vacuumlabs

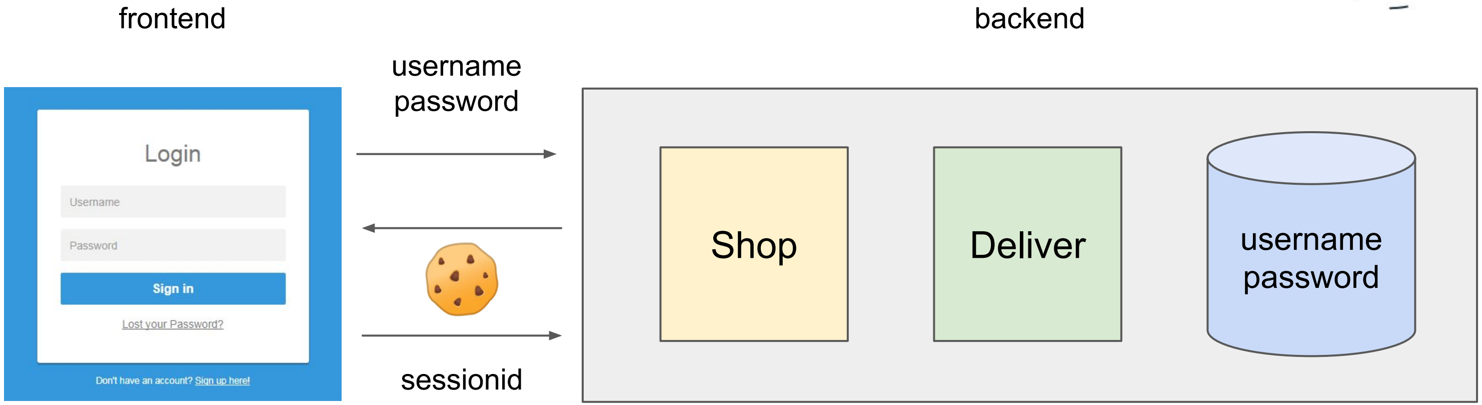
OAuth + Cognito

Gergely Nagy - *Senior Backend Engineer @* Vacuumlabs

gergely.nagy@vacuumlabs.com

https://vacuumlabs.com/jobs

- OAuthról általában
- Congitóról konkrétabban
- Demó alkalmazás



frontend

backend

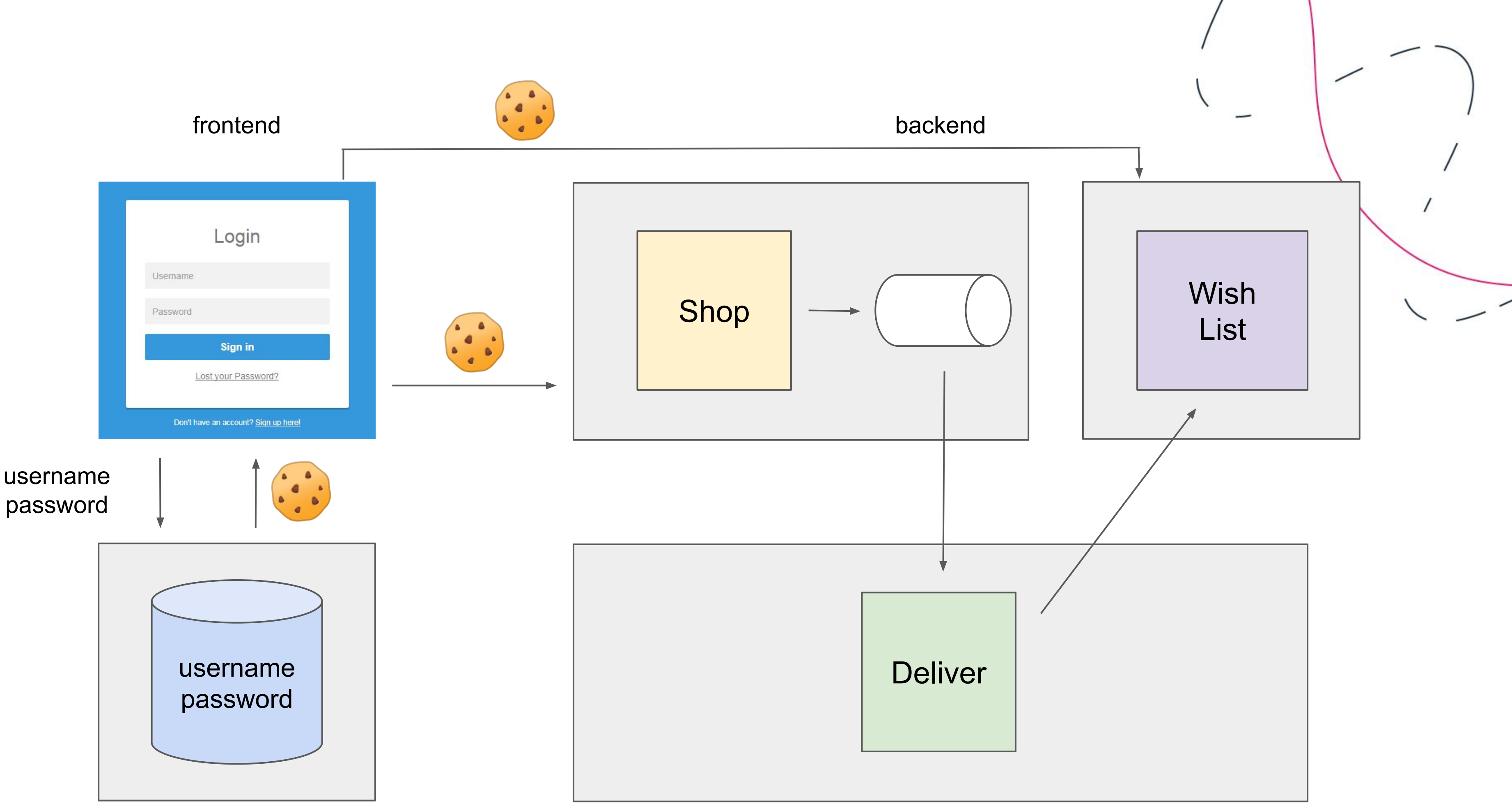
username
password

sessionid

Shop

Deliver

username
password



Login

Username

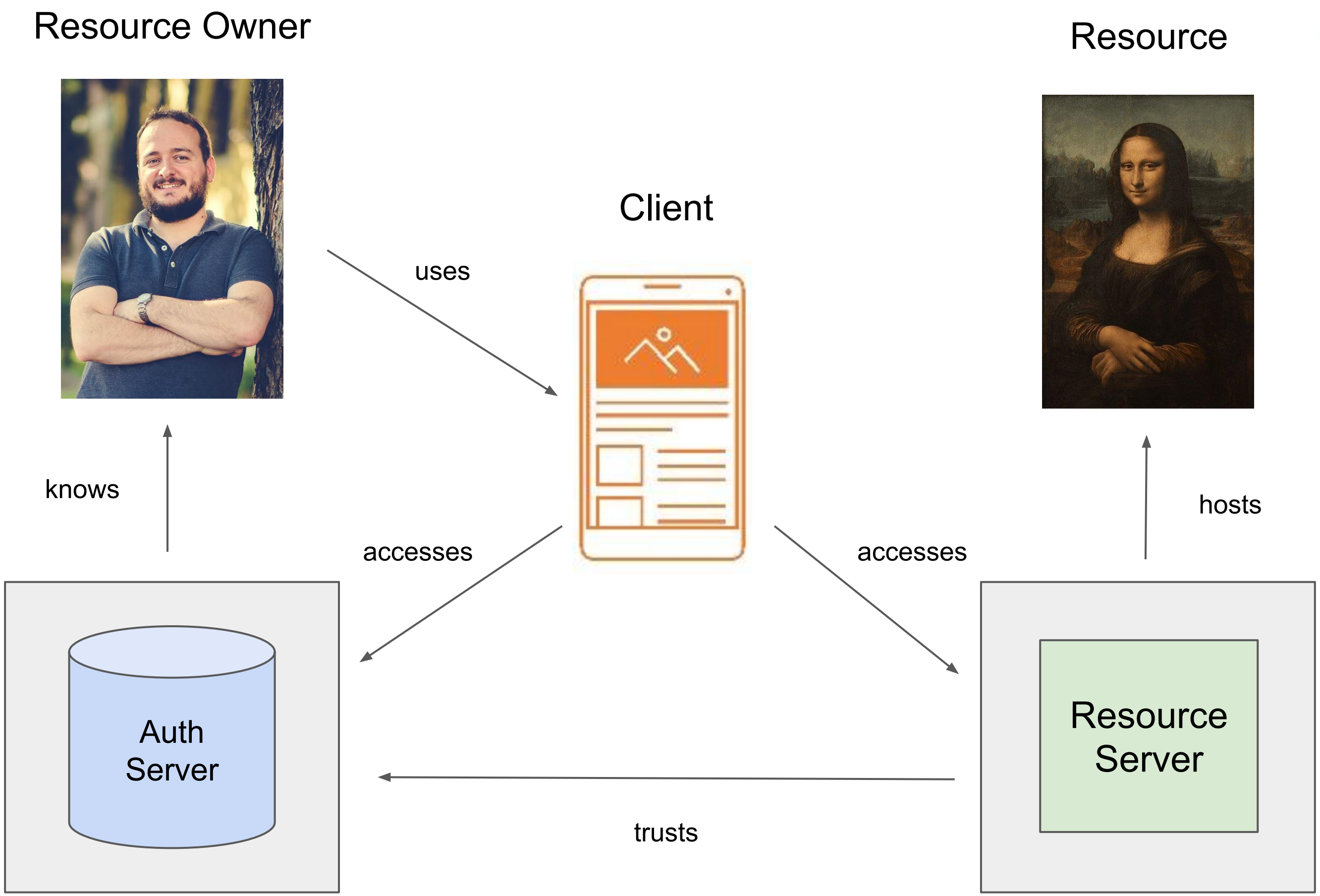
Password

Sign in

Lost your Password?

Don't have an account? Sign up here!

OAuth 2.0



Resource Owner

Client

Resource

uses

knows

hosts

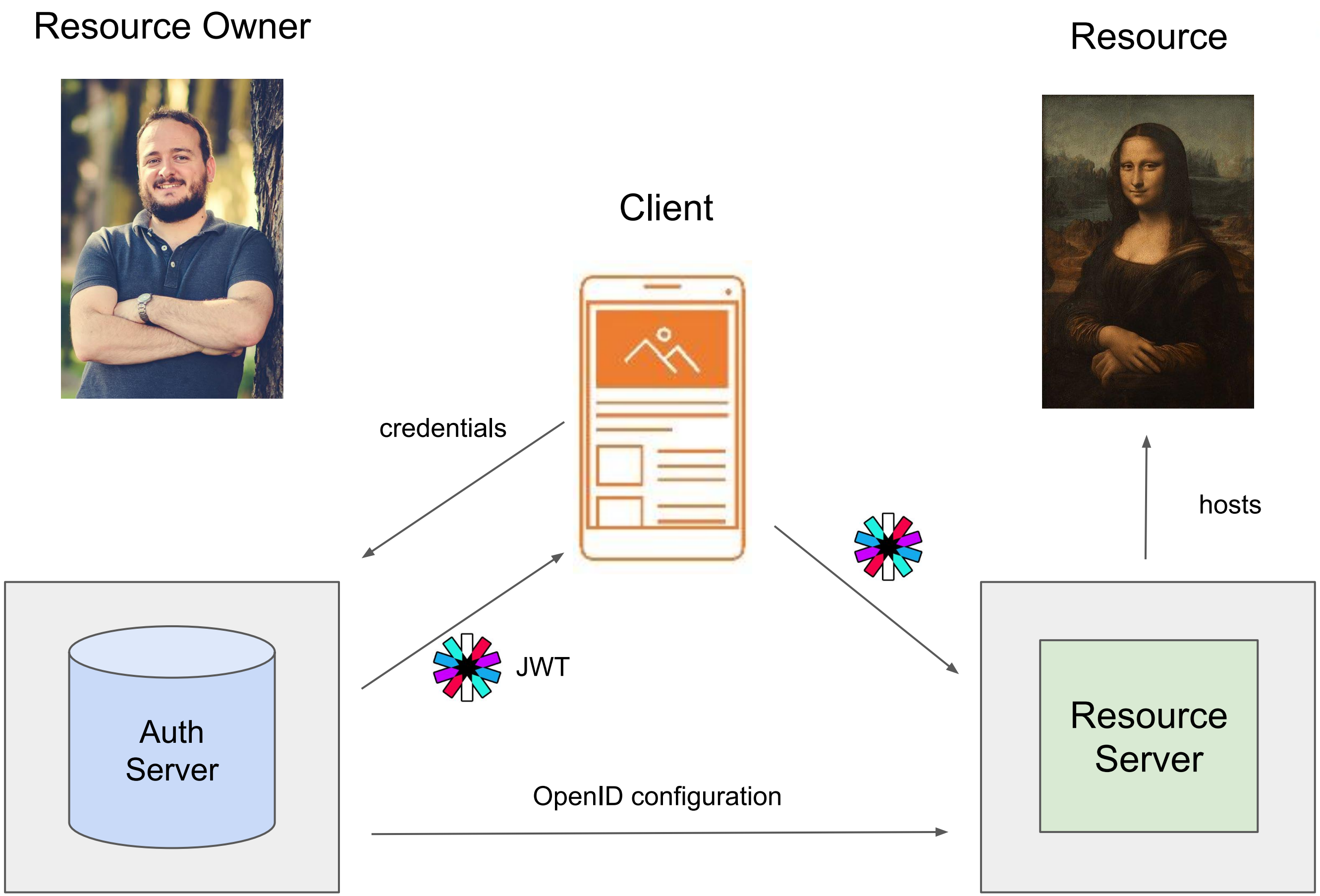
accesses

accesses

Auth Server

Resource Server

trusts



Resource Owner

Client

Resource

credentials

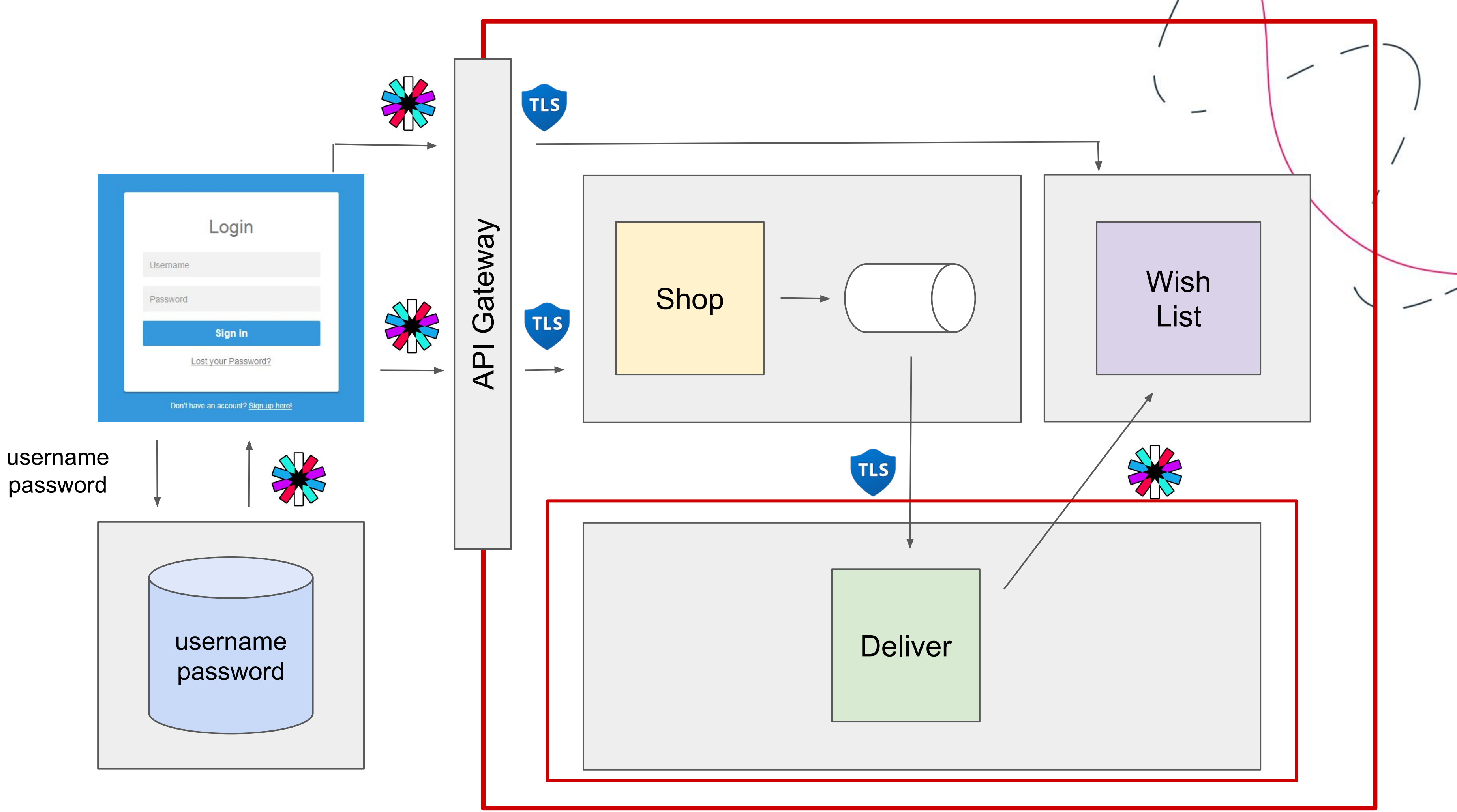
JWT

hosts

Auth Server

OpenID configuration

Resource Server



Login
Username
Password
Sign in
Lost your Password?
Don't have an account? Sign up here!
username
password
username
password
API Gateway
TLS
TLS
Shop
Wish
List
TLS
Deliver

Tokenek

(zsetonok? :)

Bearer Token

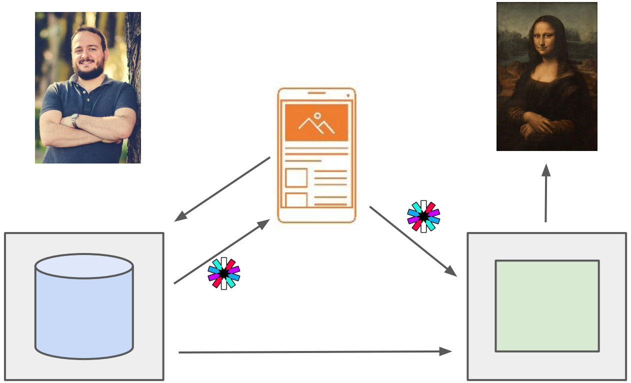
eyJhbGciOiJIUzI1NiIsIn

JSON Web Token

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpX
VCJ9.eyJzdWIiOiIxMjM0NTY3ODk
wIiwibmFtZSI6IkpvaG4gRG9lIiwia
WF0IjoxNTE2MjM5MDIyfQ.SflKxw
RJSMeKKF2QT4fwpMeJf36POk6y
JV_adQssw5c

Bearer Token

eyJhbGciOiJIUzI1NiIsIn



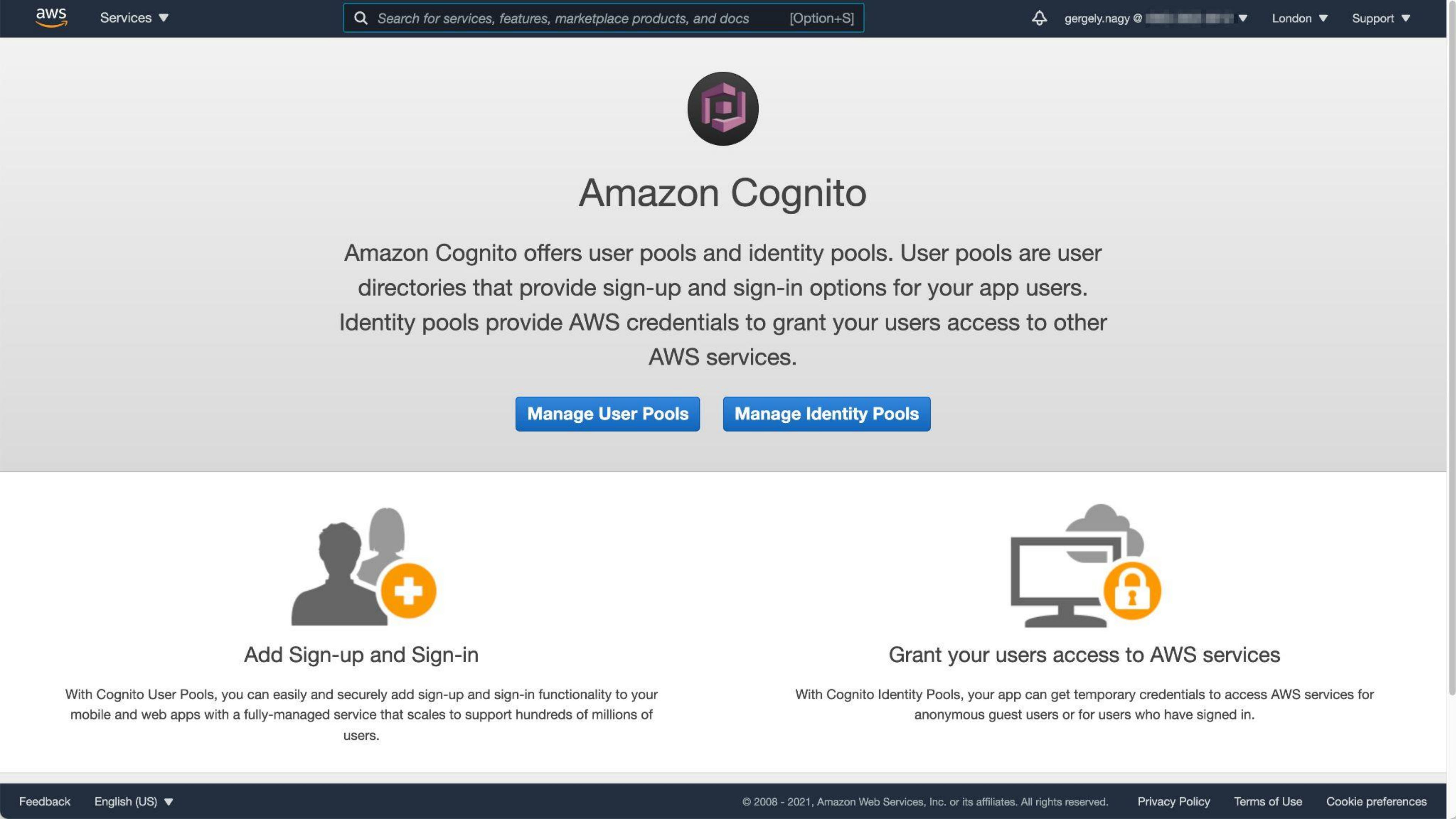
JSON Web Token

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
)
```

AWS Cognito



aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
gergely.nagy @ [redacted] ▼
London ▼
Support ▼

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.

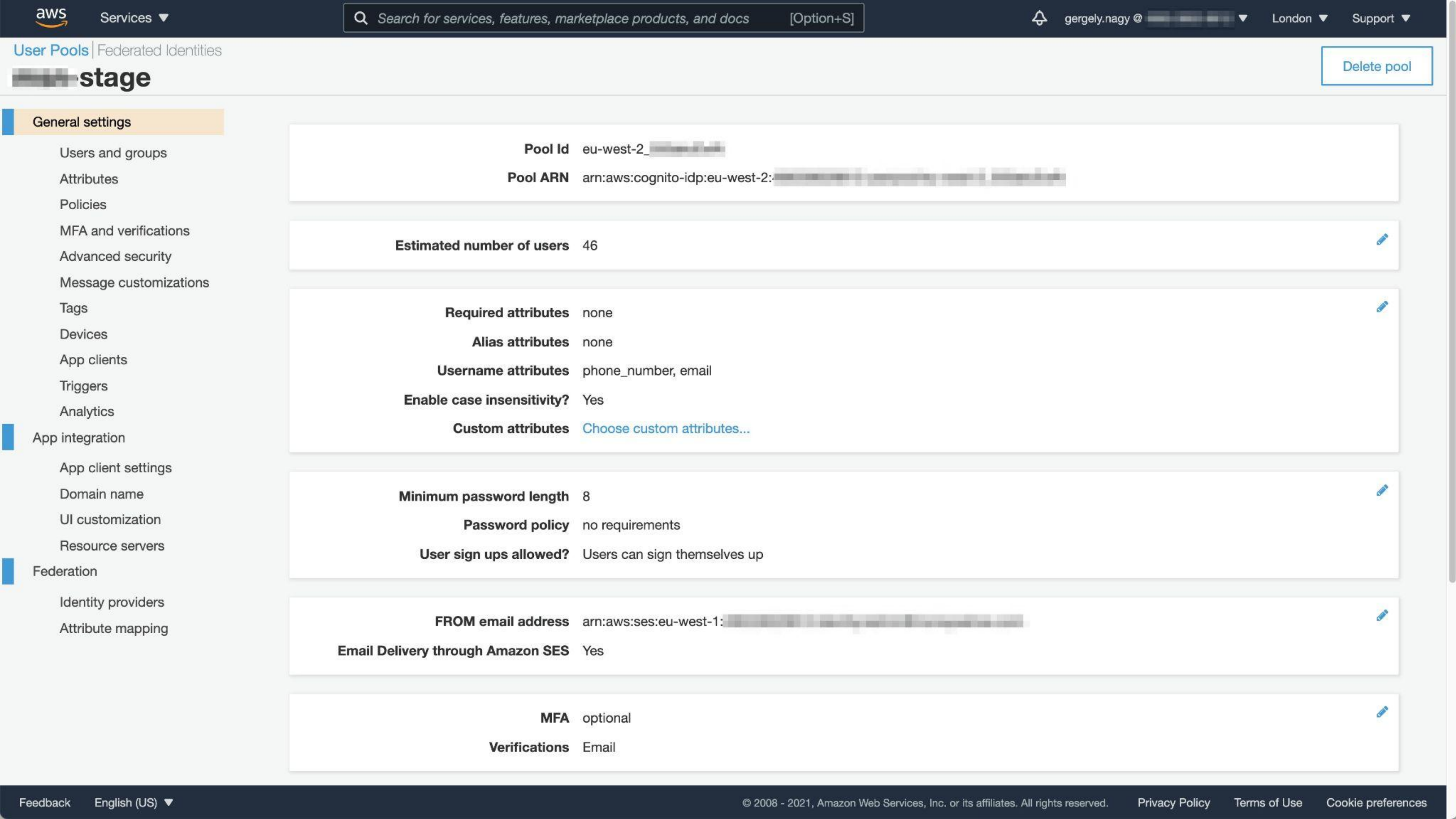
Manage User Pools
Manage Identity Pools

Add Sign-up and Sign-in

With Cognito User Pools, you can easily and securely add sign-up and sign-in functionality to your mobile and web apps with a fully-managed service that scales to support hundreds of millions of users.

Grant your users access to AWS services

With Cognito Identity Pools, your app can get temporary credentials to access AWS services for anonymous guest users or for users who have signed in.



[redacted]stage

Pool Id eu-west-2_[redacted]

Pool ARN arn:aws:cognito-idp:eu-west-2:[redacted]

Estimated number of users 46

Required attributes none

Alias attributes none

Username attributes phone_number, email

Enable case insensitivity? Yes

Custom attributes Choose custom attributes...

Minimum password length 8

Password policy no requirements

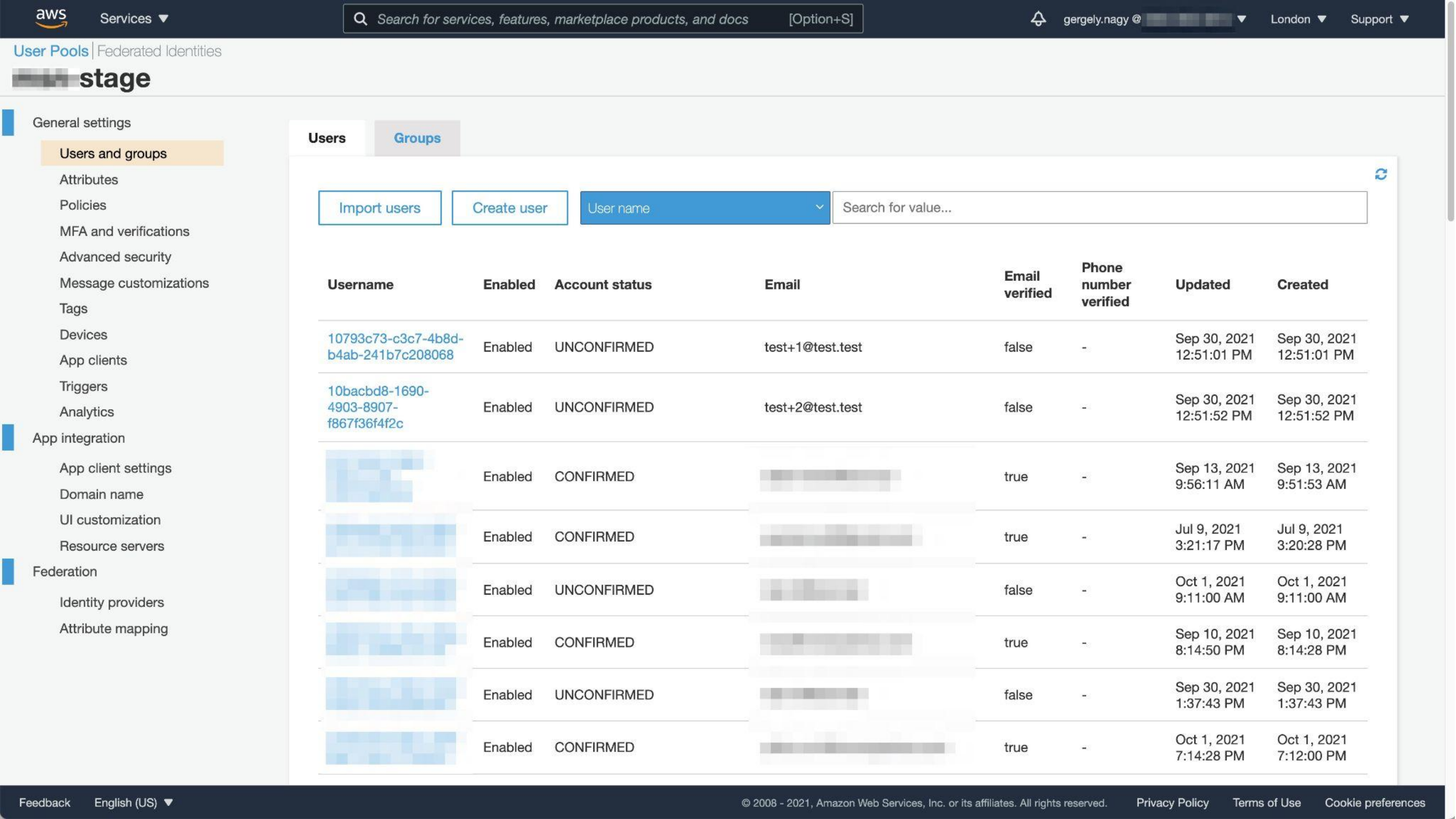
User sign ups allowed? Users can sign themselves up

FROM email address arn:aws:ses:eu-west-1:[redacted]

Email Delivery through Amazon SES Yes

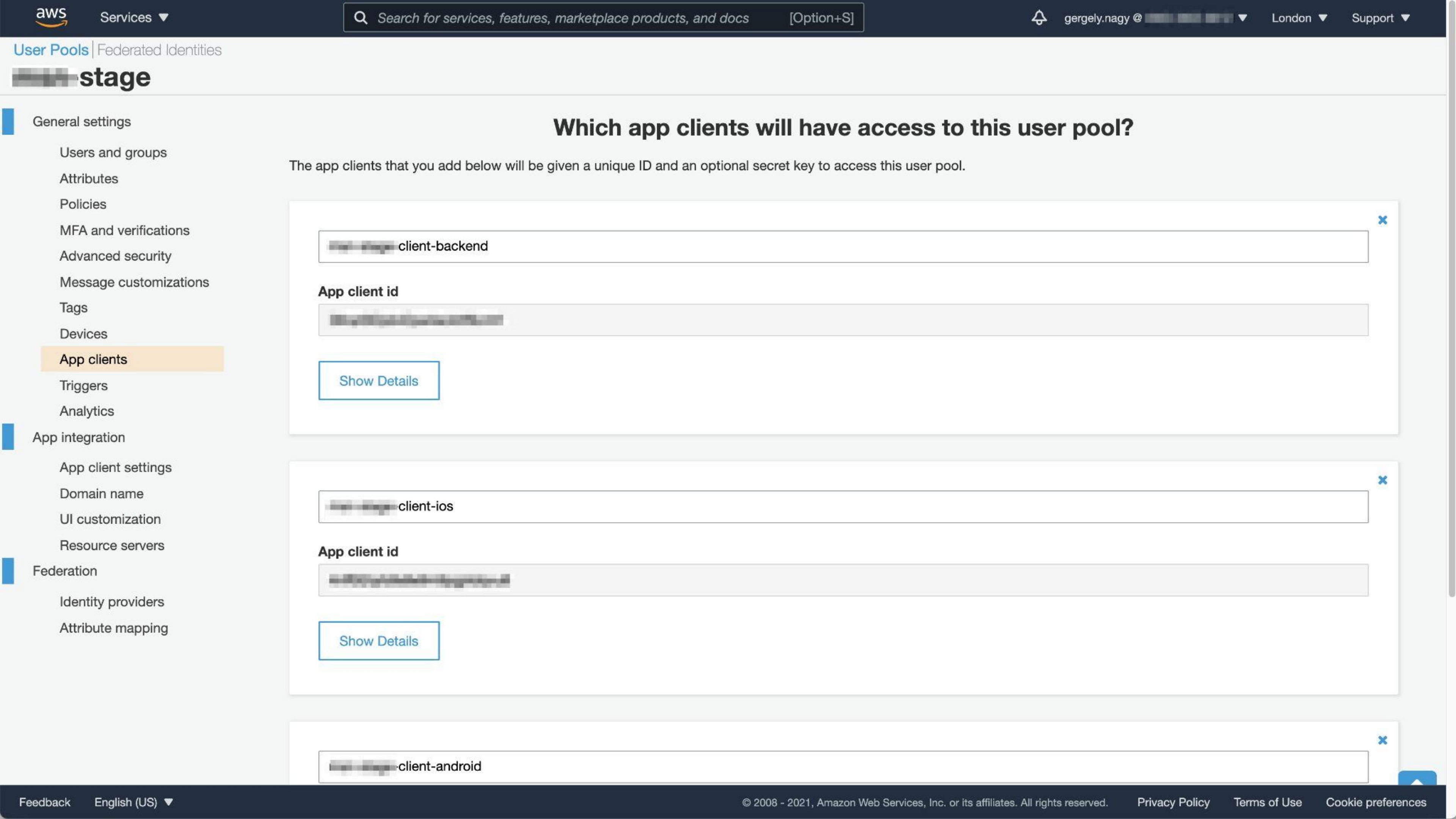
MFA optional

Verifications Email



[redacted] stage

Username	Enabled	Account status	Email	Email verified	Phone number verified	Updated	Created
10793c73-c3c7-4b8d-b4ab-241b7c208068	Enabled	UNCONFIRMED	test+1@test.test	false	-	Sep 30, 2021 12:51:01 PM	Sep 30, 2021 12:51:01 PM
10bacbd8-1690-4903-8907-f867f36f4f2c	Enabled	UNCONFIRMED	test+2@test.test	false	-	Sep 30, 2021 12:51:52 PM	Sep 30, 2021 12:51:52 PM
[redacted]	Enabled	CONFIRMED	[redacted]	true	-	Sep 13, 2021 9:56:11 AM	Sep 13, 2021 9:51:53 AM
[redacted]	Enabled	CONFIRMED	[redacted]	true	-	Jul 9, 2021 3:21:17 PM	Jul 9, 2021 3:20:28 PM
[redacted]	Enabled	UNCONFIRMED	[redacted]	false	-	Oct 1, 2021 9:11:00 AM	Oct 1, 2021 9:11:00 AM
[redacted]	Enabled	CONFIRMED	[redacted]	true	-	Sep 10, 2021 8:14:50 PM	Sep 10, 2021 8:14:28 PM
[redacted]	Enabled	UNCONFIRMED	[redacted]	false	-	Sep 30, 2021 1:37:43 PM	Sep 30, 2021 1:37:43 PM
[redacted]	Enabled	CONFIRMED	[redacted]	true	-	Oct 1, 2021 7:14:28 PM	Oct 1, 2021 7:12:00 PM



[redacted]stage

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.

[redacted]client-backend

App client id

[redacted]

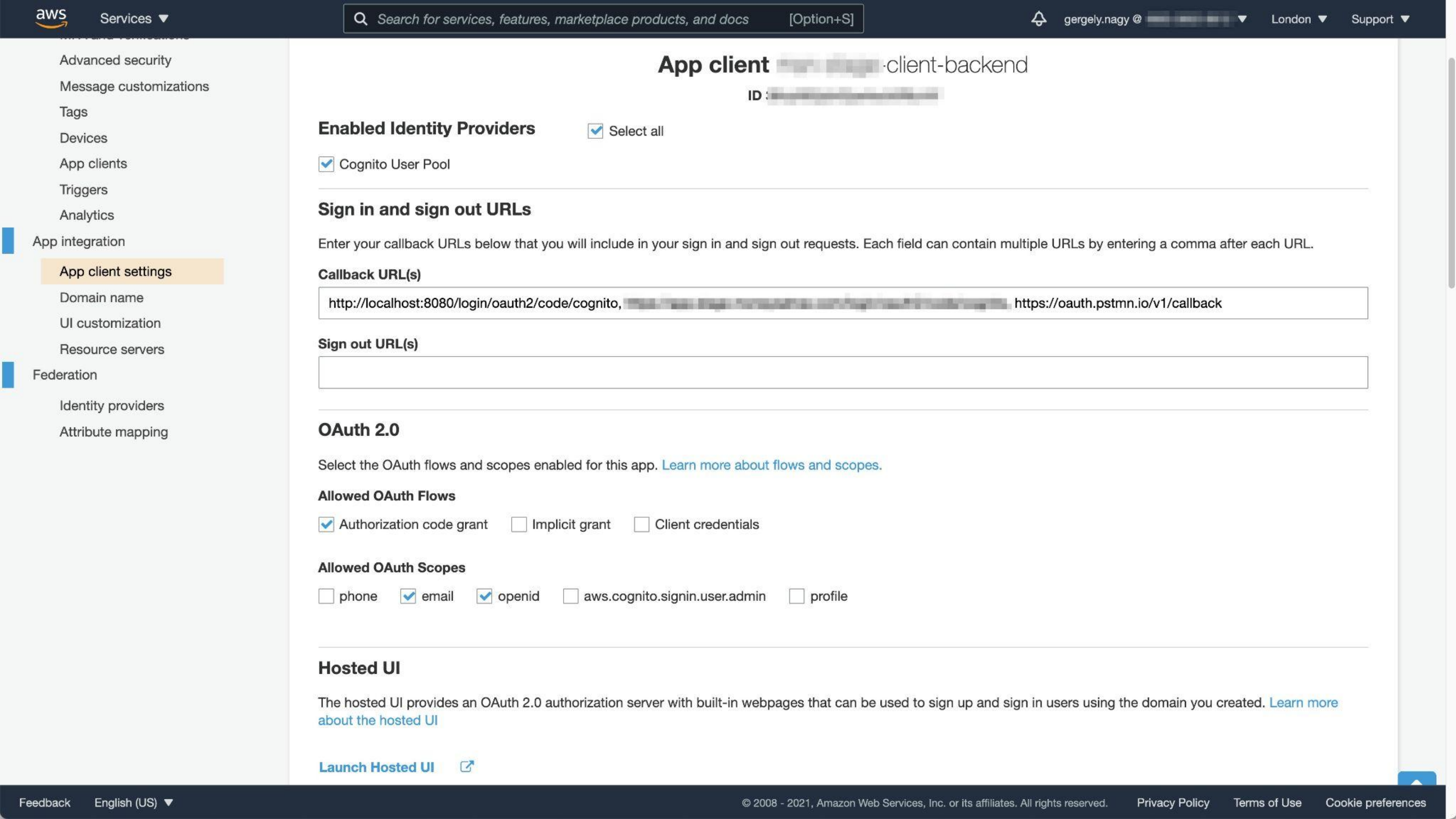
[redacted]client-ios

App client id

[redacted]

[redacted]client-android

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.


aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
gergely.nagy @ [redacted] ▼
London ▼
Support ▼

App client [redacted]-client-backend

ID : [redacted]

Enabled Identity Providers

☑ Select all

☑ Cognito User Pool

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)

http://localhost:8080/login/oauth2/code/cognito, [redacted] https://oauth.pstmn.io/v1/callback

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

Allowed OAuth Scopes

□ phone ☑ email ☑ openid □ aws.cognito.signin.user.admin □ profile

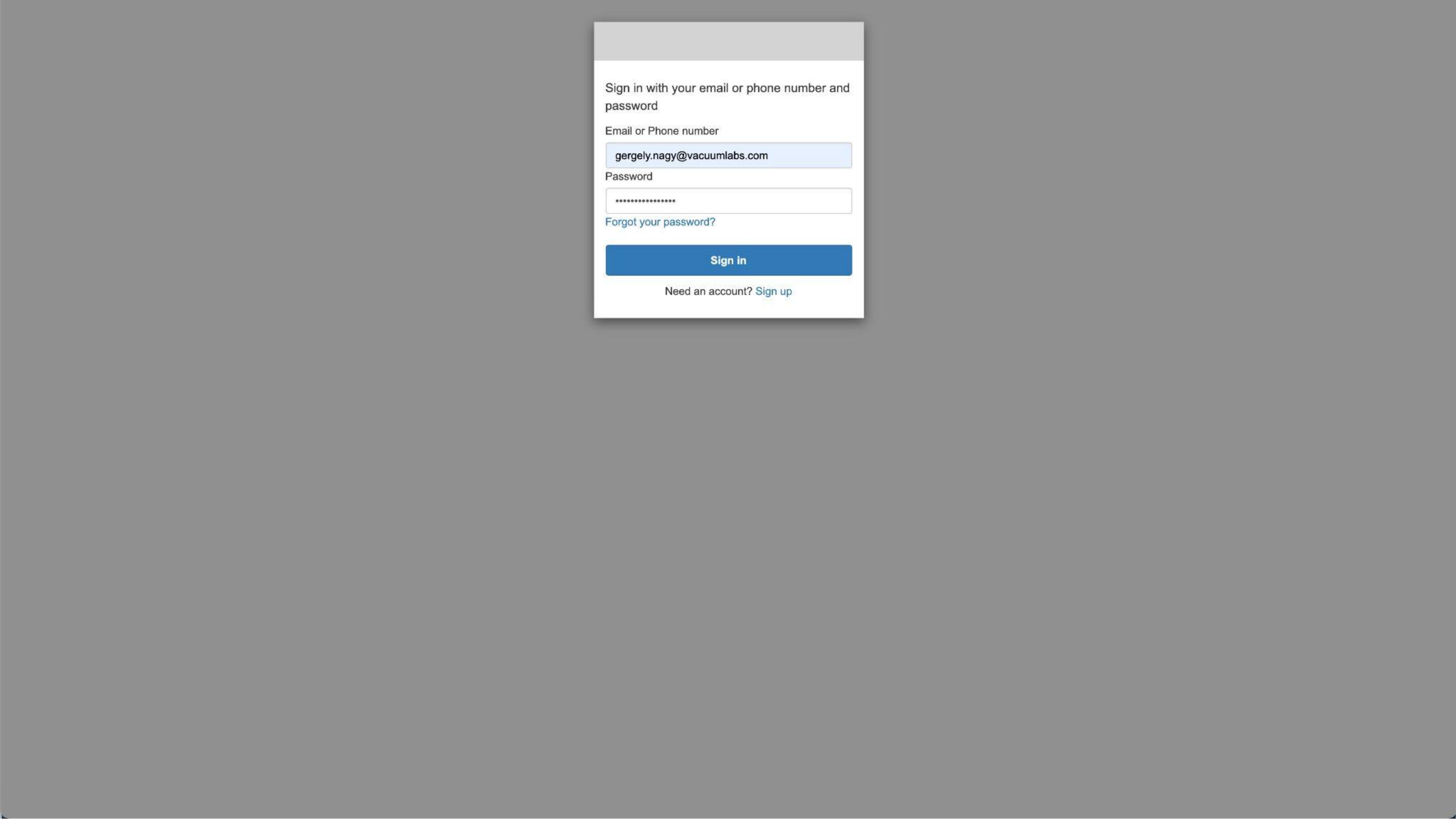
Hosted UI

The hosted UI provides an OAuth 2.0 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

Feedback
English (US) ▼
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences

Demo App



Sign in with your email or phone number and password

Email or Phone number

gergely.nagy@vacuumlabs.com

Password

••••••••••••••••

```yaml
spring:
 security:
   oauth2:
     resourceserver:
       jwt:
         issuer-uri: https://cognito-idp.eu-west-2.amazonaws.com/eu-west-*******
```

```yaml
spring:
 security:
   oauth2:
     resourceserver:
       jwt:
         issuer-uri: https://cognito-idp.eu-west-2.amazonaws.com/eu-west-*******
     client:
       registration:
         cognito:
           provider: cognito
           client-id: *************
           client-authentication-method: none
           authorization-grant-type: authorization_code
           redirect-uri: "{baseUrl}/login/oauth2/code/{registrationId}"
           scope: openid
       provider:
         cognito:
           issuer-uri: https://cognito-idp.eu-west-2.amazonaws.com/eu-west-2_*******
           user-name-attribute: cognito:username
```

```
// https://cognito-idp.eu-west-2.amazonaws.com/eu-west-2_***/.well-known/openid-configuration
{
    "authorization_endpoint": "https://auth.****.com/oauth2/authorize",
    "id_token_signing_alg_values_supported": [
        "RS256"
    ],
    "issuer": "https://cognito-idp.eu-west-2.amazonaws.com/eu-west-2_***",
    "jwks_uri": "https://cognito-idp.eu-west-2.amazonaws.com/eu-west-2_***/.well-known/jwks.json",
    "response_types_supported": [
        "code",
        "token"
    ],
    "scopes_supported": [
        "openid",
        "email",
        "phone",
        "profile"
    ],
    "subject_types_supported": [
        "public"
    ],
    "token_endpoint": "https://auth.***.com/oauth2/token",
    "token_endpoint_auth_methods_supported": [
        "client_secret_basic",
        "client_secret_post"
    ],
    "userinfo_endpoint": "https://auth.***.com/oauth2/userInfo"
}
```

```
// https://cognito-idp.eu-west-2.amazonaws.com/eu-west-2_***/.well-known/jwks.json
{
   "keys": [
      {
         "alg": "RS256",
         "e": "AQAB",
         "kid": "**********=",
         "kty": "RSA",
         "n": "*******...",
         "use": "sig"
      },
      {
         "alg": "RS256",
         "e": "AQAB",
         "kid": "*******=",
         "kty": "RSA",
         "n": "*******...",
         "use": "sig"
      }
   ]
}
```

Cognito Pro / Contra

+ Egyszerű fellőni (főleg ha már használunk AWS-t)

+ Barátságos árazás

- Kicsit fapad

vacuumlabs

Q&A

gergely.nagy@vacuumlabs.com