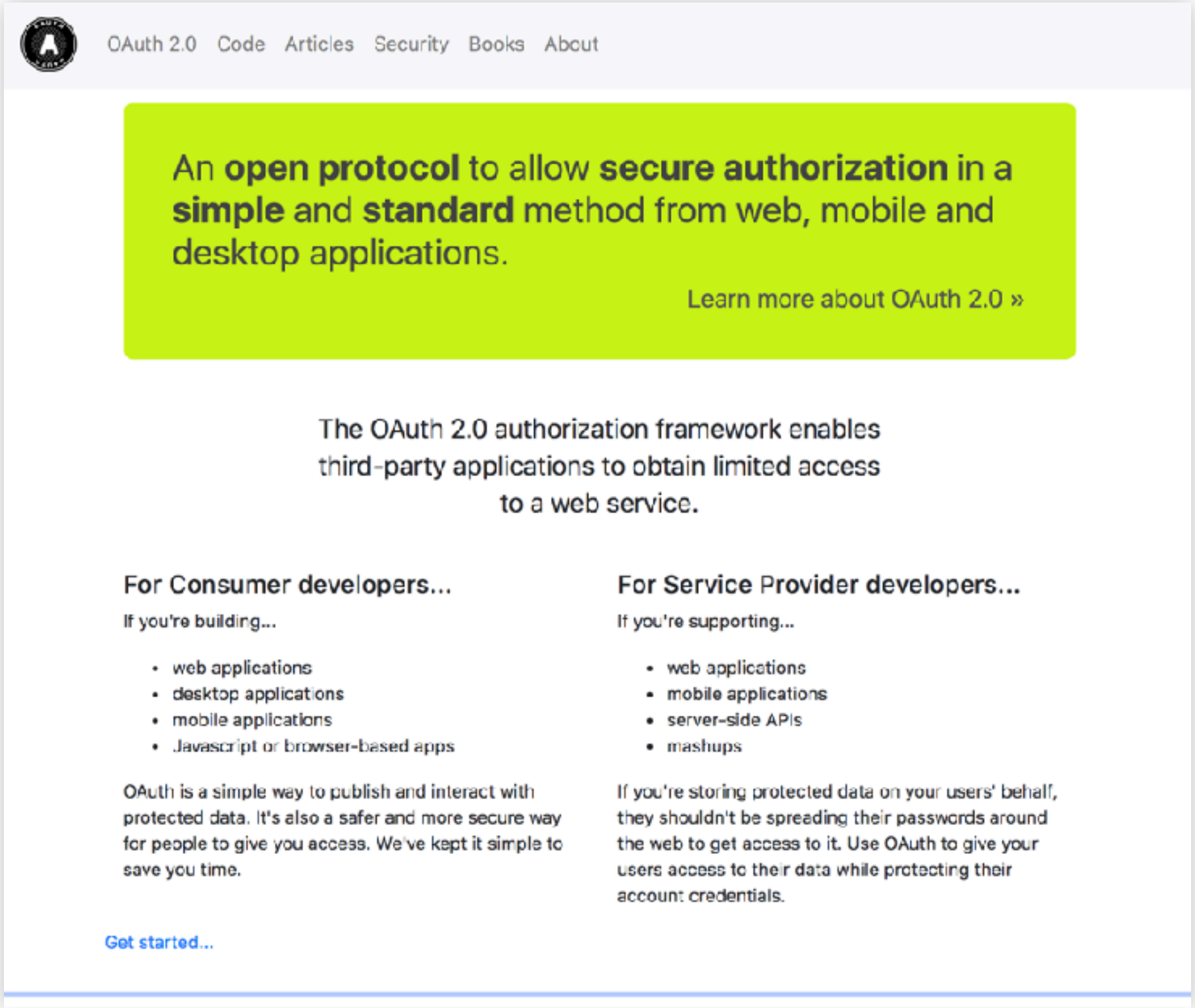
ADD AUTHENTICATION TO ANY APPLICATION

Aaron Parecki • @aaronpk • aaronpk.com

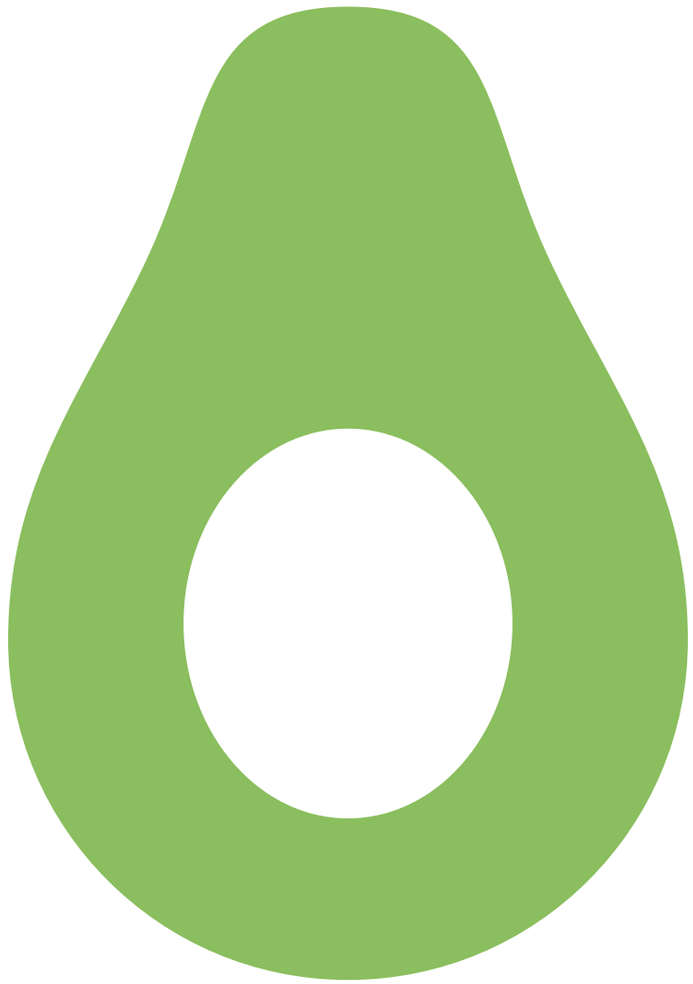
Developer Advocate at Okta • @oktadev

oauth.net



@aaronpk

oauth2simplified.com



avocado.lol

@aaronpk

avocado.lol

avocado.lol

wiki.avocado.lol

avocado.lol

Public Internet

Private Network

wiki.avocado.lol

avocado.lol

wiki.avocado.lol

User Database

Public Internet

avocado.lol

wiki.avocado.lol

User Database

stats.avocado.lol

avocado.lol

wiki.avocado.lol

User Database

stats.avocado.lol

.htpasswd

avocado.lol

wiki.avocado.lol

User Database

stats.avocado.lol

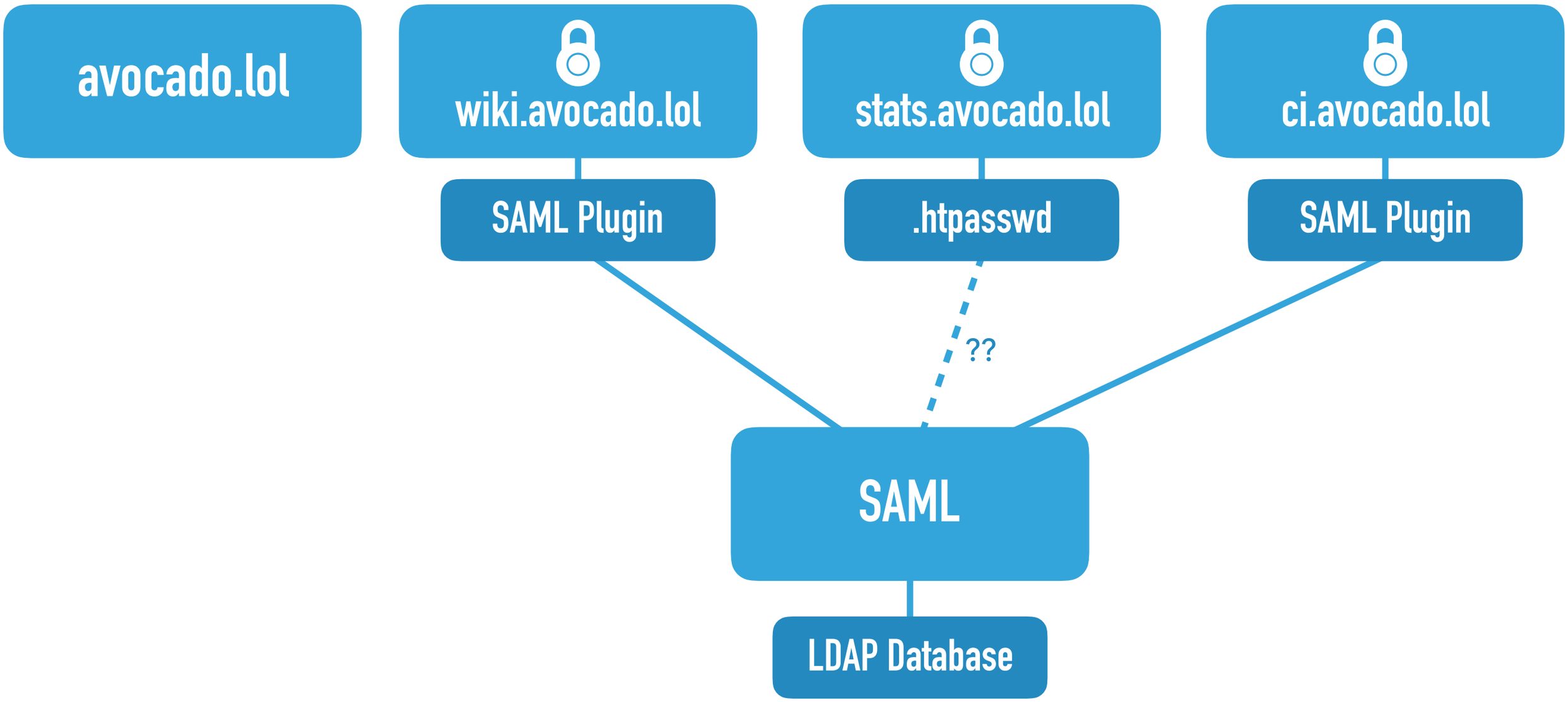
.htpasswd

ci.avocado.lol

GitHub Auth

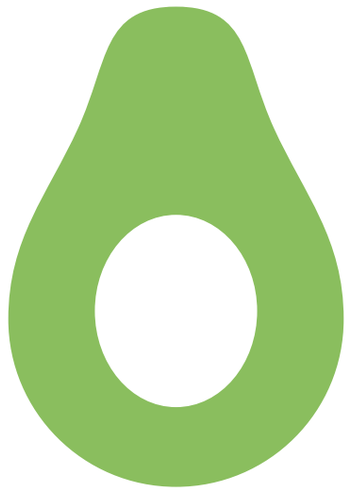
USER MANAGEMENT

- Add the user to wiki account database
- Add password to .htpasswd file
- Add the user to the GitHub organization


avocado.lol
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol
SAML Plugin
.htpasswd
SAML Plugin
??
SAML
LDAP Database

@aaronpk

There must be a better way!



@aaronpk

ngx_http_auth_request_module

http://nginx.org/en/docs/http/ngx_http_auth_request_module.html

Module ngx_http_auth_request_module

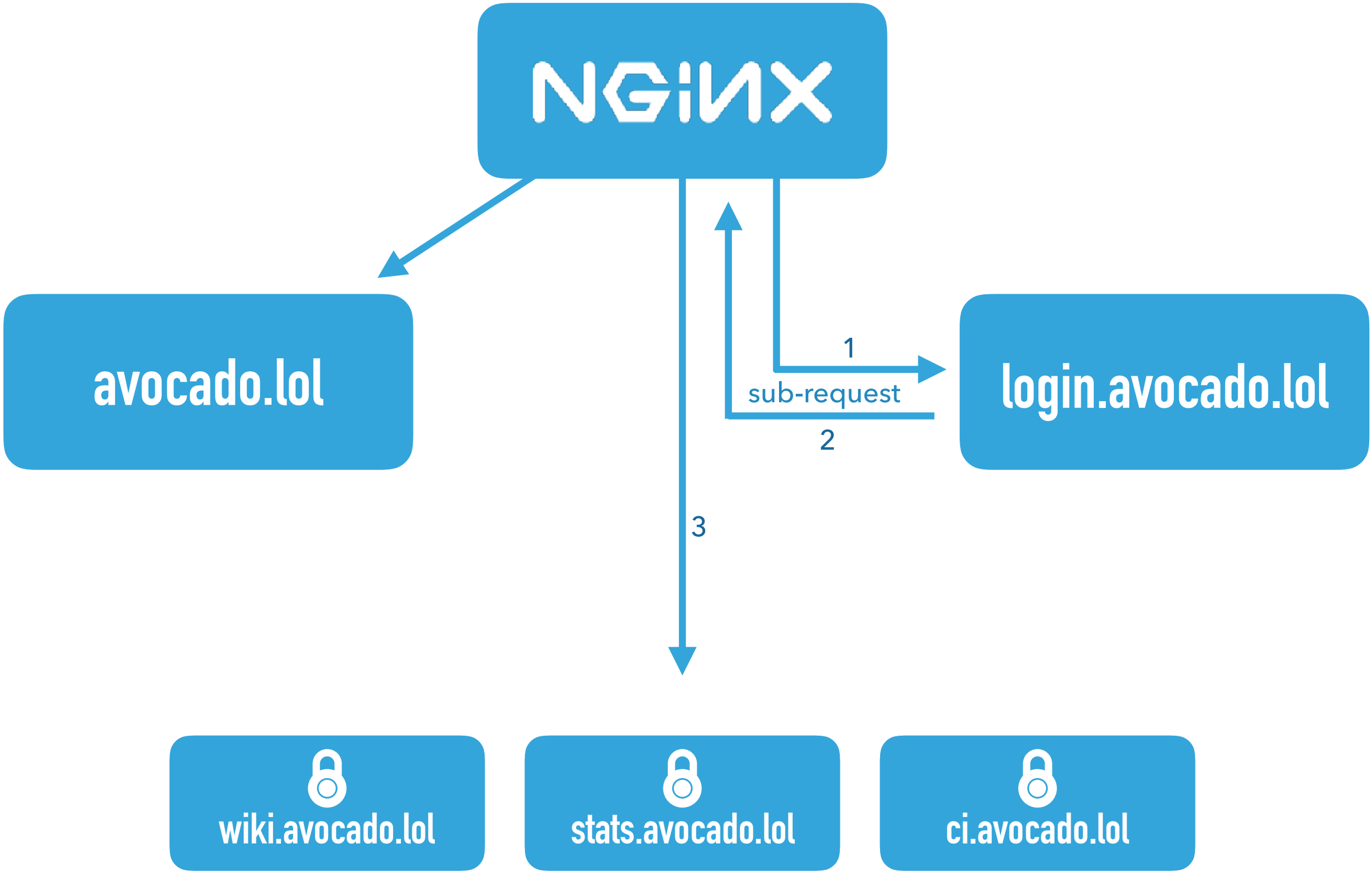
The `ngx_http_auth_request_module` module (1.5.4+) implements client authorization based on the result of a subrequest. If the subrequest returns a 2xx response code, the access is allowed. If it returns 401 or 403, the access is denied with the corresponding error code. Any other response code returned by the subrequest is considered an error.

For the 401 error, the client also receives the "WWW-Authenticate" header from the subrequest response.

This module is not built by default, it should be enabled with the `--with-http_auth_request_module` configuration parameter.

The module may be combined with other access modules, such as ngx_http_access_module, ngx_http_auth_basic_module, and ngx_http_auth_jwt_module, via the satisfy directive.

> Before version 1.7.3, responses to authorization subrequests could not be cached (using proxy_cache, proxy_store, etc.).


NGINX
avocado.lol
1
sub-request
2
login.avocado.lol
3
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol

@aaronpk

Enable the auth subrequest

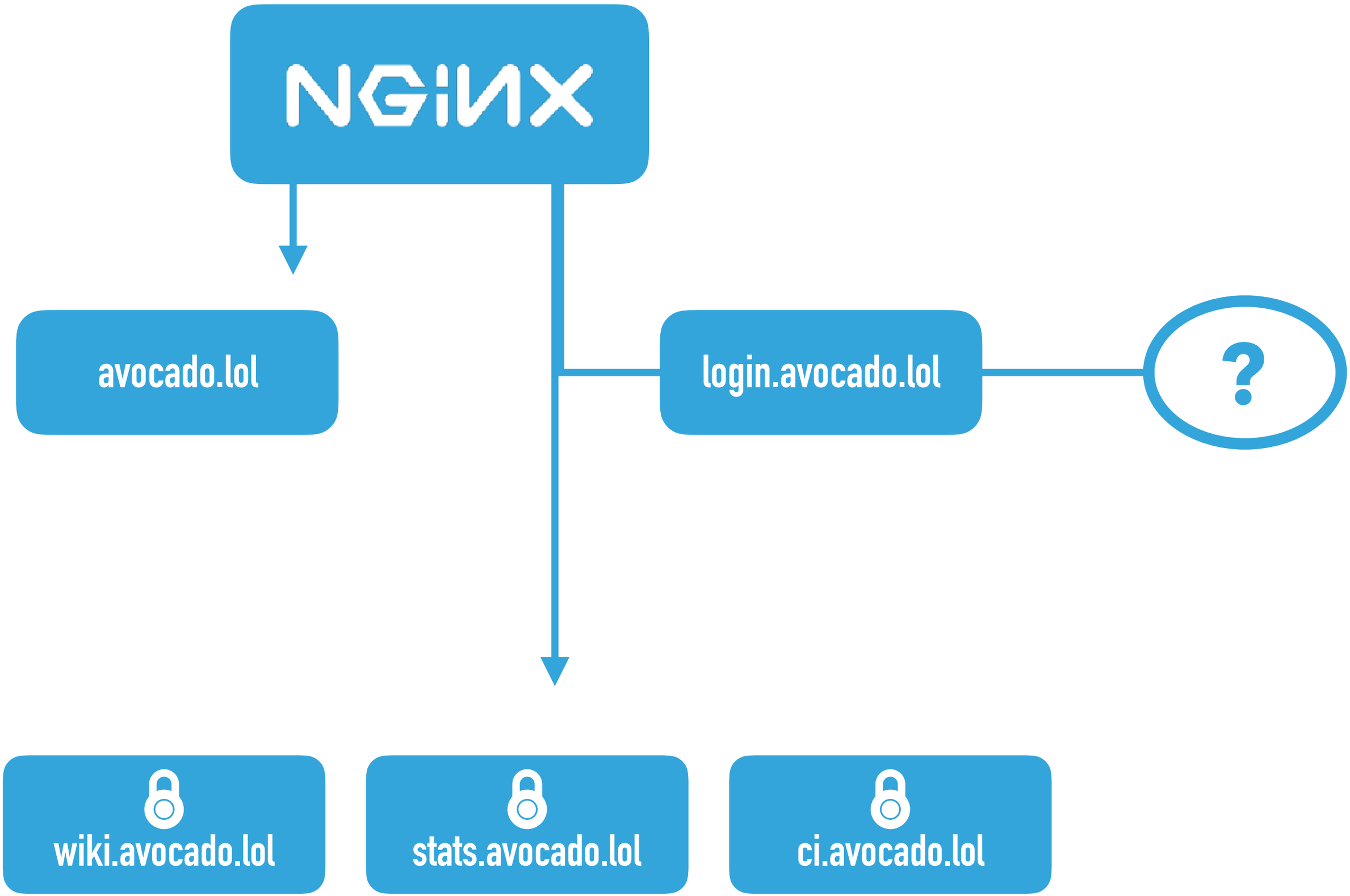
Send the subrequest to here

```
location / {
    auth_request /validate;
    ...
}
```

Pass the subrequest to this backend

We don’t care about the request body

```
location = /validate {
    proxy_pass ...
    proxy_pass_request_body off;
    proxy_set_header Content-Length "";
    proxy_set_header X-Original-URI $request_uri;
}
```


NGINX
avocado.lol
login.avocado.lol
?
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol

@aaronpk

LASSO

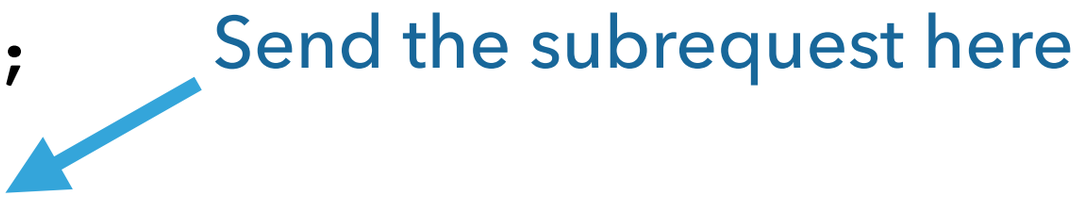
github.com/LassoProject

LASSO

- A microservice written in Go
- Supports a variety of OAuth/OIDC authentication mechanisms
- Configurable session cookie lifetime
- Handles the nginx auth_module subrequest, returning HTTP 200 or 401
- Uses a JWT cookie for fast and stateless verification

NGINX CONFIG

```
server {
  listen 443 ssl http2;
  server_name stats.avocado.lol;

  auth_request /lasso-validate;

    ...
}
```



```
server {
  listen 443 ssl http2;
  server_name stats.avocado.lol;

  auth_request /lasso-validate;

  auth_request_set $auth_user $upstream_http_x_lasso_user;

  location = /lasso-validate {
    proxy_pass http://127.0.0.1:9090/validate;
    proxy_pass_request_body     off;

    proxy_set_header Content-Length "";
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
```

This is the address that Lasso is listening on

```
    # these return values are passed to the @error401 call
    auth_request_set $auth_resp_jwt $upstream_http_x_lasso_jwt;
    auth_request_set $auth_resp_err $upstream_http_x_lasso_err;
    auth_request_set $auth_resp_failcount $upstream_http_x_lasso_failcount;
  }

  error_page 401 = @error401;

  location @error401 {
   return 302 https://login.avocado.lol/login?url=
     https://$http_host$request_uri&lasso-failcount=$auth_resp_failcount
     &X-Lasso-Token=$auth_resp_jwt&error=$auth_resp_err;
  }
}
```

When Lasso says they are not logged in, redirect to the login URL

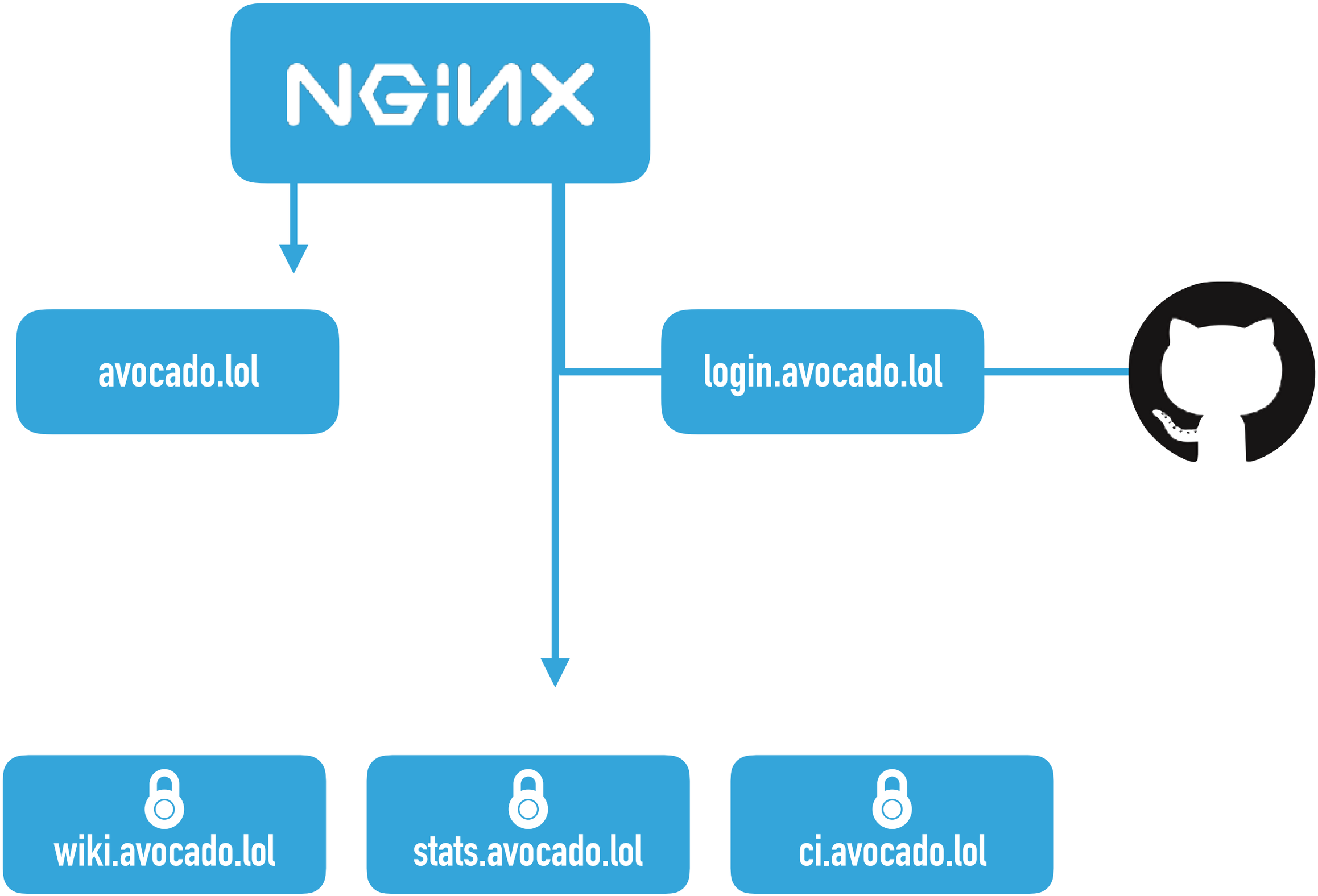
@aaronpk

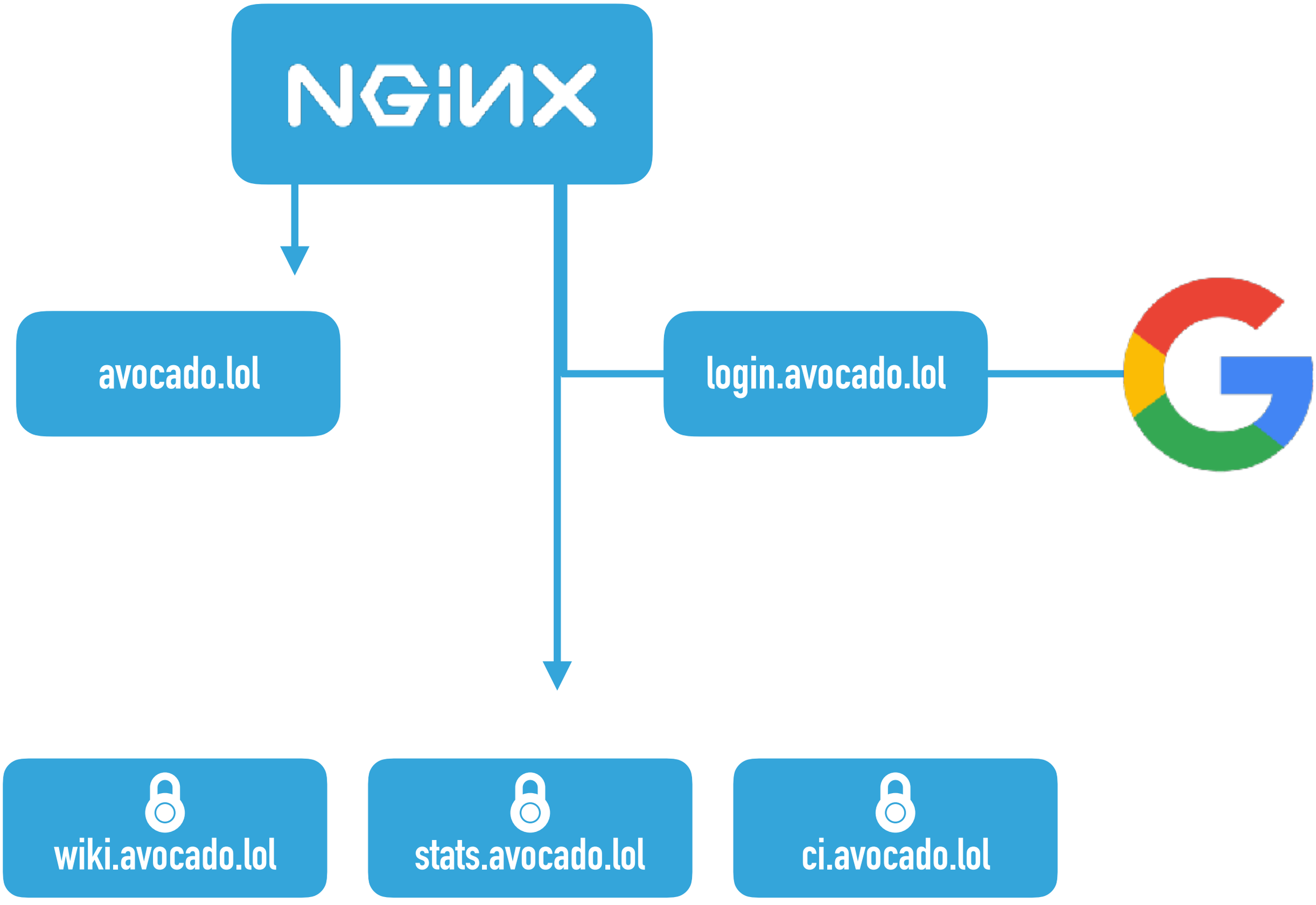
NGINX CONFIG

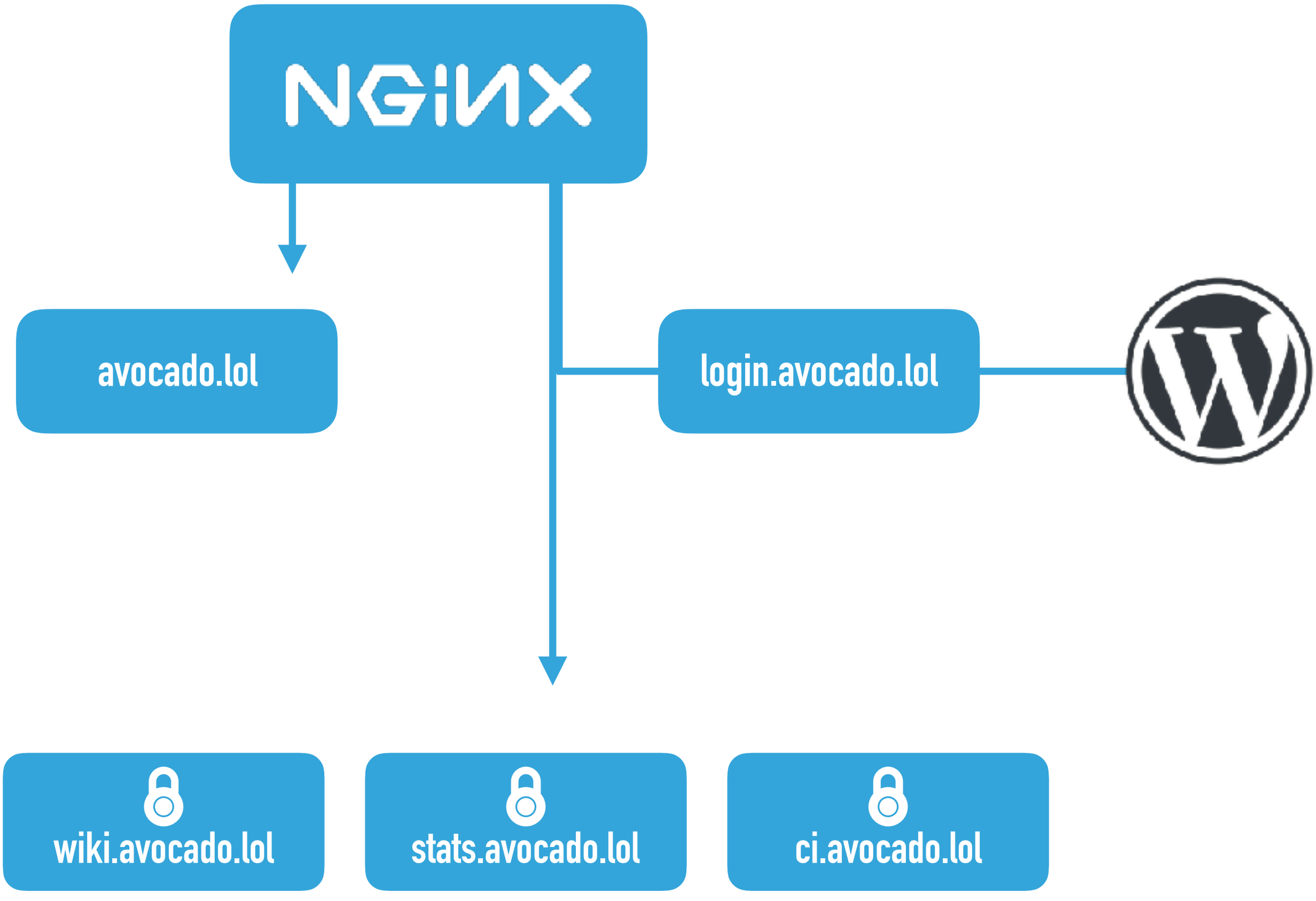
The public hostname of the Lasso server

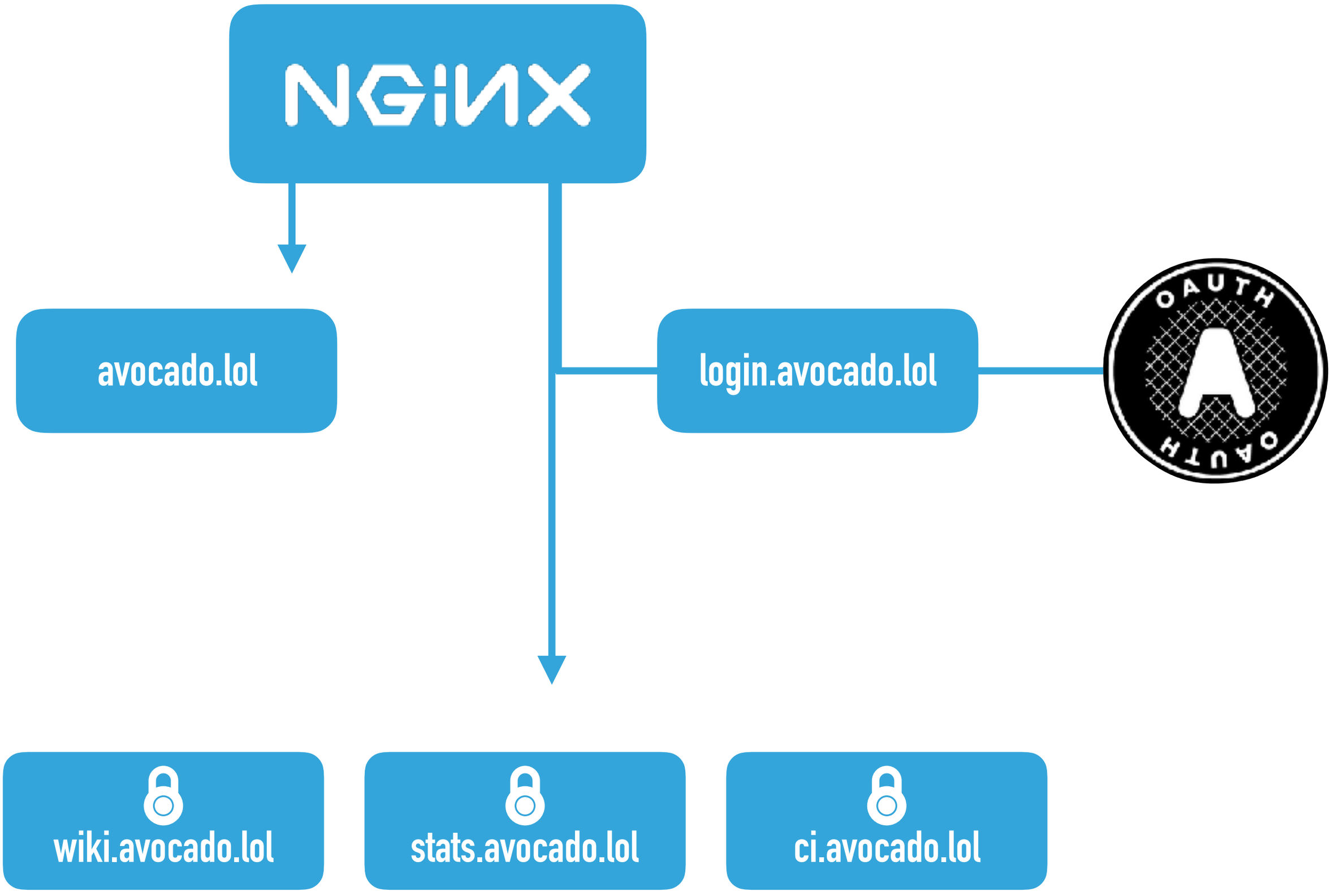
```
server {
  listen 443 ssl http2;
  server_name login.avocado.lol;

  ssl_certificate /etc/letsencrypt/live/login.avocado.lol/fullchain.pem;
  ssl_certificate_key /etc/letsencrypt/live/login.avocado.lol/privkey.pem;

  # Proxy to your Lasso instance
  location / {
    proxy_set_header  Host  login.avocado.lol;
    proxy_set_header  X-Forwarded-Proto https;
    proxy_pass        http://127.0.0.1:9090;
  }
}
```

This is the address that Lasso is listening on

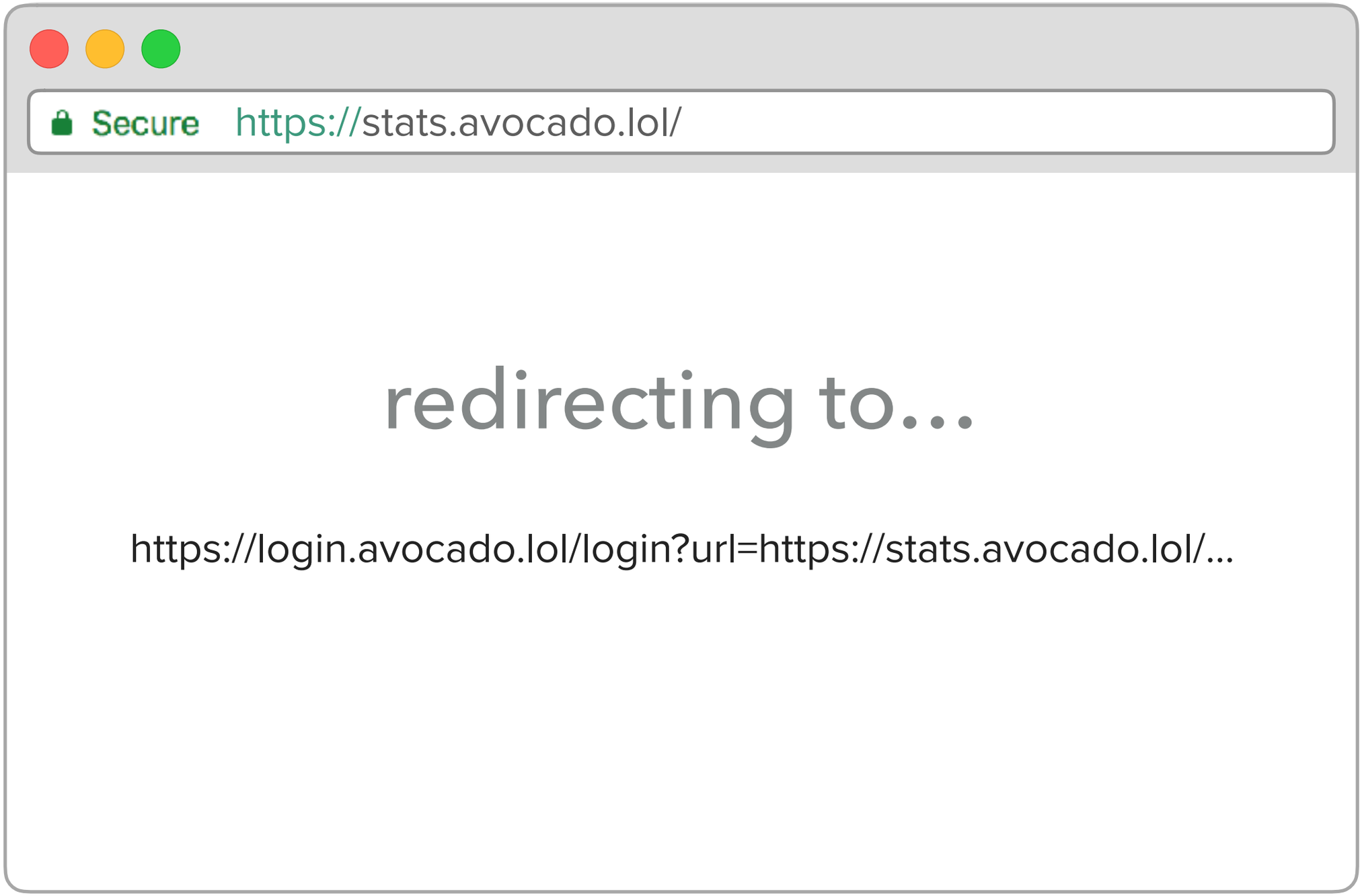

NGINX
avocado.lol
login.avocado.lol
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol

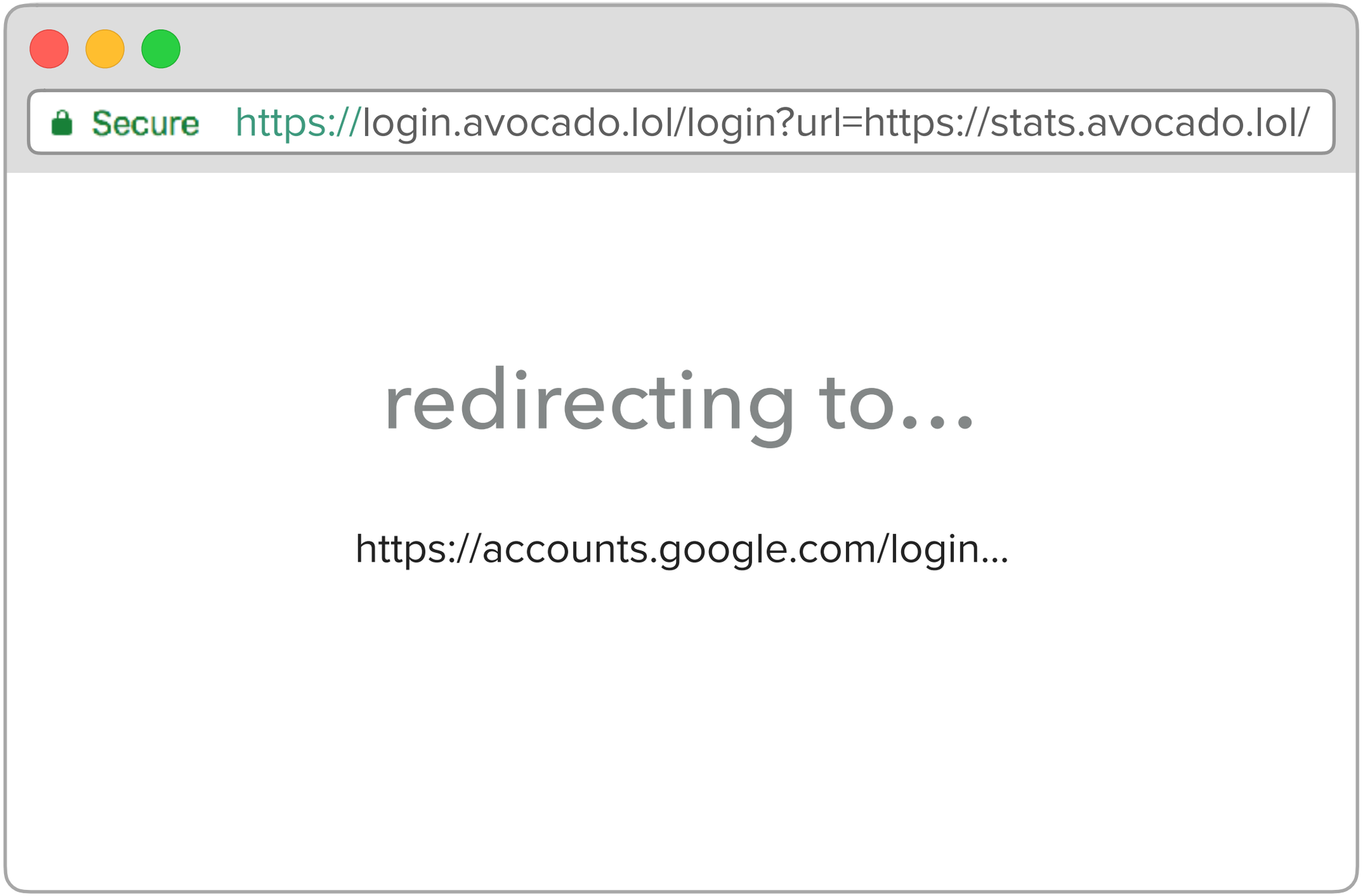

NGINX
avocado.lol
login.avocado.lol
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol

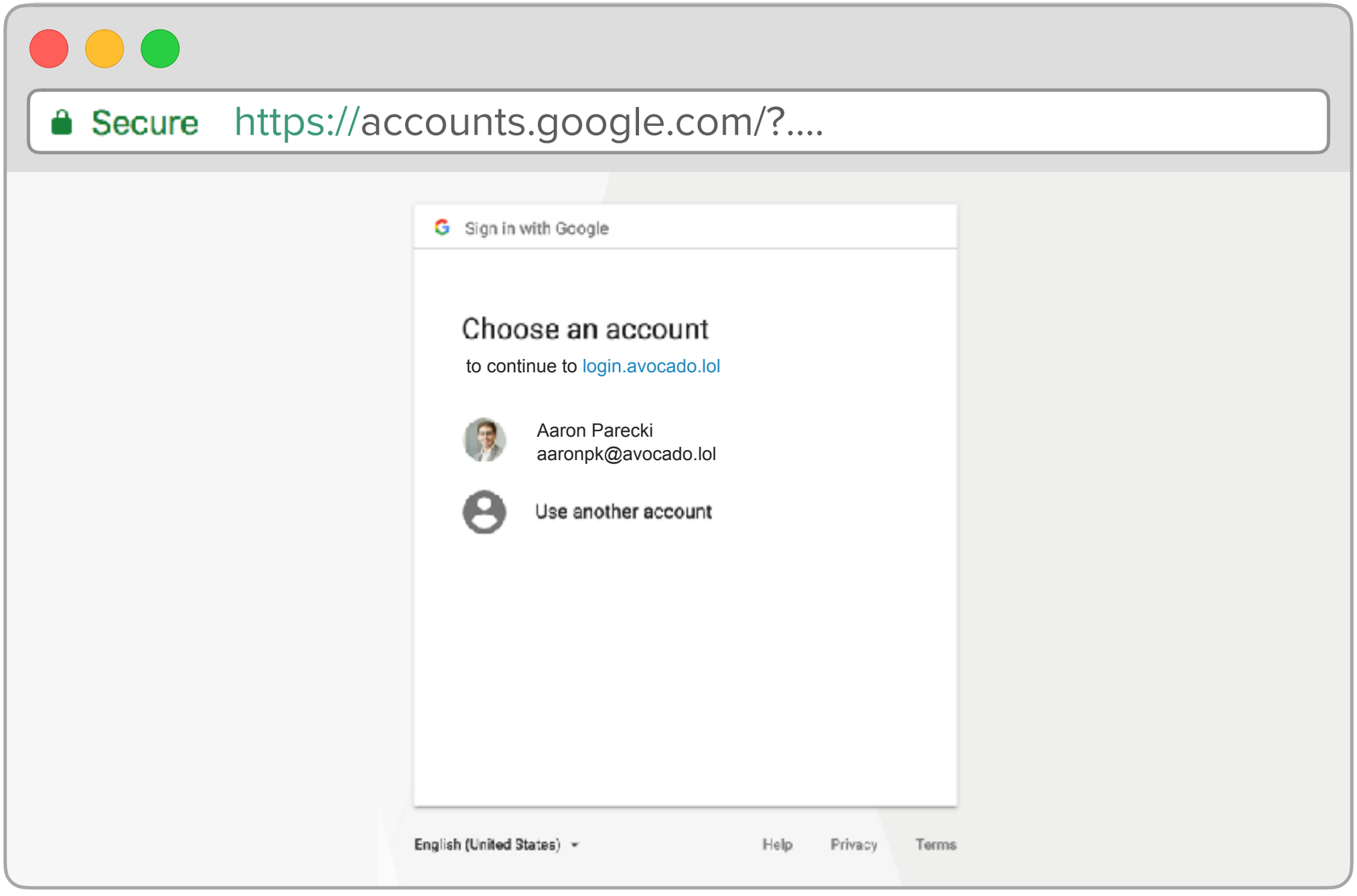

NGINX
avocado.lol
login.avocado.lol
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol


NGINX
avocado.lol
login.avocado.lol
OAUTH
OAUTH
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol

@aaronpk

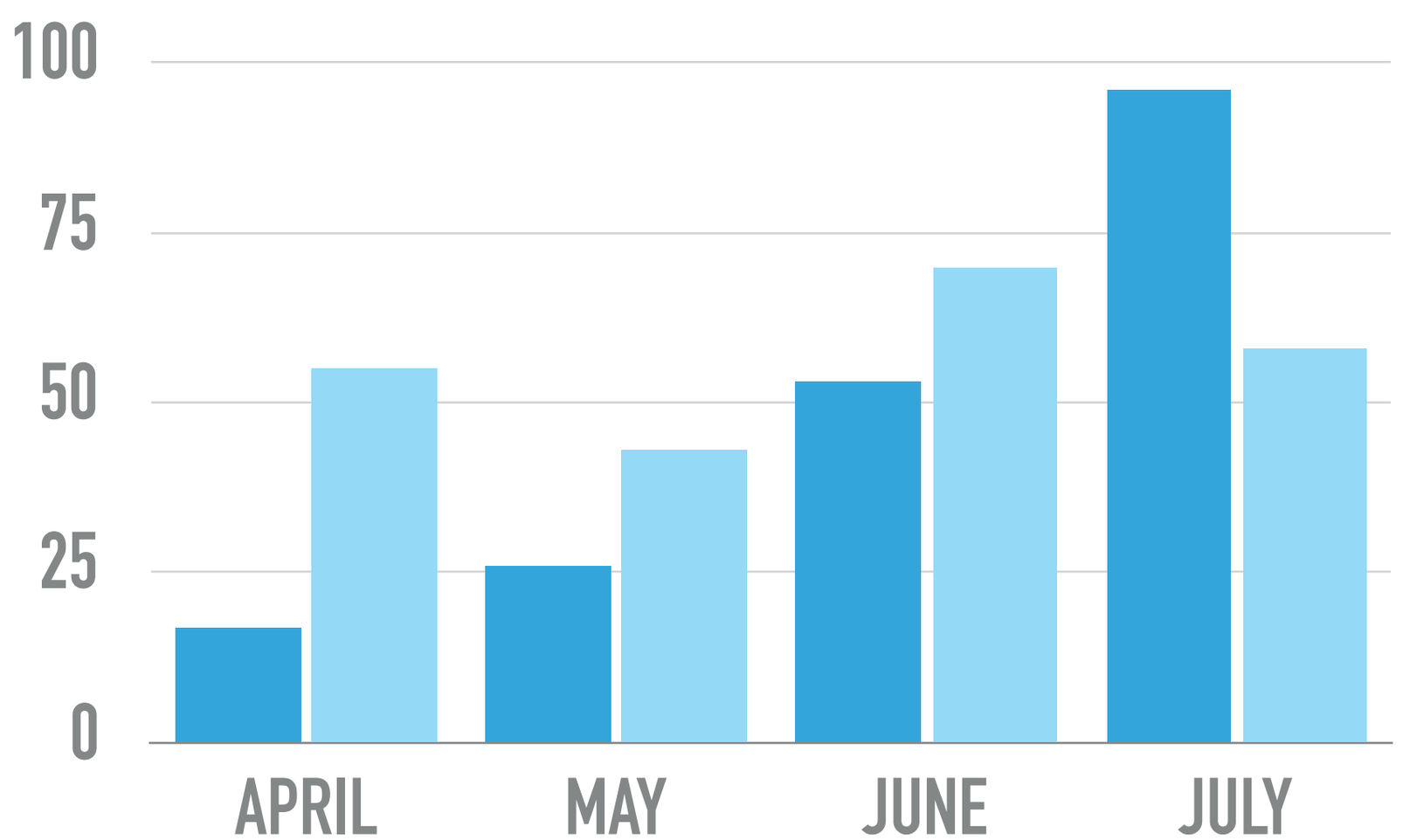

Secure
https://stats.avocado.lol/
redirecting to...
https://login.avocado.lol/login?url=https://stats.avocado.lol/...


Secure
https://login.avocado.lol/login?url=https://stats.avocado.lol/
redirecting to...
https://accounts.google.com/login...

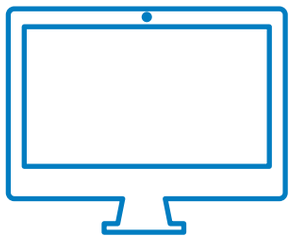

Secure
https://accounts.google.com/?....
Sign in with Google
Choose an account
to continue to login.avocado.lol
Aaron Parecki
aaronpk@avocado.lol
Use another account
English (United States)
Help
Privacy
Terms


Secure
https://login.avocado.lol/callback?code=azsyxuqmdkfhgpw
redirecting to...
https://stats.avocado.lol/

Secure https://stats.avocado.lol/



@aaronpk



Nginx

Lasso

Google

Not Authorized

GET stats.avocado.lol

GET login.avocado.lol/validate

401 Not Authorized

302 login.avocado.lol

Lasso Login

GET login.avocado.lol

302 accounts.google.com/oauth/authorize

Google OAuth

GET accounts.google.com/oauth/authorize

302 login.avocado.lol/callback?code=x

GET login.avocado.lol/callback?code=x

Lasso Begins Session

POST accounts.google.com/oauth/token

{ "user": "username@avocado.lol" }

302 stats.avocado.lol

Cookie: Lasso-Session: eyJ...

Authorized!

GET stats.avocado.lol

GET login.avocado.lol/validate

200 OK

200 OK

LASSO USE CASES

Restrict to email address domain name
(e.g. Google Apps Accounts)

Allow all users if they can authenticate
(e.g. your own OAuth/OpenID Connect server)

Public access, authenticate for additional privileges
(e.g. read-only public wiki, log in to edit)

CONFIGURING LASSO – GOOGLE APPS DOMAIN

```
config.yml

lasso:

  listen: 127.0.0.1
  port: 9090

  publicAccess: false
  allowAllUsers: false

  domains:
    - avocado.lol

oauth:
  provider: google
  client_id: 144124...
  client_secret: u_eWvYCtD
  callback_urls:
  - https://login.avocado.lol/auth
  preferredDomain: avocado.lol
```

Require authentication on every request

Allow only users at the domains below

Allow users with email addresses at this domain

CONFIGURING LASSO – CUSTOM OPENID SERVER


```
config.yml

lasso:

  listen: 127.0.0.1
  port: 9090

  publicAccess: false

  allowAllUsers: true
```

Require authentication on every request

Allow any user at the OAuth server

```
  oauth:
    provider: oidc
    client_id: 014223
    client_secret: JKLOL
    auth_url: https://dev-442449.oktapreview.com/oauth2/default/v1/authorize
    token_url: https://dev-442449.oktapreview.com/oauth2/default/v1/token
    user_info_url: https://dev-442449.oktapreview.com/oauth2/default/v1/userinfo
    scopes:
      - openid
      - email
      - profile
    callback_url: https://login.avocado.lol/auth
```

Custom OpenID Connect server configuration

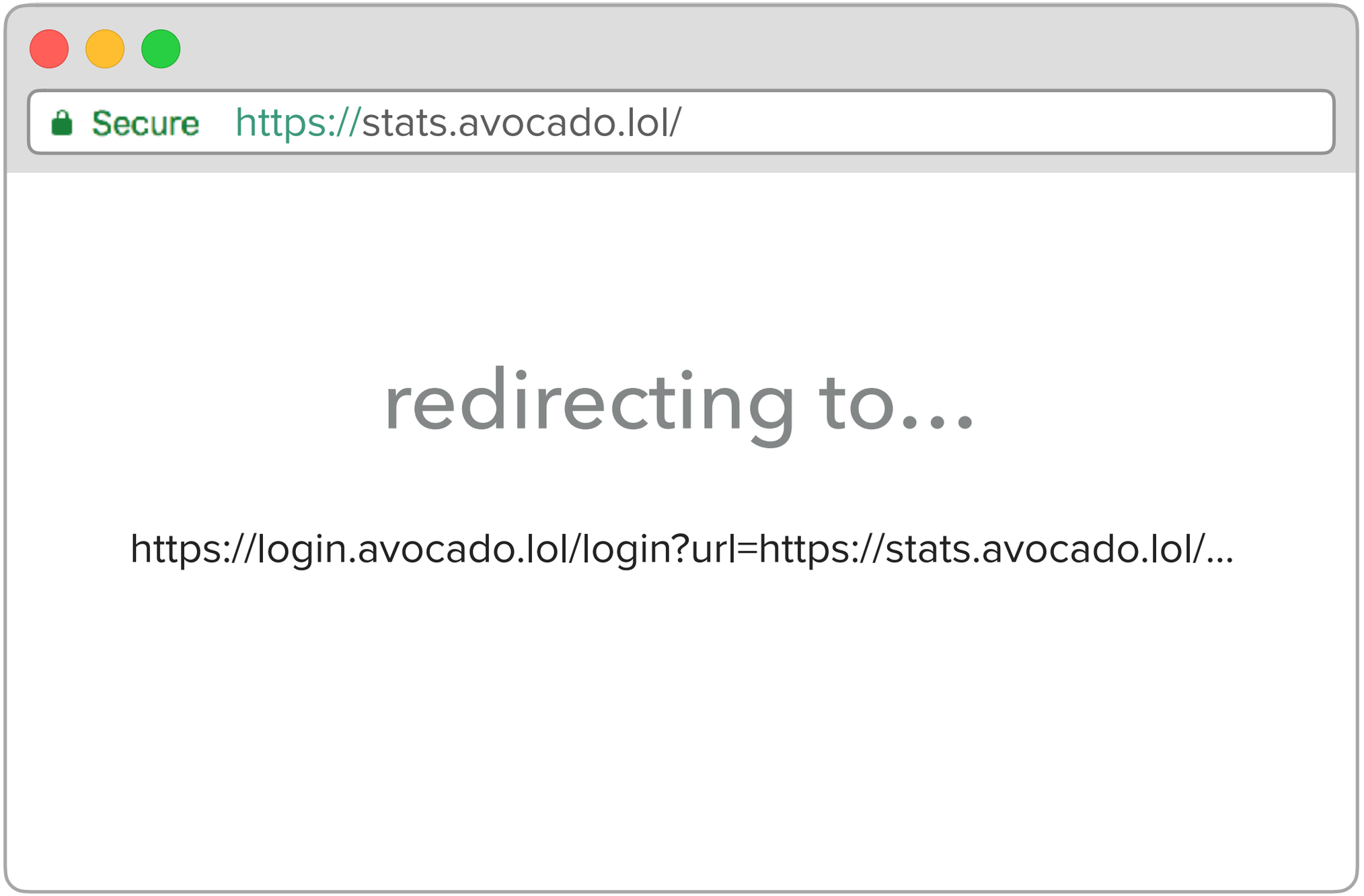
CONFIGURING LASSO – WORDPRESS SERVER

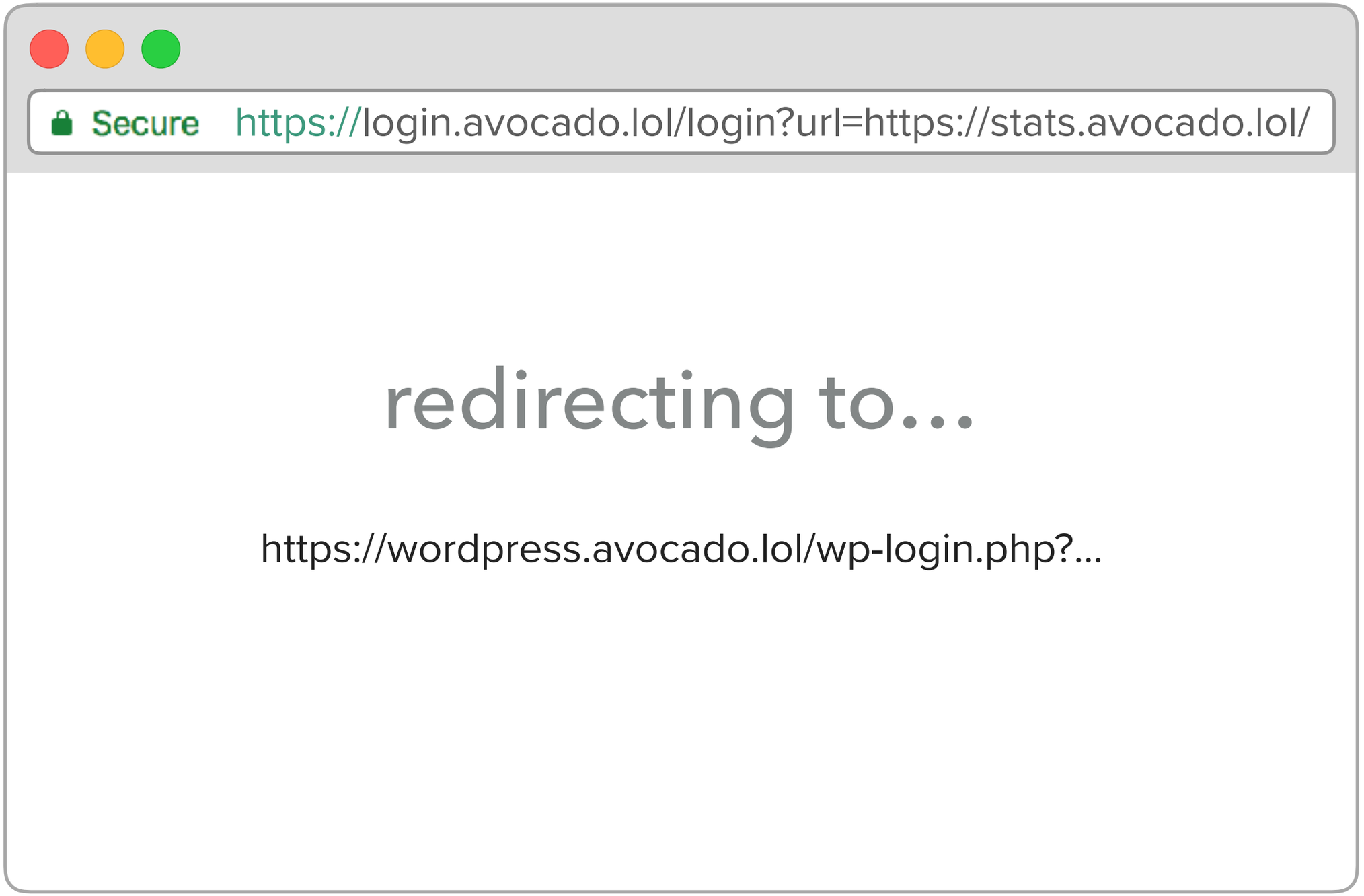
```
config.yml

lasso:

  listen: 127.0.0.1
  port: 9090

  publicAccess: false

  allowAllUsers: true

oauth:
  provider: indieauth
  client_id: https://login.avocado.lol/
  auth_url: https://wordpress.avocado.lol/wp-json/indieauth/1.0/auth
  callback_url: https://login.avocado.lol/auth
```

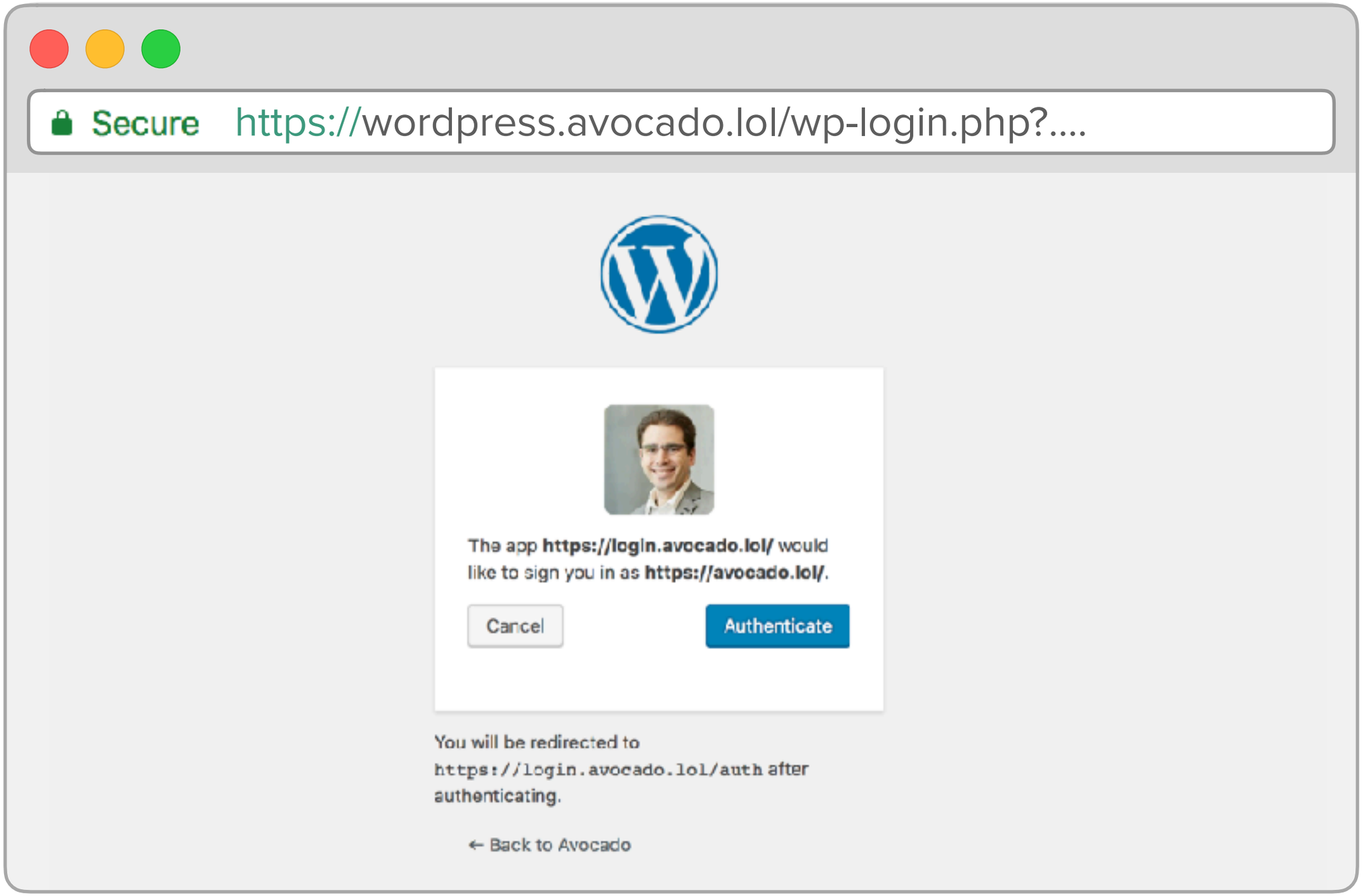
Require authentication on every request

Allow any user who can log in to this WordPress

WordPress OAuth server configuration


Secure
https://stats.avocado.lol/
redirecting to...
https://login.avocado.lol/login?url=https://stats.avocado.lol/...

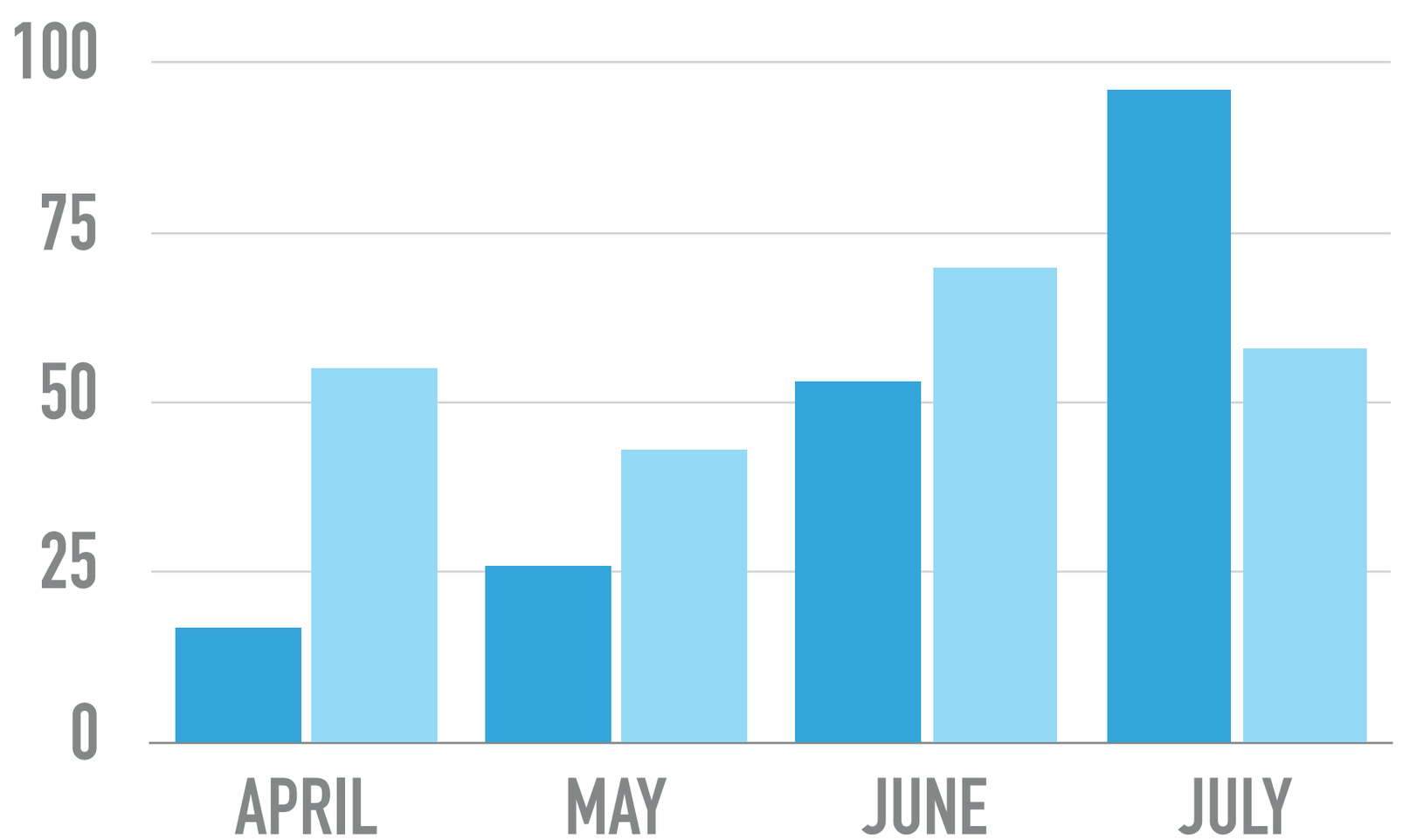

Secure
https://login.avocado.lol/login?url=https://stats.avocado.lol/
redirecting to...
https://wordpress.avocado.lol/wp-login.php?...


Secure
https://wordpress.avocado.lol/wp-login.php?....
The app https://login.avocado.lol/ would like to sign you in as https://avocado.lol/.
Cancel
Authenticate
You will be redirected to https://login.avocado.lol/auth after authenticating.
← Back to Avocado

@aaronpk


Secure
https://login.avocado.lol/callback?code=azsyxuqmdkfhgpw
redirecting to...
https://stats.avocado.lol/

Secure https://stats.avocado.lol/



@aaronpk

CONFIGURING LASSO – PUBLIC ACCESS WITH GITHUB LOGIN

config.yml

```
lasso:

  listen: 127.0.0.1
  port: 9090

  publicAccess: true

  allowAllUsers: true

oauth:
  provider: github
  client_id:
  client_secret:
  auth_url: https://github.com/login/oauth/authorize
  token_url: https://github.com/login/oauth/access_token
  scopes:
    - user
  user_info_url: https://api.github.com/user?access_token=
```

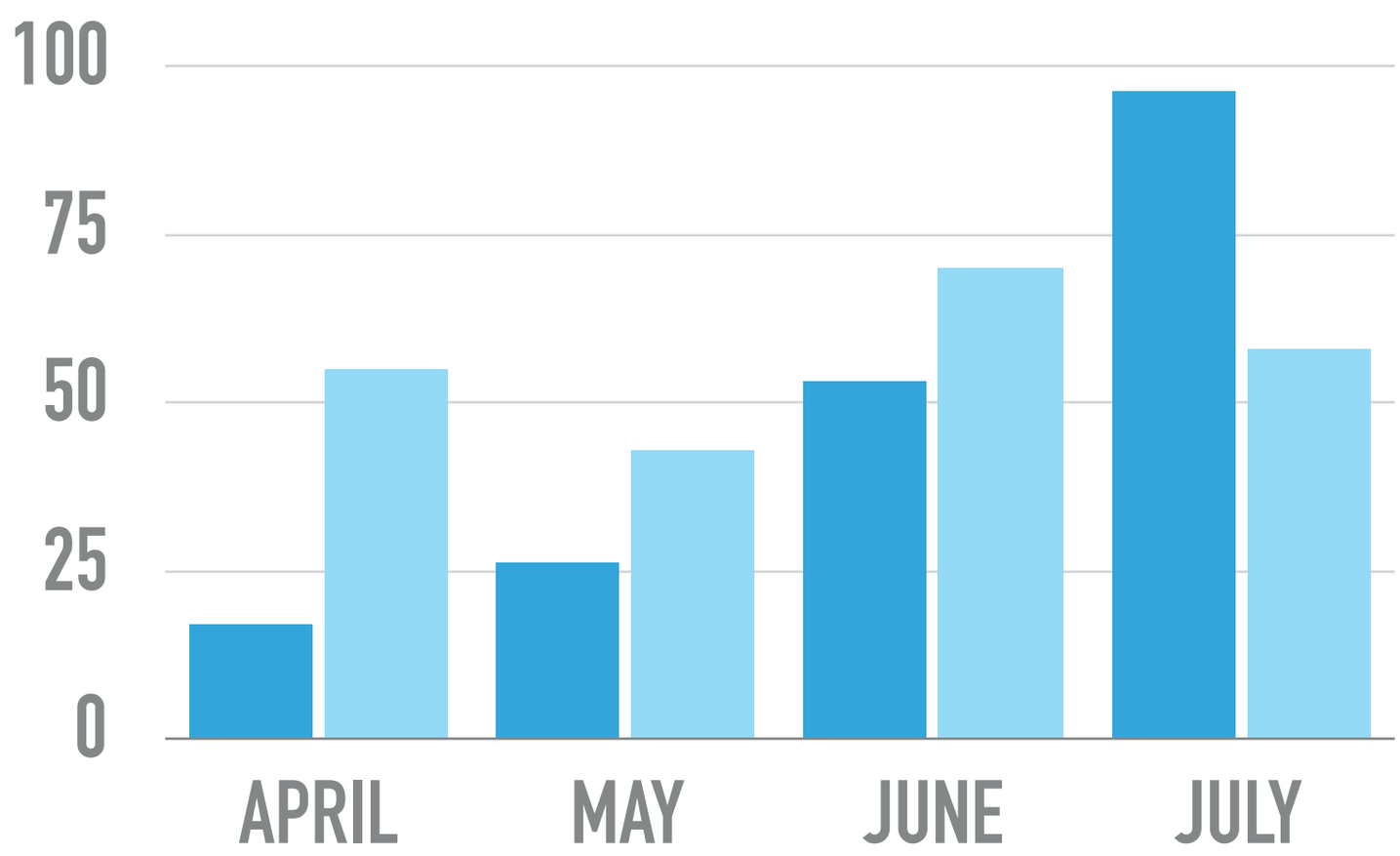
Allow requests even without authentication

Anyone with a GitHub account can log in

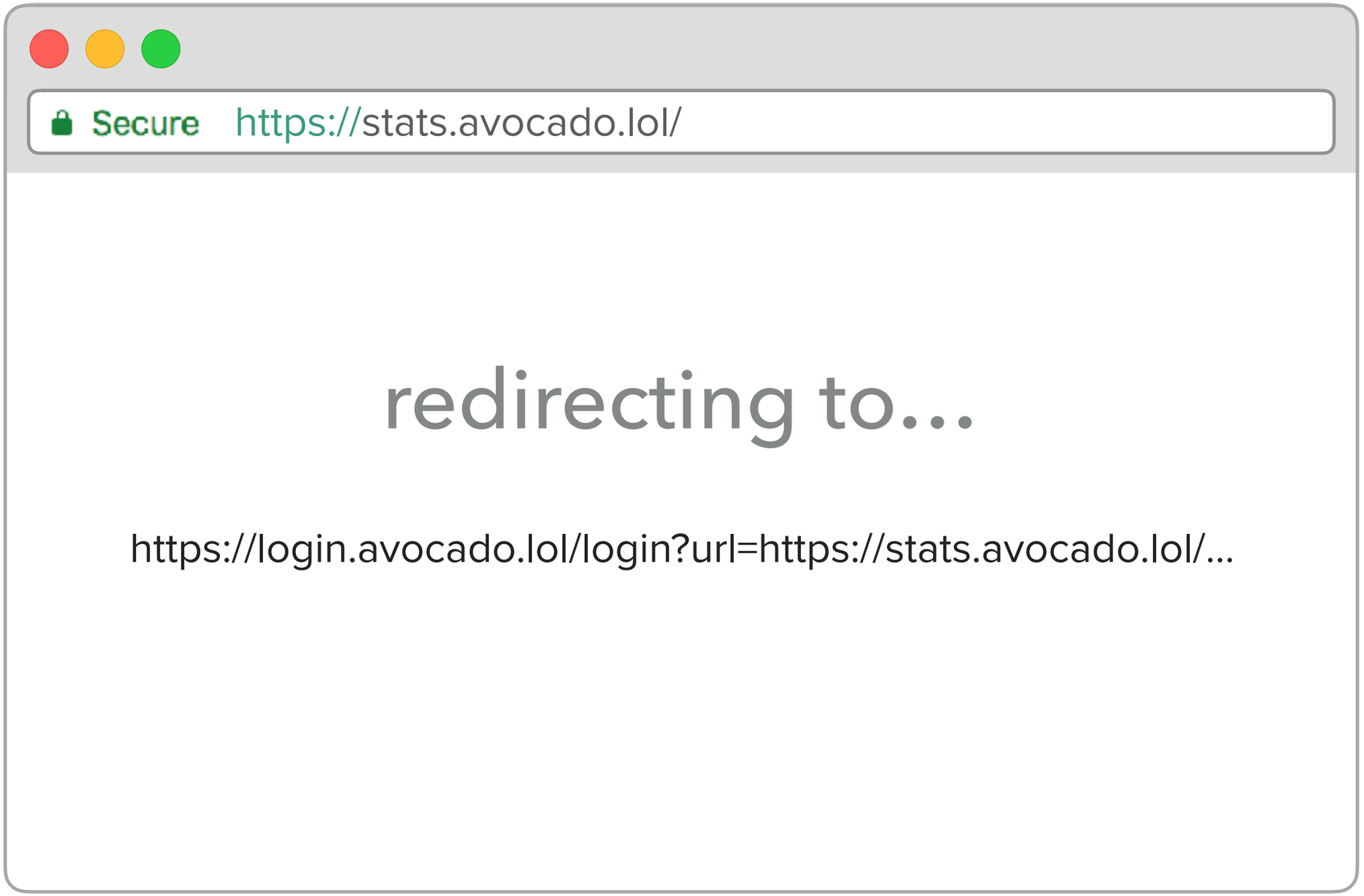
Configure GitHub credentials

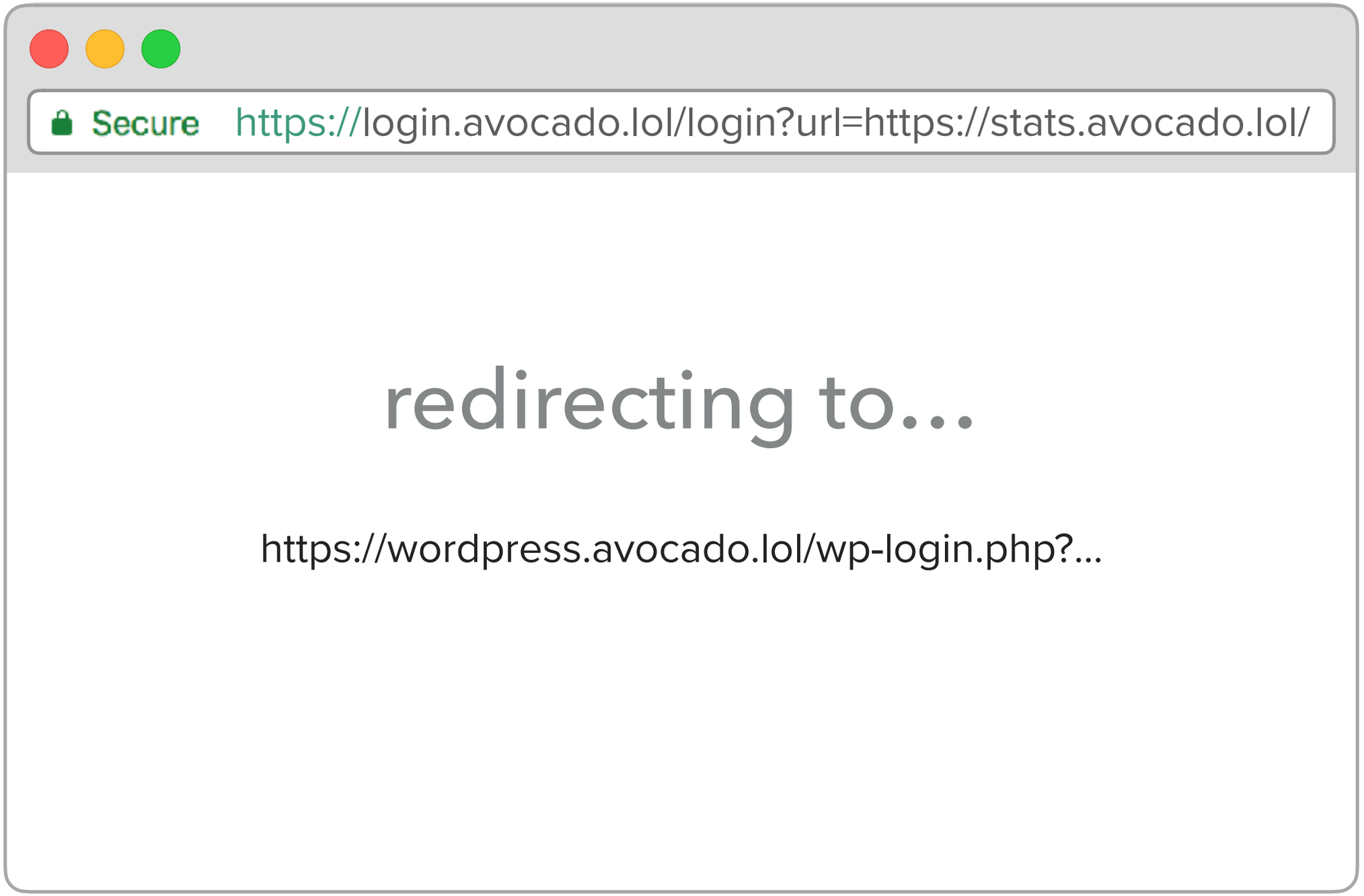
Secure https://stats.avocado.lol/

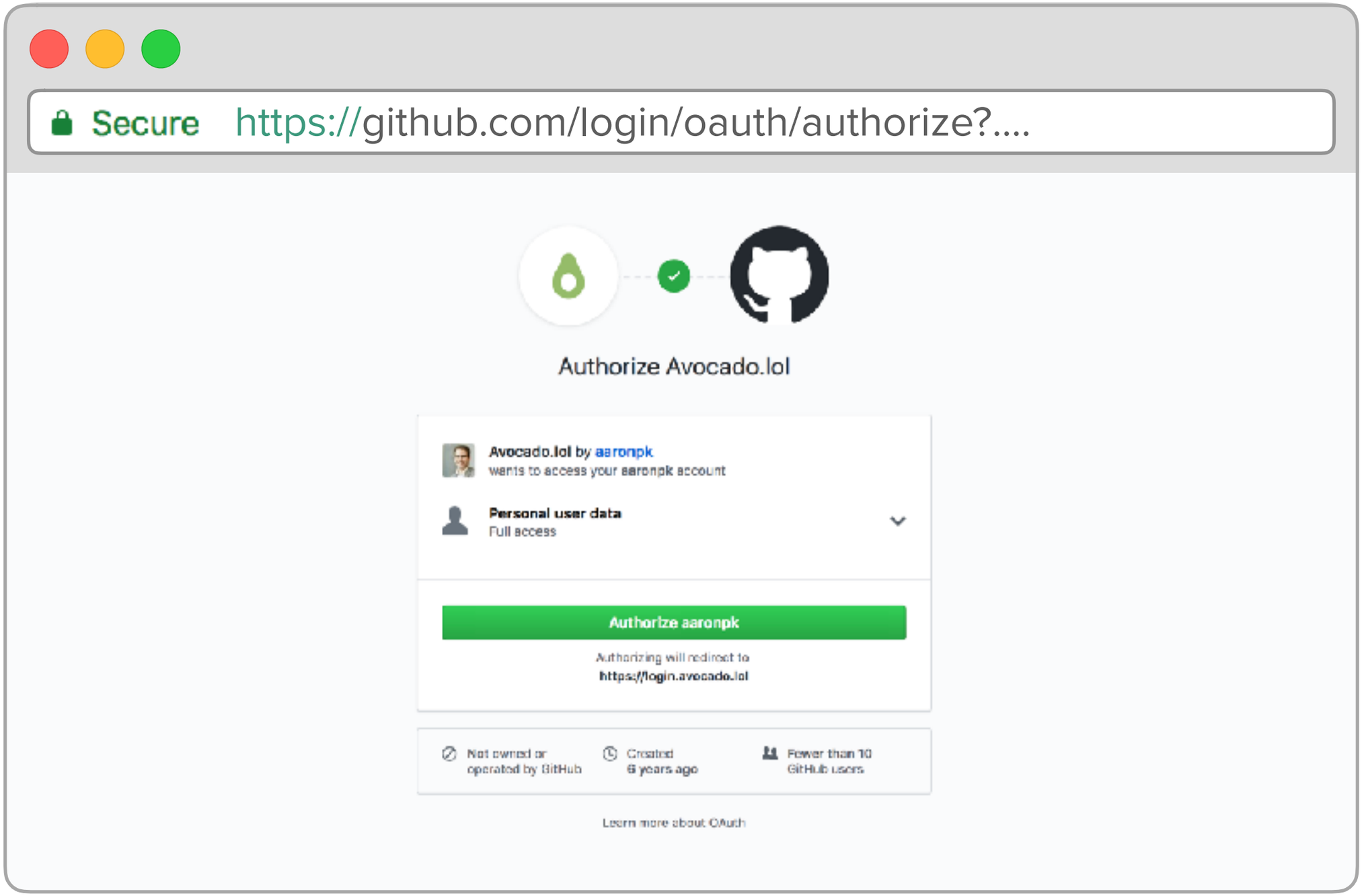
Log In



@aaronpk


Secure
https://stats.avocado.lol/
redirecting to...
https://login.avocado.lol/login?url=https://stats.avocado.lol/...


Secure
https://login.avocado.lol/login?url=https://stats.avocado.lol/
redirecting to...
https://wordpress.avocado.lol/wp-login.php?...

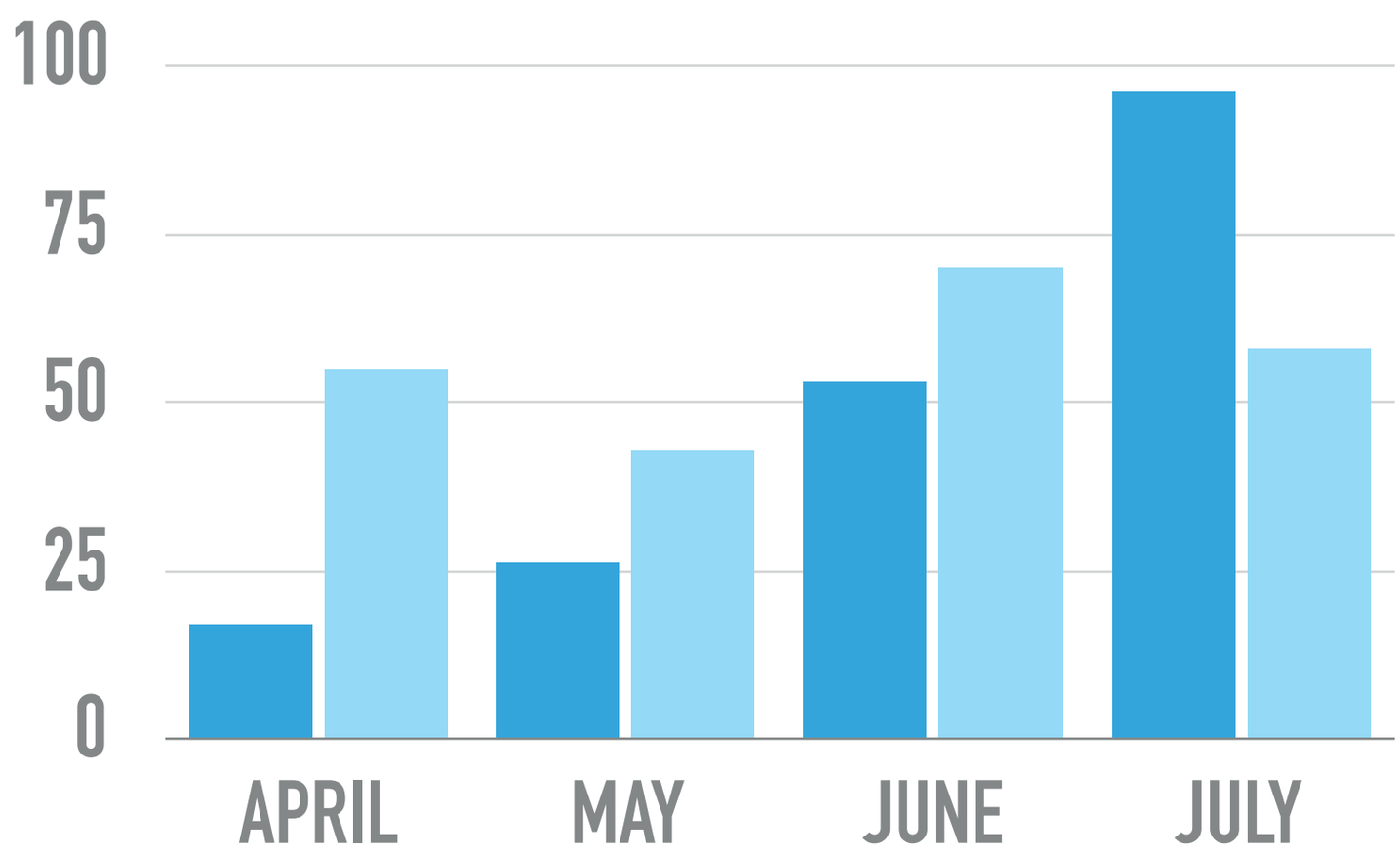

Secure https://github.com/login/oauth/authorize?....
Authorize Avocado.lol
Avocado.lol by aaronpk
wants to access your aaronpk account
Personal user data
Full access
Authorize aaronpk
Authorizing will redirect to
https://login.avocado.lol
Not owned or operated by GitHub
Created 6 years ago
Fewer than 10 GitHub users
Learn more about OAuth

@aaronpk


Secure
https://login.avocado.lol/callback?code=azsyxuqmdkfhgpw
redirecting to...
https://stats.avocado.lol/

Secure https://stats.avocado.lol/

Logged in as @aaronpk



WHO LOGGED IN?

```
server {
  ...
  auth_request_set $auth_user $upstream_http_x_lasso_user;
  ...
  fastcgi_param REMOTE_USER $auth_user;
    # or
  proxy_set_header Remote-User $auth_user;
  ...
}
```

```
<?php

if($_SERVER['REMOTE_USER'])
  echo 'Hello, ' . $_SERVER['REMOTE_USER'] . '!';
else
  echo 'Not logged in';
```

LOGIN.AVOCADO.LOL

- Start the OAuth flow with the configured provider
- Verifies the OAuth callback with the provider
- Creates a JWT and returns it in a Set-Cookie header
- Verifies the cookie sent in each subrequest

JSON WEB TOKEN

Header

Payload

Signature

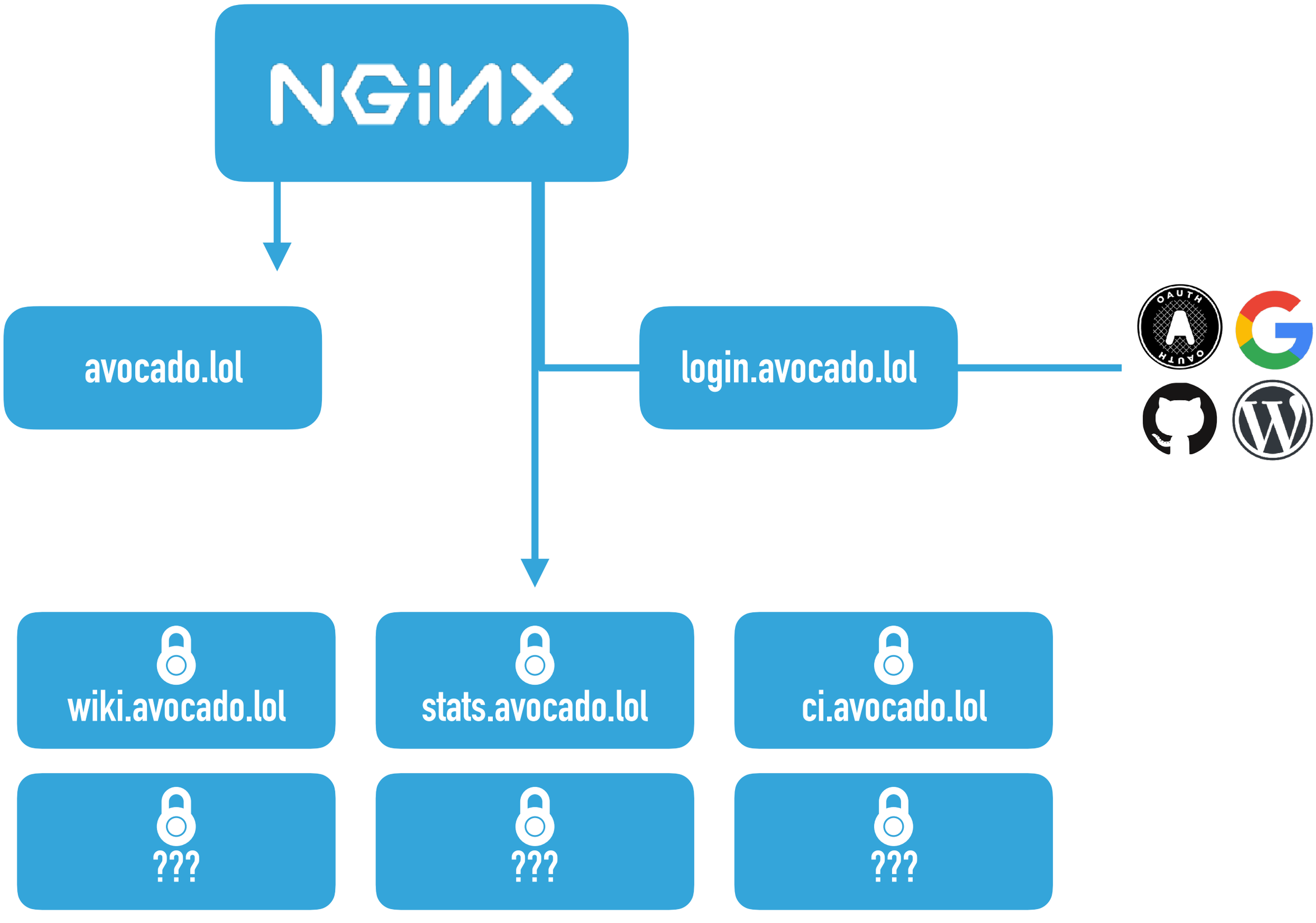
```
eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp
XVCJ9
.
eyJlbWFpbCI6ImFhcm9uQHBhcmVja2k
uY29tIiwic2l0ZXMiOltdLCJleHAiOj
E1MzQ3NDk2OTcsImlzcyI6Ikxhc3NvI
n0
.
I78cOzljav3vASI9Nj5Q2l_4QJcnRJH
g3Y5Aj-mkNQ
```

JSON WEB TOKEN

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
{ "typ": "JWT", "alg": "HS256" }


eyJlbWFpbCI6ImFhcm9uQHBhcmVja2kuY29tIiwic2l0
ZXMiOltdLCJleHAiOjE1MzQ3NDk2OTcsImlzcyI6Ikxh
c3NvIn0
{
 "email": "aaron@parecki.com",
 "sites": [],
 "exp": 1534749697,
 "iss": "Lasso"
}


I78cOzljav3vASI9Nj5Q2l_4QJcnRJHg3Y5Aj-mkNQ
```

JWT COOKIE

- Set cookie with `HttpOnly` and `Secure`
- Cryptographically signed with a secret key
- Signed key can be validated in less than 1ms
- No need to store in a database


NGINX
avocado.lol
login.avocado.lol
OAUTH
wiki.avocado.lol
stats.avocado.lol
ci.avocado.lol
???
???
???

@aaronpk

WHY IS THIS AWESOME

- Single place to manage access to your backend tools
- Each user has their own login, no shared passwords for internal tools
- Can protect any application without that application needing to support authentication itself

GETTING STARTED

- go get github.com/LassoProject/lasso
- cd ~/go/src/github.com/LassoProject/lasso
- go build
- cp config/config.yml_example config/config.yml
- # set up the config file
- ./lasso

THANK YOU!

- github.com/LassoProject
- Slides from this talk at avocado.lol
- twitter.com/aaronpk
- aaronpk.com
- developer.okta.com/blog