

# Evolução na camada de autenticação de **API da Neoway**

## Utilizando Go



# Rafael Mateus

API Platform at Neoway



[linkedin.com/in/rafaelbmateus](https://www.linkedin.com/in/rafaelbmateus)

# AGENDA

- Neoway
- OAuth Neoway
- Protocolo OAuth2
- Usando Fosite SDK
- Usando Hydra
- Limitações
- Aprendizados

# NEOWAY

Empresa de **Big Data Analytics** e  
**Inteligência Artificial** para **negócios**

- Modelo de negócio Web e API

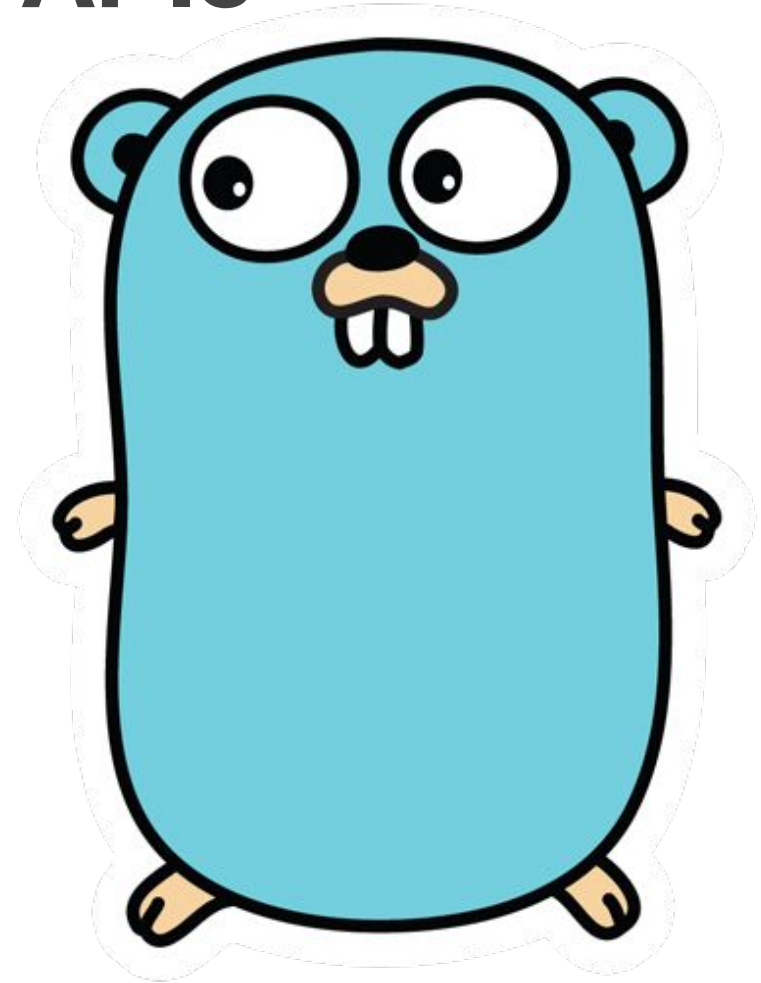


# OAuth Neoway

Como tudo começou...

## Primeira implementação de autenticação de APIs

POST - auth/token



Set/2016



# Obter um Token

Como obter um token  
de autenticação de API

POST - <https://api.neoway.com.br/oauth/token>

```
{  
  "application": "<application>",  
  "application_secret": "<secret>"  
}
```

# Retorno do Token

Como era o *body* do retorno do *token*

Status: 200 - OK

```
{  
  "token": "<token>"  
}
```



Autenticação - OK



# Consumir API

Como fazer uma chamada para uma API protegida

GET - <https://api.neoway.com.br/v1/data>

header: "Authorization: Bearer **<token>**"



Autorização - OK

# LIMITAÇÕES

Limitações do projeto inicial OAuth Neoway

- Informações sobre o token
  - Escopos de acesso
  - Informação de quando expira o token
- Não compatível com bibliotecas de autenticação no padrão de mercado

# OAuth2

## protocolo de autorização

**RFC6749** - The OAuth 2.0 Authorization Framework



# OAuth2 Grant Types

**Client  
Credentials**

**Authorization  
Code**

**PKCE**  
Proof Key for Code Exchange

**Device  
Code**

# OAuth2 Grant Types

**Client  
Credentials**

**Authorization  
Code**

**PKCE**

Proof Key for Code Exchange






**Device  
Code**






# Como implementar o protocolo **OAuth2 ???**












# Fosite


 Search or jump to...  [Pulls](#) [Issues](#) [Marketplace](#) [Explore](#)   

 [ory / fosite](#) Public  [Sponsor](#)  [Watch](#) 45  [Fork](#) 259  [Starred](#) 1.9k

[Code](#) [Issues](#) 20 [Pull requests](#) 5 [Actions](#) [Security](#) 4 [Insights](#)


 master  [Go to file](#)  [Add file](#) [Code](#)

 [aeneasr](#) chore: update repository te...   6 days ago  727

 .circleci


Revert "chore: delete .circleci fo...

8 days ago

 .github

chore: update repository templa...

6 days ago

 compose

chore: format using Make (#703)

8 days ago

## About

Extensible security first OAuth 2.0 and OpenID Connect SDK for Go.

 [www.ory.sh/?utm\\_source=github...](http://www.ory.sh/?utm_source=github...)

[golang](#) [security](#) [oauth](#) [library](#)

[oauth2](#) [sdk](#) [authentication](#)

Seguindo as RFCs

**RFC6749** - The OAuth 2.0  
Authorization Framework

**RFC6819** - OAuth 2.0 Threat  
Model and Security  
Considerations



# ● Primeira release

Fosite SDK


Pre-release

v0.1.0

6c40c08

Compare ▼

## 0.1.0

 aeneasr released this on Aug 3, 2016

oauth2: implicit handlers do not require tls over https (#61)

closes #60

# • IMPLEMENTAMOS

e ficamos felizes com o padrão **OAuth2**



nossos clientes também...

# E como ficou o rolê?



# Obter um Token

Como obter um token  
de autenticação de API  
**OAuth2**

POST - <https://api.neoway.com.br/oauth2/token>

```
{  
  "client_id": "<client_id>",  
  "client_secret": "<secret>",  
  "scope": "<scope>"  
}
```

# Retorno do Token

Retorno do token

OAuth2

Status: 200 - OK

```
{  
  "access_token": "<token>",  
  "expires_in": 1800,  
  "scope": "clients.read",  
  "token_type": "bearer"  
}
```





Autenticação - OK

# Consumir API

Como fazer uma chamada para uma API protegida

GET - <https://api.neoway.com.br/clients/2>

header: "Authorization: Bearer **<token>**"



Autorização - OK

# LIMITAÇÕES


Limitações do projeto com o Fosite

- Implementações e evoluções:
  - Handlers
  - Logs
  - Struct das entidades
  - Migrações de banco de dados
- Apenas usando o **client credentials** flow




**E agora?**  
Qual será o próximo passo?





# Hydra





[Pulls](#) [Issues](#) [Marketplace](#) [Explore](#)


  

 [ory / hydra](#) Public


 [Sponsor](#)

 [Watch](#) 226


 [Fork](#) 1.3k


 [Starred](#) 13.1k


[Code](#) [Issues](#) 63 [Pull requests](#) 24 [Discussions](#) [Actions](#) [Security](#) 2

 master

[Go to file](#) [Add file](#) [Code](#)

 [kevgo](#) chore: remove double tabs fr... 2 days ago 3,418

 .docker-home 0.1-beta 6 years ago



 docker fix: docker image build (#3247) 22 days ago

## About

OpenID Certified™ OpenID Connect and OAuth Provider written in Go - cloud native, security-first, open source API security for your infrastructure.



# DOCUMENTAÇÃO

[Documentation](#)[API reference](#)[SDKs](#)[Examples](#)[Open source](#)[Website](#)[Discussions](#)[Slack](#)[GitHub](#)[OAuth2 & OpenID Connect \(Ory Hydra\)](#) [Introduction](#) [Introduction](#)[5 minute tutorial](#)[Installation](#)[Concepts](#) [Guides](#) [OAuth2 & OpenID Connect \(Ory Hydra\)](#)  [Introduction](#)  [Introduction](#)

## Introduction

Hydra is an OAuth 2.0 and OpenID Connect Provider. In other words, an implementation of the OAuth 2.0 Authorization Framework as well as the OpenID Connect Core 1.0 framework. As such, it issues OAuth 2.0 Access, Refresh, and ID Tokens that enable third-parties to access your APIs in the name of your users.





# E como ficou o rolê?



# Obter um Token

Como obter um token  
de autenticação de API  
**OAuth2**

POST - <https://api.neoway.com.br/oauth2/token>

```
{  
  "client_id": "<client_id>",  
  "client_secret": "<secret>",  
  "scope": "<scope>"  
}
```

# Retorno do Token

Retorno do token

OAuth2

Status: 200 - OK

```
{  
  "access_token": "<token>",  
  "expires_in": 1800,  
  "scope": "clients.read",  
  "token_type": "bearer"  
}
```



Autenticação - OK

# Consumir API

Como fazer uma chamada para uma API protegida

GET - <https://api.neoway.com.br/clients/2>

header: "Authorization: Bearer **<token>**"



Autorização - OK

# Sem quebrar o contrato de API!





# Aprendizados



## APRENDIZADOS

Aprendemos mais sobre  
**OAuth2**

## APRENDIZADOS

OAuth2 e OpenID Connect  
são **protocolos difíceis**

## APRENDIZADOS

Não precisamos reescrever  
todos os **fluxos padrão**

## APRENDIZADOS

O crescimento do **Go** e da  
**comunidade**

## APRENDIZADOS

... e que a luta do **dev**  
**não costuma acabar**  
tão cedo ...



**@rafaelbmateus**

API Engineer | Tech Lead |


Golang | Neoway | Uma empresa B3

• **Obrigado!**

# Perguntas?







# PODER PARA SUAS DECISÕES

Serviços de dados confiáveis em um só lugar. Feito pra você,  
por quem mais entende de inteligência e negócios no Brasil.