Deployment Instructions for GenAI with QBusiness

Deployment Version 2

Steps to Deploy the CloudFormation Stack

Deploy the provided CloudFormation (CFN) template, ensuring to add the required certificate ARN and application ID.

After successful deployment, retrieve the following values from the stack output:

- Audience: Used to set up the customer application in IAM Identity Center.

- RoleArn: The ARN of the IAM role required to set up the token exchange in IAM Identity Center.

- TrustedIssuerUrl: The endpoint of the trusted issuer to set up IAM Identity Center.

- URL: The load balancer URL to access the UI application.

Steps to Create IAM Identity Center Application

On the IAM Identity Center console, add a new custom managed application.

For Application type, select OAuth 2.0, then choose Next.

Enter an application name and description.

Set Application visibility as Not visible, then choose Next.

On the Trusted token issuers tab, choose Create trusted token issuer.

For Issuer URL, provide the TrustedIssuerUrl copied from the CloudFormation stack output.

Enter an issuer name and keep the map attributes as Email.

In the IAM Identity Center application authentication settings, select the trusted token issuer created in the previous step and add the Aud claim, providing the audience you copied from the CloudFormation stack output, then choose Next.

On the Specify application credentials tab, choose Enter one or more IAM roles and provide the value for RoleArn copied from the CloudFormation stack output.

Review all the steps and create the application.

After the application is created, go to the application, choose Assign users and groups, and add the users who will have access to the UI application.

On the Select setup type page, choose All applications for service with same access, choose Amazon Q from the Services list, and choose Trust applications.

Final Steps

On the AWS CloudFormation console, update the stack and provide the IAM Identity Center application ARN for the parameter IdcApplicationArn, then run the stack.

When the update process is complete, go to the CloudFormation stack's Outputs tab and copy the URL provided there.

Go to the URL provided in the CloudFormation stack output to access the application.

If accessing for the first time, sign up the user with the same credentials as the user created in IAM Identity Center and assigned to the IAM Identity Center application.

After successful user creation, log in. Upon successful login, you will be redirected to the application.

Code Flow (Same for Both Versions)

On load of the application, a login button is shown to the user. Upon clicking, the user is redirected to the Cognito hosted UI.

If accessing for the first time, sign up the user with the same credentials as the user created in IAM Identity Center and assigned to the IAM Identity Center application.

After successful user creation, log in. Upon successful login, the user is redirected to the application.

In the application, retrieve the token from the response after successful login and set it in the state.

Get the IAM OIDC token using the ID token retrieved from Cognito.

Assume the IAM role with the IAM OIDC idToken.

Create the Q client using the identity-aware AWS Session and start the conversation.