Creating a Google authentication service with users stored in own database in Golang

Ask Question

Asked 2 years, 5 months ago Active 2 years, 5 months ago Viewed 319 times

1

First step in creating my new suite of react frontend applications is to make a simple Authentication server/service in Go preferably, where users can authenticate with their google account which will either result in:

- creation a new user in the database
- login if matching user is found in db (how to determine match without password?)

I realize that I will get a JWT from the Auth server/service with the usual claims such as:

```
{
    "iss":"accounts.google.com",
    "at_hash":"HK6E_P6Dh8Y93mRNtsDB1Q",
    "email_verified":"true",
    "sub":"107691503500661507151130823 67",
    "azp":"1234987819200.apps.googleusercontent.com",
    "email":"jsmith@example.com",
    "aud":"1234987819200.apps.googleusercontent.com",
    "iat":1353601026,
    "exp":1353604926,
    "nonce": "0394852-3190485-2490358",
    "hd":"example.com"
}
```

So far so good, but after that I'm not really sure what fields I need to store for the user "table" (using a dgraph db, but I guess it doesn't matter if it's a relational or graph db) in the database other than the email, which will to my understanding be the identifier pairing the user in db with the JWT?

How do you handle integration with your own database:

1. First time a user authenticates with google through the auth server/service and a user is created in the db
2. Subsequent times a user authenticates with google through the same auth server/service and logs in (already exists in db - but how to verify this in a safe way - couldn't others just make a false token with the same email?)

Do you store the token in the user table along with the email? In that case what to do if the token expires/changes and what about security?

So the question is not about how to get a token, it's about how to connect the user in the db with the JWT user that just got authenticated.

Most tutorials and articles I've read does not describe the database part in much detail.

go oauth-2.0 jwt openid-connect

share improve this question follow edited Jun 28 '18 at 19:29 asked Jun 28 '18 at 19:17 Dac0d3r 1,541 3 29 52

Not marking for closure since there's a lot here, but "recommendation regarding libs" is specifically off-topic for Stack Overflow. – Adrian Jun 28 '18 at 19:19

Sorry you're right. Deleted it. – Dac0d3r Jun 28 '18 at 19:29

It really depends on what information you need about users. If you need to remember permissions, preferences, whatever, store that. Otherwise just an email should do until you need more. – Fishdigger Jun 28 '18 at 19:37

I can easily query for groups, roles and permissions or whatever in the graph database afterwards and put it in redux. I'm not a fan of putting unnecessary stuff in jwt. It's the connection with the db that i'm interested in. – Dac0d3r Jun 28 '18 at 19:51

add a comment

1 Answer

Active Oldest Votes

1

Creation a new user in the database

In principle, you only really need to store the user's email (along with whatever other information your system needs internally for that user) to be able to 'link' your user with the "external" account they are using to login.

Login if matching user is found in db (how to determine match without password?)

One of the main reasons to rely on an external authentication mechanism is that you don't need to perform any password storage/validation yourself.

You just need to match the email the user is using to authenticate with the email you have stored in your DB.

Couldn't others just make a false token with the same email?

No, they cannot, otherwise this would not be useful at all.

Tokens are signed by the authentication server, and it is not possible to "sign" the token without having the authentication server's private key.

How to verify this in a safe way

See here: https://developers.google.com/identity/sign-in/web/backend-auth

Section "Verify the integrity of the ID token" discusses how you do this either by yourself or by calling an external endpoint.

Do you store the token in the user table along with the email?

You only need to store the user's token if besides authenticating them you plan to use Google's APIs on behalf of the user.

In that case what to do if the token expires/changes and what about security?

See here: https://developers.google.com/identity/protocols/OAuth2

You will need to store both a token and a refresh token, and there is a flow to follow in order to refresh it.

About security, you need to make sure no user is able to see other user's token, since the token enables an application to make requests to the API on behalf of that user.

share improve this answer follow answered Jun 28 '18 at 19:51 eugenioy 9,749 15 25

Thanks for listing up and answering all my questions ;-). – Dac0d3r Jun 29 '18 at 9:04

One more question. Since you say the email is used for creating the user in the database or "linking" an already existing user after a login, is it correctly understood that OpenID will not be sufficient, since the JWT received from OpenID does not contain email info? I only need one key to identify the user in the database - and then I will fetch (from the db) the user info I need into redux or whatever state management solution. So that leaves OpenID Connect and OAuth2? I only want the minimum user info in JWT that I need to match it against that same user in the database, so which is best? – Dac0d3r Jun 29 '18 at 10:05

@Dac0d3r: this link describes the same flow for OpenID: developers.google.com/identity/protocols/OpenIDConnect, take a look at the "Obtain user information from the ID token" section. – eugenioy Jun 29 '18 at 15:16

add a comment

Your Answer

Sign up or log in

Sign up using Google

Sign up using Facebook

Sign up using Email and Password

Post as a guest

Name

Email

Required, but never shown

Post Your Answer

By clicking "Post Your Answer", you agree to our terms of service, privacy policy and cookie policy

Not the answer you're looking for? Browse other questions tagged go oauth-2.0 jwt openid-connect or ask your own question.

The Overflow Blog
How to write an effective developer resume: Advice from a hiring manager
Podcast 290: This computer science degree is brought to you by Big Tech

Featured on Meta
"Question closed" notifications experiment results and graduation
MAINTENANCE WARNING: Possible downtime early morning Dec 2/4/9 UTC (8:30PM…
Congratulations VonC for reaching a million reputation

Related
60 Service Applications and Google Analytics API V3: Server-to-server OAuth2 authentication?
15 Google oAuth 2.0 (JWT token request) for Service Application
461 Invalidating JSON Web Tokens
0 different payload from google oauth2 response causes json error
0 AppIdentityError: Wrong recipient while verifying Bearer token
0 Google identity toolkit token validation exception with .NET JSON web token handler
118 Single sign-on flow using JWT for cross domain authentication
2 Not getting user identity in JWT used in OAuth2 access token from ADFS 3.0
2 JWT access tokens: a contradiction?
0 How to use Google Speech API in an end user c# application securely after Authenticating them with Firebase Auth?

Hot Network Questions
Va, pensiero, sull'ali dorate – in Latin?
What happens if my Zurich public transportation ticket expires while I am traveling?
Why does my IT block Firefox?
Why are most helipads in São Paulo blue coated and identified by a "P"?
Do multiple routers increase security?
What inner tube to buy for 47 tire size, 650bx47c tires?
How much do propellers stutter?
Why do some languages have genders and some don't?
When and why did the use of the lifespans of royalty to limit clauses in contracts come about?
What does "Ф" as an independent verb means?
Unusual or archaic usage of "young"
How can a hard drive provide a host device with file/directory listings when the drive isn't spinning?
BJT and signal source
Connecting an axle to a stud on the ground for railings
How to highlight "risky" action by its icon, and make it stand out from other icons?
Is Descriptive Complexity dead?
Can the Battle Master fighter's Precision Attack maneuver be used on a melee spell attack?
Joining Tikz paths seamlessly
Density of States of Supercells
Why did the 8087 need a special socket?
Merging values into an object
How easy it is to actually track another person credit card?
Concatenating `s///` in raku
Prevent sagging shelves in alcove
Question feed

site design / logo © 2020 Stack Exchange Inc; user contributions licensed under cc by-sa, rev 2020.11.30.38071