DOW JONES

Securing Applications Inside and Out with AWS Cognito and Federated IdP’s

Steve Stevenson
Scott Canham

10/3/2018

Introduction

Who we are

What you can expect

- Overview of OpenID Connect (OIDC) and use of federated Identity Provider (IdP)
- Overview of Cognito and Load Balancer Authentication
- Demo (Setting up Cognito with IdP & Enabling)
- Demo (Enabling IdP authentication on Load Balancer)

Dow Jones

- Consumer websites, mobile applications and print media
- Internal tools that support our front end applications

WSJ

MarketWatch

BARRON'S

Internal Authenticated Applications

- Applications that aid in publishing and managing content
- Built using the identity providers we’ve used over the years
- Hope to provide a consistent interface going forward

AWS Cognito

- Provides user management as well as authentication and authorization
- User data synchronization across multiple platforms
- Federated IdP integration

AWS Cognito

- Standards based authentication
- Provides industry level compliance with HIPAA and many ISO based standards

AWS Cognito - User Pools

- Stores user information in directories known as user pools
- User data can come from multiple sources
- User sign in / sign up functionality
- Scales to hundreds of millions of users

AWS Cognito - Identity Pools

- Identity pools are generally used to authenticate a user and associate them to aws roles
- Integrates with third parties easily
- Grants AWS credentials for using other amazon services

AWS Cognito - Other Features

- Lamdba integration for customized security features or workflows
- Cognito Sync for syncing user data across devices, and applications

OpenID Connect

- This standard was established in 2015 by the open source community
- Standardized claims to improve IdP Interoperability

JSON Web Token

eyJraWQiOiJWeGRmNTVtcnBsSmJHNDlxNStscGdYajlzdnRyOGlJTXE3dlRxeU80ZjY4PSIsImFsZyI6IlJTMjU2In0.ey
JhdF9oYXNoIjoiem9BS0Y4MEpnSmNtTWJWcEhSOVVjdyIsInN1YiI6ImVlMDg2NDNkLTVhNTktNGUzMi1hNmM5LT
Q5MTQxNzY5NWM3MCIsImNvZ25pdG86Z3JvdXBzIjpbInVzLWVhc3QtMV9ESTljT0ZzN2lfRG93am9uZXMtZGVtbyJ
dLCJlbWFpbF92ZXJpZmllZCI6ZmFsc2UsImlzcyI6Imh0dHBzOlwvXC9jb2duaXRvLWlkcC51cy1lYXN0LTEuYW1hem9
uYXdzLmNvbVwvdXMtZWFzdC0xX0RJOWNPRnM3aSIsImNvZ25pdG86dXNlcm5hbWUiOiJEb3dqb25lcy1kZW1vX2
F1dGgwfDViYWQyOTc2Yzg2MmFhMTA1NDQ0YzA0MyIsImF1ZCI6IjE1Mm5oMW8wczBjZWVnM2g3OWIxNzI2MWZ
vIiwiaWRlbnRpdGllcyI6W3sidXNlcklkIjoiYXV0aDB8NWJhZDI5NzZjODYyYWExMDU0NDRjMDQzIiwicHJvdmlkZXJO
YW1lIjoiRG93am9uZXMtZGVtbyIsInByb3ZpZGVyVHlwZSI6IlNBTUwiLCJpc3N1ZXIiOiJ1cm46ZG93am9uZXMtZGVtb
y5hdXRoMC5jb20iLCJwcmltYXJ5IjoidHJ1ZSIsImRhdGVDcmVhdGVkIjoiMTUzODA4MDc2MjkxNCJ9XSwidG9rZW5fd
XNlIjoiaWQiLCJhdXRoX3RpbWUiOjE1Mzg0OTMwNzQsImV4cCI6MTUzODQ5NjY3NCwiaWF0IjoxNTM4NDkzMDc0
LCJlbWFpbCI6InN0ZXZlLnN0ZXZlbnNvbkBkb3dqb25lcy5jb20ifQ.JLkUI0B_0aGRHJE0M8A1Sz27VKet4198-K5oqXtN
Z5Jtyv3SQg22Ef-hTEU5jzrV7L3Zv0ikSl-GthiwOu0wya5yIUKTjyNcSYBy_uH--Y6y7YbJVq9RlbgamrN_IYvFjWDChi6w
cSozdTBRbnnZZwxk3lcy3AKgnSFdghqBT8yQhuKR5Iccyq04ZFpaS5UDXRZT1gfliCKeiRQ0Q680CixBXQI0fR67DgH
onE3htYHKMJ_7kjg_gLOVqrSv4LJOvWIMF06dp2bQA9ADQww20-P2ozRG9wQKSnCRsoZWWNjnPEKRgXZmFfT0f
c3zOI1V8u1PKk4pN6-_b7h98rah-Q

JSON Web Token

- Header

```
{
  "kid": "Vxdf55mrplJbG49q5+lpgXj9svtr8iIMq7vTqyO4f68=",
  "alg": "RS256"
}
```

JSON Web Token

- Payload

```
{
  "at_hash": "zoAKF80JgJcmMbVpHR9Ucw",
  "sub": "ee08643d-5a59-4e32-a6c9-491417695c70",
  "email_verified": false,
  "iss": "https://cognito-idp.us-east-1.amazonaws.com/us-east-1_DI9cOFs7i",
  "aud": "152nh1o0s0ceeg3h79iq79v1fo",
  "token_use": "id",
  "auth_time": 1538493074,
  "exp": 1538496674,
  "iat": 1538493074,
  "email": "steve.stevenson@dowjones.com"
}
```

JSON Web Token

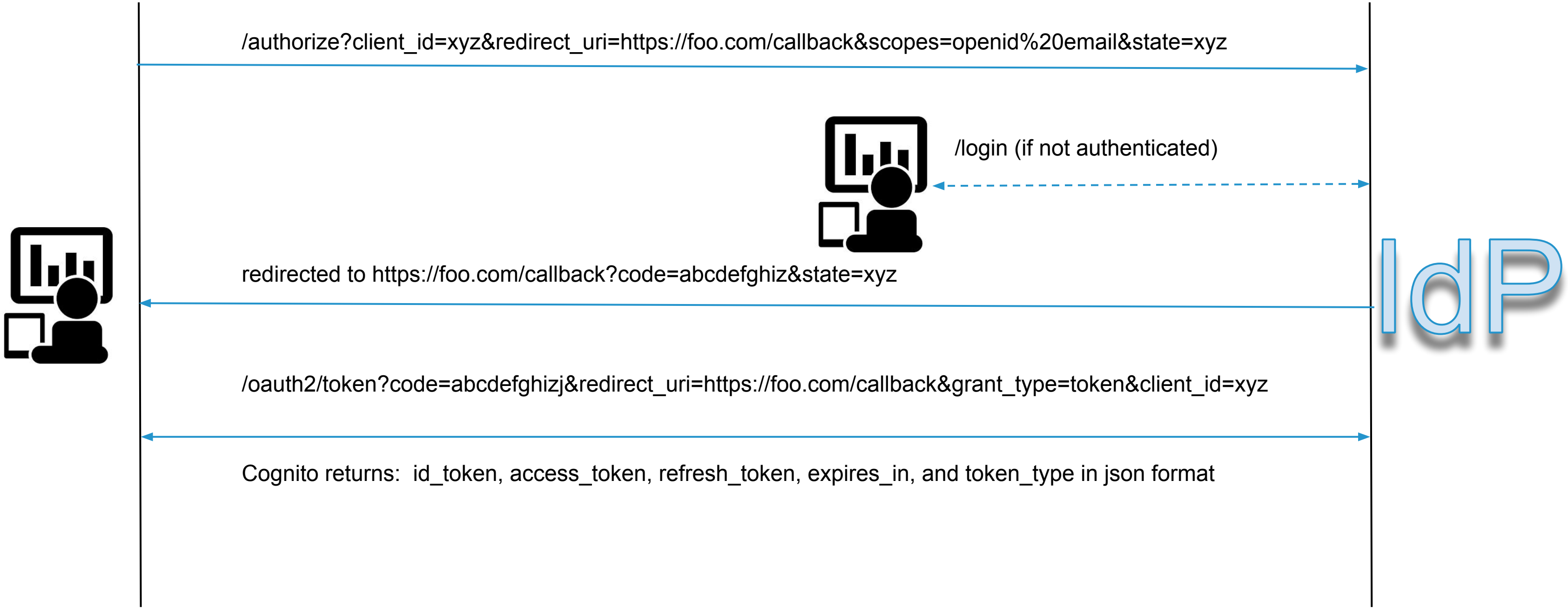
- Signature

```
RSASHA256(
base64UrlEncode(header) + "." +  base64UrlEncode(payload), public key, private key
)
```

OpenID Connect

- It is a layer on top of the Oauth2 specification
- Allows authentication without knowledge of passwords
- Removes ambiguity of Oauth2 tokens by defining a structured identity token
- Enhanced interoperability between identity providers
- Simplifies engineering efforts

OpenID Connect Authentication Code Flow



/authorize?client_id=xyz&redirect_uri=https://foo.com/callback&scopes=openid%20email&state=xyz

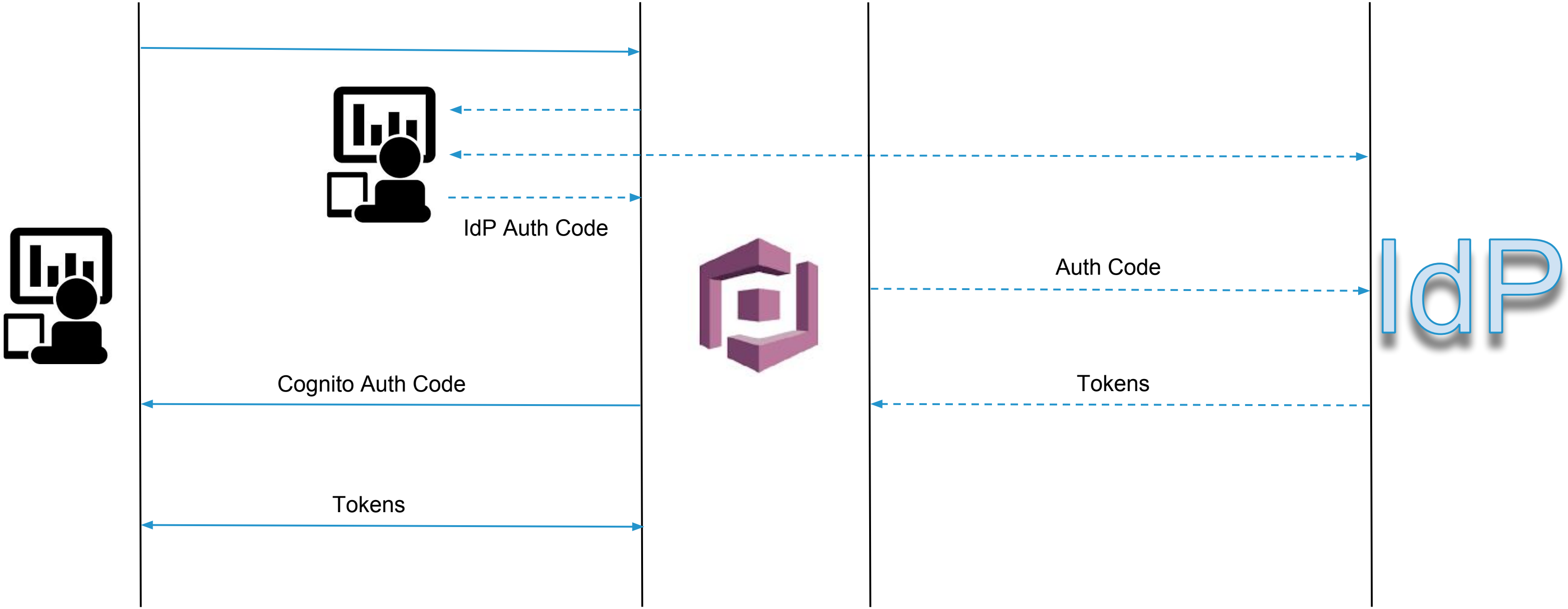
/login (if not authenticated)

redirected to https://foo.com/callback?code=abcdefghiz&state=xyz

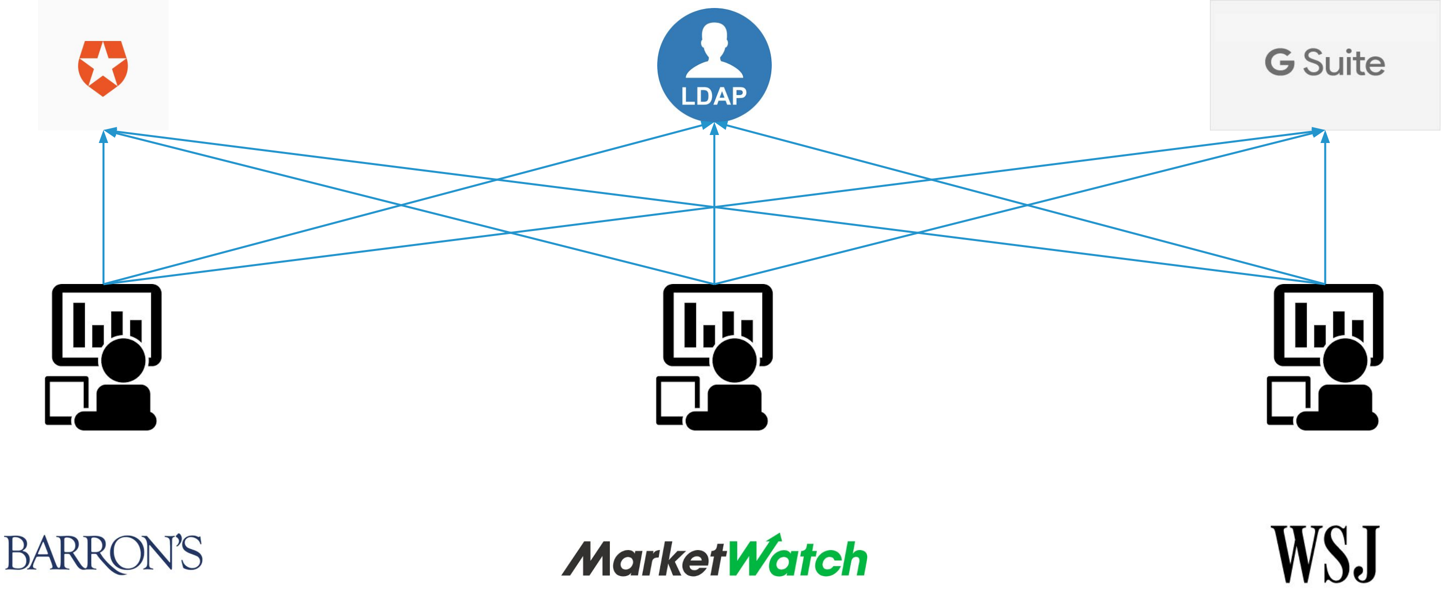
/oauth2/token?code=abcdefghizj&redirect_uri=https://foo.com/callback&grant_type=token&client_id=xyz

Cognito returns: id_token, access_token, refresh_token, expires_in, and token_type in json format

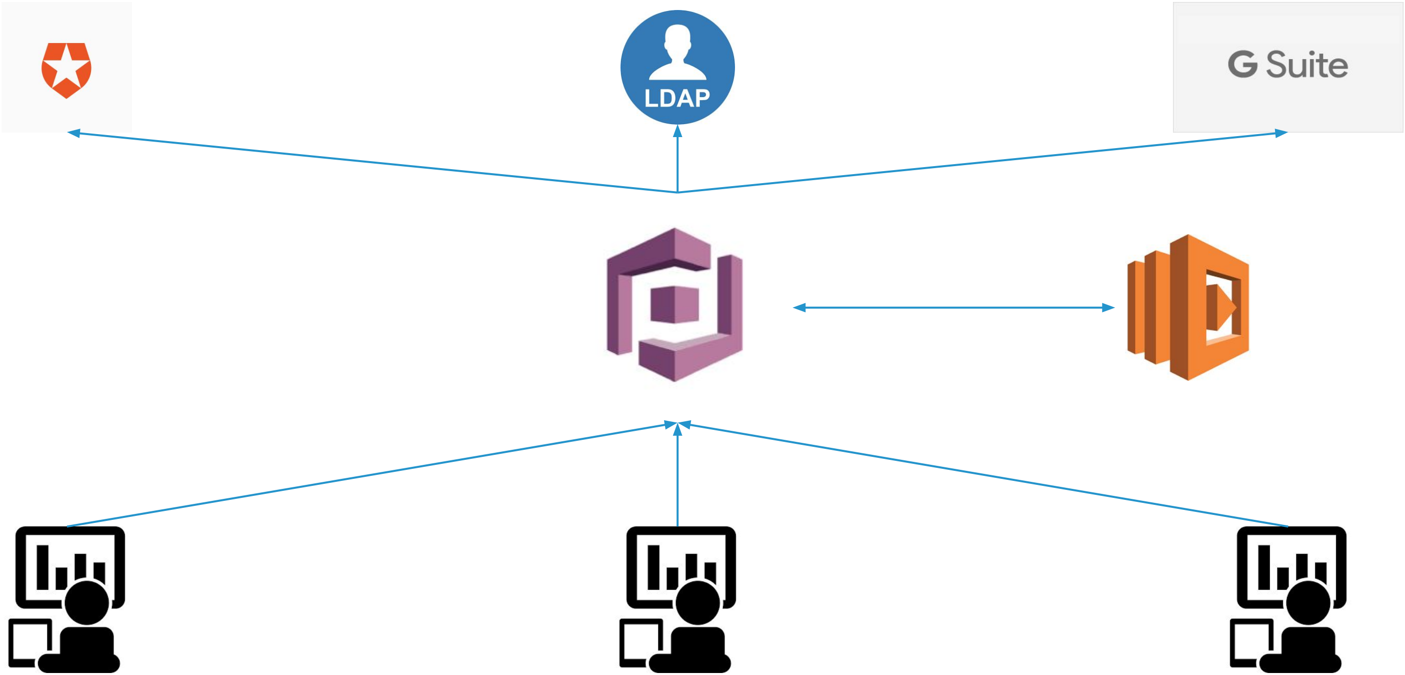
Cognito Federated IdP Authentication Flow



Pre migration



Post migration



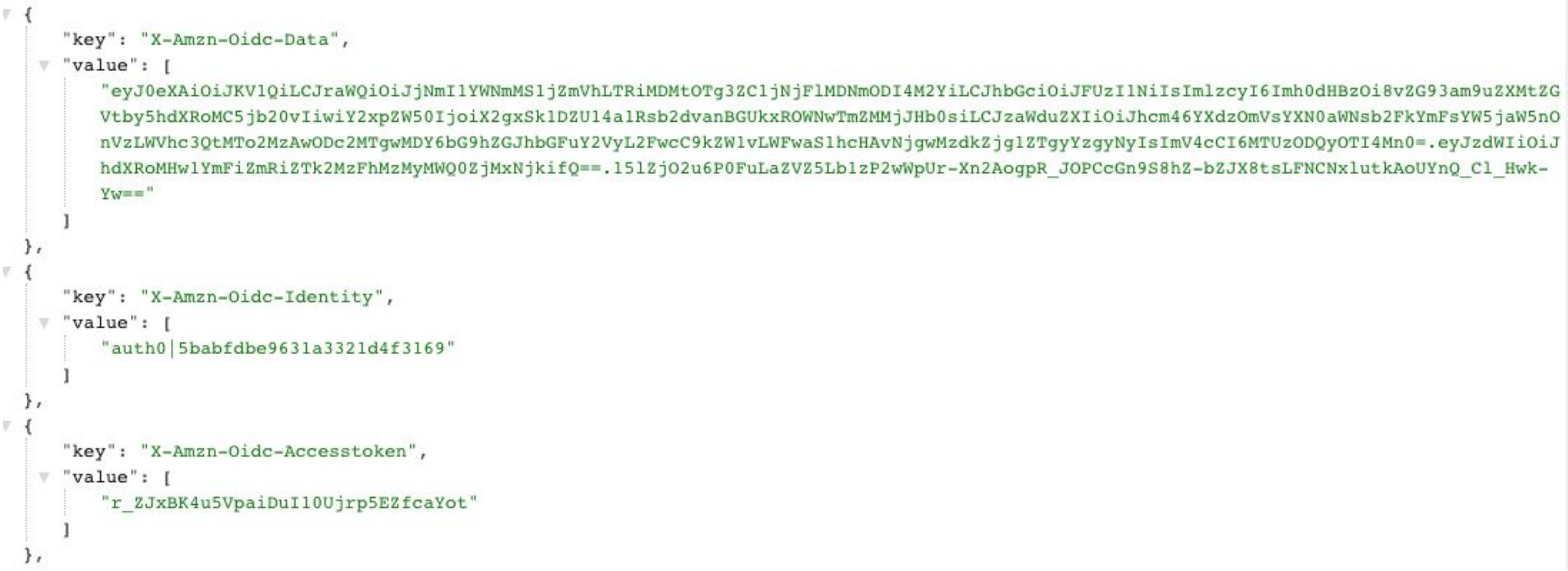
Demo

Cognito Setup and Usage

Load Balancer Authentication

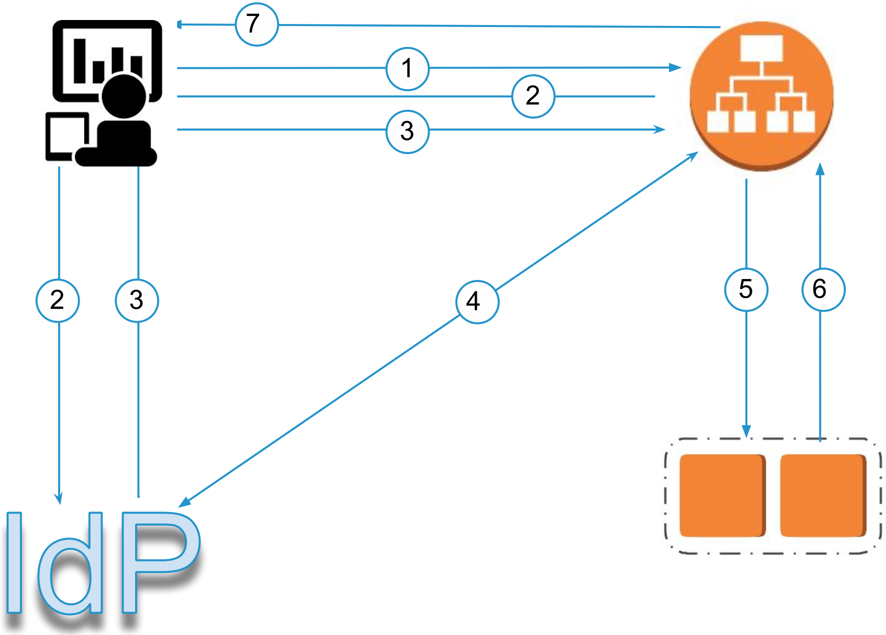
- Handles authentication code flow to Cognito or an OIDC compliant IdP
- Allows you keep the authentication flow logic out of your application
- Application can just focus on the authorization based on token & claims

Load Balancer Authentication



```
{
    "key": "X-Amzn-Oidc-Data",
    "value": [
        "eyJ0eXAiOiJKV1QiLCJraWQiOiJjNmI1YWNmMS1jZmVhLTRiMDMtOTg3ZC1jNjFlMDNmODI4M2YiLCJhbGciOiJFUzI1NiIsImlzcyI6Imh0dHBzOi8vZG93am9uZXMtZG
        Vtby5hdXRoMC5jb20vIiwiY2xpZW50IjoiX2gxSk1DZU14a1Rsb2dvanBGUkxROWNwTmZMMjJHb0siLCJzaWduZXIiOiJhcm46YXdzOmVsYXN0aWNsb2FkYmFsYW5jaW5nO
        nVzLWVhc3QtMTo2MzAwODc2MTgwMDY6bG9hZGJhbGFuY2VyL2FwcC9kZW1vLWFwaS1hcHAvNjgwMzdkZjg1ZTgyYzgyNyIsImV4cCI6MTUzODQyOTI4Mn0=.eyJzdWIiOiJ
        hdXRoMHw1YmFiZmRiZTk2MzFhMzMyMWQ0ZjMxNjkifQ==.15lZjO2u6P0FuLaZVZ5LblzP2wWpUr-Xn2AogpR_JOPCcGn9S8hZ-bZJX8tsLFNCNxlutkAoUYnQ_Cl_Hwk-
        Yw=="
    ]
},
{
    "key": "X-Amzn-Oidc-Identity",
    "value": [
        "auth0|5babfdbe9631a3321d4f3169"
    ]
},
{
    "key": "X-Amzn-Oidc-Accesstoken",
    "value": [
        "r_ZJxBK4u5VpaiDuIl0Ujrp5EZfcaYot"
    ]
},
```

Load Balancer Flow



Demo

ALB Authentication

Demo Summary

- Setup and configured a Cognito federated identity authentication system
- Implemented load balancer authentication using OIDC
- Remember regardless of implementation always validate your JWT’s

So again why do this?

- Simplify engineering efforts by normalizing the authentication workflow and reducing dev friction
- User Management can be moved to a central location
- Improved security for our web applications and api’s
- Grants us ability to give groups of identities aws access credentials
- With just a few lines of code implement sign in and sign up functionality

Thank You!

Steve.Stevenson@dowjones.com / Scott.Canham@dowjones.com

https://aws.amazon.com/cognito/dev-resources/
https://openid.net/specs/openid-connect-core-1_0.html
https://www.dowjones.com