access to resources. The names are filled in for you already. There are two roles, authenticated and unauthenticated. As stated earlier, we are doing unauthenticated access since it is anonymous login and not using an authentication provider.

Your Cognito identities require access to your resources

Assigning a role to your application end users helps you restrict access to your AWS resources. Amazon Cognito integrates with Identity and Access Management (IAM) and lets you select specific roles for both your authenticated and unauthenticated identities. [Learn more about IAM.](#)

By default, Amazon Cognito creates a new role with limited permissions - end users only have access to Cognito Sync and Mobile Analytics. You can modify the roles if your application needs access to other AWS resources, such as S3 or DynamoDB.

▼ Hide Details

Role Summary ?

Role Your authenticated identities would like access to Cognito.

Description

IAM Role Create a new IAM Role ▼

Role Name Cognito_ReleventAppRelatedNan

► View Policy Document

Role Summary ?

Role Your unauthenticated identities would like access to Cognito.

Description

IAM Role Create a new IAM Role ▼

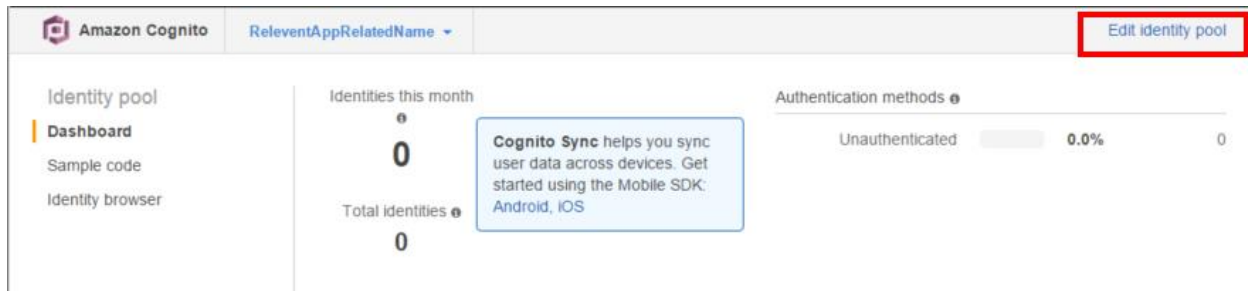
Role Name Cognito_ReleventAppRelatedNan

► View Policy Document

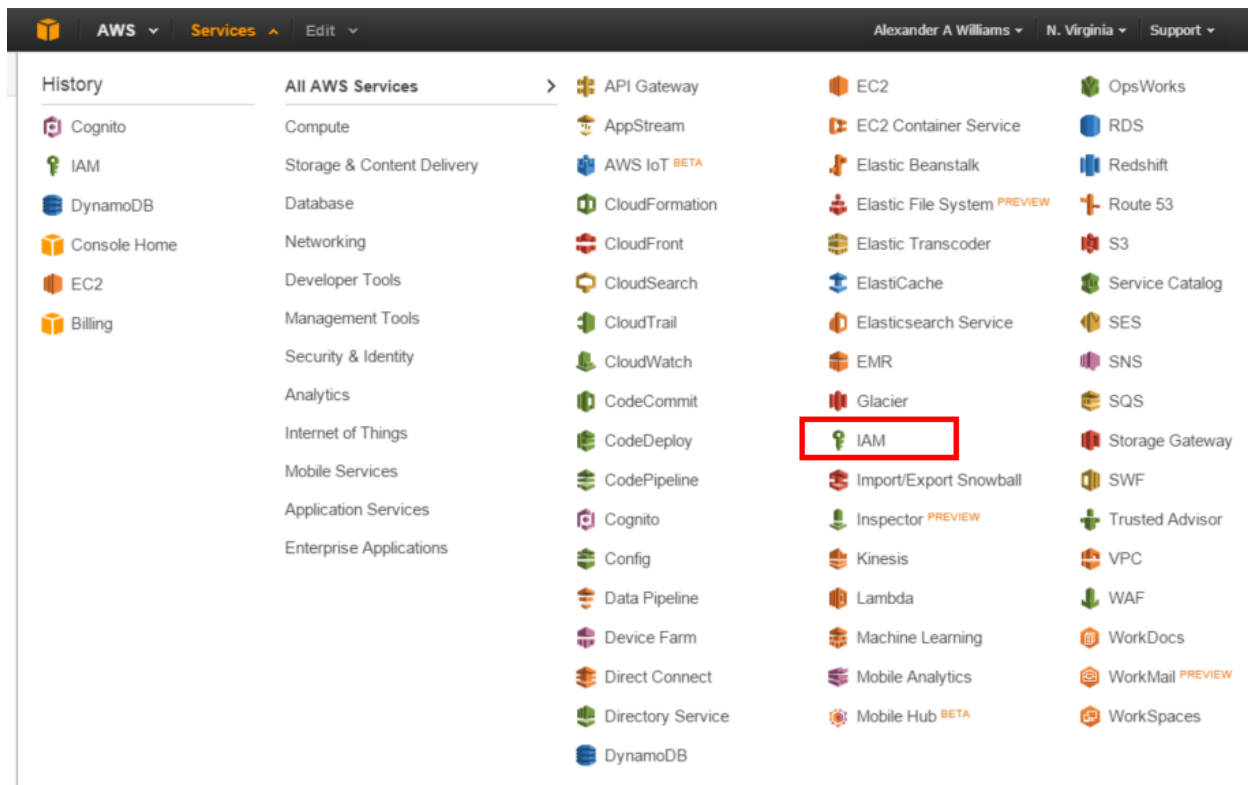
Don't Allow

Allow

- If you want to change your pool identity settings, even after creation, there is a link in the upper-right of the page for 'Edit Identity Pool'



- Now that the Identity Pool is created, and the Roles, we need to give the Roles access to resources. Select the IAM link from the AWS Services dropdown.



7. On the left, select 'Roles' – then from the list of roles that are populated, we will select the Cognito_<RoleName>Unauth_Role or whatever you named it. We're editing the Unauthorized access role.

The screenshot shows the AWS IAM console 'Roles' page. The left sidebar contains a navigation menu with 'Roles' highlighted. The main content area shows a table of roles. The role 'Cognito_ReleventAppRelatedNameUnauth_Role' is highlighted with a red box.

<input type="checkbox"/>	Role Name ↕	Creation Time ↕
<input type="checkbox"/>	Cognito_DDBHelperAuth_Role	2015-08-04 21:44 EDT
<input type="checkbox"/>	Cognito_DDBHelperUnauth_Role	2015-08-04 21:44 EDT
<input type="checkbox"/>	Cognito_DDBTestAuth_Role	2015-08-15 17:30 EDT
<input type="checkbox"/>	Cognito_DDBTestUnauth_Role	2015-08-15 17:30 EDT
<input type="checkbox"/>	Cognito_ReleventAppRelatedNameAuth_Role	2015-11-13 16:07 EST
<input type="checkbox"/>	Cognito_ReleventAppRelatedNameUnauth_Role	2015-11-13 16:07 EST

8. Once viewing the role, we will want to attach a policy to the role.

The screenshot shows the AWS IAM console role details page for 'Cognito_ReleventAppRelatedNameUnauth_Role'. The 'Permissions' tab is selected, and the 'Attach Policy' button is highlighted with a red box.

Summary

Role ARN arn:aws:iam::349106405996:role/Cognito_ReleventAppRelatedNameUnauth_Role

Instance Profile ARN(s)

Path /

Creation Time 2015-11-13 16:07 EST

Permissions | Trust Relationships

Managed Policies

There are no managed policies attached to this role.

Attach Policy

Inline Policies

This view shows all inline policies that are embedded in this role.

Create Role Policy

Policy Name	Actions
oneClick_Cognito_ReleventAppRelatedNameUnauth_Role_1447448672023	Show Policy Edit Policy Remove Policy Simulate Policy

9. You can search for the policy you want, create a new policy, or just filter the policies from the top. I usually filter for 'DynamoDB' and depending on what sort of access you want, you can give them... well, whatever you want. For this tool and demonstration purposes, we are attaching the 'AmazonDynamoDBFullAccess' policy.

Attach Policy

Select one or more policies to attach. Each role can have up to 10 policies attached.

Filter: Policy Type ▾		Showing 5 results		
<input type="text" value="DynamoDB"/>				
	Policy Name ▴	Attached Entities ⇅	Creation Time ⇅	Edited Time ⇅
<input checked="" type="checkbox"/>	AmazonDynamoDBFullAccess	2	2015-02-06 13:40 EST	2015-11-11 21:17 EST
<input type="checkbox"/>	AmazonDynamoDBFullAccesswithDataPipel...	0	2015-02-06 13:40 EST	2015-11-11 21:17 EST
<input type="checkbox"/>	AmazonDynamoDBReadOnlyAccess	1	2015-02-06 13:40 EST	2015-11-11 18:39 EST
<input type="checkbox"/>	AWSLambdaDynamoDBExecutionRole	0	2015-04-09 11:09 EDT	2015-04-09 11:09 EDT
<input type="checkbox"/>	AWSLambdaInvocation-DynamoDB	0	2015-02-06 13:40 EST	2015-02-06 13:40 EST

Cancel **Attach Policy**

10. Once the policy has been attached, it will show as the Policy Name in the Roles Summary. Additionally, if you need to find your Cognito connection string, it can be found under the Trust Relationships section in the Roles, or in the Cognito Service section from earlier.

IAM > Roles > Cognito_RelaventAppRelatedNameUnauth_Role

Summary

Role ARN: arn:aws:iam::349106405996:role/Cognito_RelaventAppRelatedNameUnauth_Role

Instance Profile ARN(s):

Path: /

Creation Time: 2015-11-13 16:07 EST

Permissions | **Trust Relationships**

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

Edit Trust Relationship

Trusted Entities

The following trusted entities can assume this role.

Trusted Entities		
cognito-identity.amazonaws.com		

Conditions

The following conditions define how and when trusted entities can assume the role.

Condition	Key	Value
StringEquals	cognito-identity.amazonaws.com:aud	us-east-1:fa5fb468-a6b9-417f-a6e4-5354c5421ac
ForAnyValue:StringLike	cognito-identity.amazonaws.com:amr	unauthenticated

11. At this point, you should be able to use that Congito connection value to use DynamoDBHelper to connect to the database resources. Once you connect, you will see in the Cognito services that an identity was created upon connection.