Cognito Machine Authentication Setup Guide

The TEAM Cognito machine authentication configuration is an optional configuration to make the TEAM graph API accessible programmatically.

Run API Machine Authentication configuration script

The **api-machine-auth.sh** bash script in the **deployment** folder performs the following actions within the **TEAM_ACCOUNT**:

- Creates a Resource Server with an id of `api` on the Cognito User Pool with a custom scope of `admin`.
- Creates a User Pool Client on the Cognito User Pool with client secret generation enabled along with the other needed configuration for machine auth flows and allows it access to the `api/admin` custom scope.

> **IMPORTANT**
> Ensure that the named profile for the **TEAM Deployment account** has sufficient permissions before executing the **api-machine-auth.sh** script

Execute the following command in the root directory:

```
cd deployment
./api-machine-auth.sh
```

The **api-machine-auth.sh** script should be deployed successfully without any errors.

The configuration to enable machine authentication against your AWS TEAM API is now complete.

Retrieve Machine Authentication Credentials

The simplest method to retrieve the machine authentication credentials is to run the **get-machine-auth-credentials.sh** script. The script will output the following information to your terminal:

- `token_endpoint` - The oath token endpoint for the configured aws cognito pool.

- `graph_endpoint` - The graph endpoint for the TEAM deployment.
- `client_id` - The client id of the `machine_auth` cognito user pool client.
- `client_secret` - The client secret of the `machine_auth` cognito user pool client.

> **IMPORTANT**
>
> Ensure that the named profile for the **TEAM Deployment account** has sufficient permissions before executing the **get-machine-auth-credentials.sh** script

```
cd deployment
./get-machine-auth-credentials.sh
# example script output
token_endpoint="https://my.token.endpoint/oauth2/token"
graph_endpoint="https://my.graph.endpoint/graphql"
client_id="MyClientID"
client_secret="MyClientSecret"
```

These credentials can then be used for accessing the TEAM graph API programmatically with the language of your choice and can also be used to configure the terraform provider for awsteam.

Using Machine Authentication with the Graph API

In order to use machine authentication on the Graph API, you need:

1. Obtain the client Id and Secret from the Cognito User Pool Client named `machine_auth` or using the **get-machine-auth-credentials.sh** script.
2. Use these to obtain a token from the token endpoint for the Cognito User Pool. This process is detailed in the AWS Cognito Guide.
3. Use this token in the `Authorization` header when making calls to the TEAM Graph API.

Using the Terraform Provider

Explore the community-supported Terraform provider designed for awsteam, enabling seamless configuration management through Terraform. Machine authentication credentials are required to use the provider.

> **IMPORTANT**
>
> The Terraform provider is maintained independently of the aws-samples community, and the TEAM authors do not assume responsibility for its maintenance.