eZeeKonfigurator

Vlad Grigorescu

vlad@es.net

Zeek Week 2019

Outline

1. Background & Motivation
2. Demo
3. Design & Architecture
4. Roadmap & Future Plans
5. How To Try It (...and Contribute?)
6. Q & A

$ cat $vlad/.plan

I am a...

- Zeek user
- Zeek developer
- ESnet security engineer

What is ESnet?

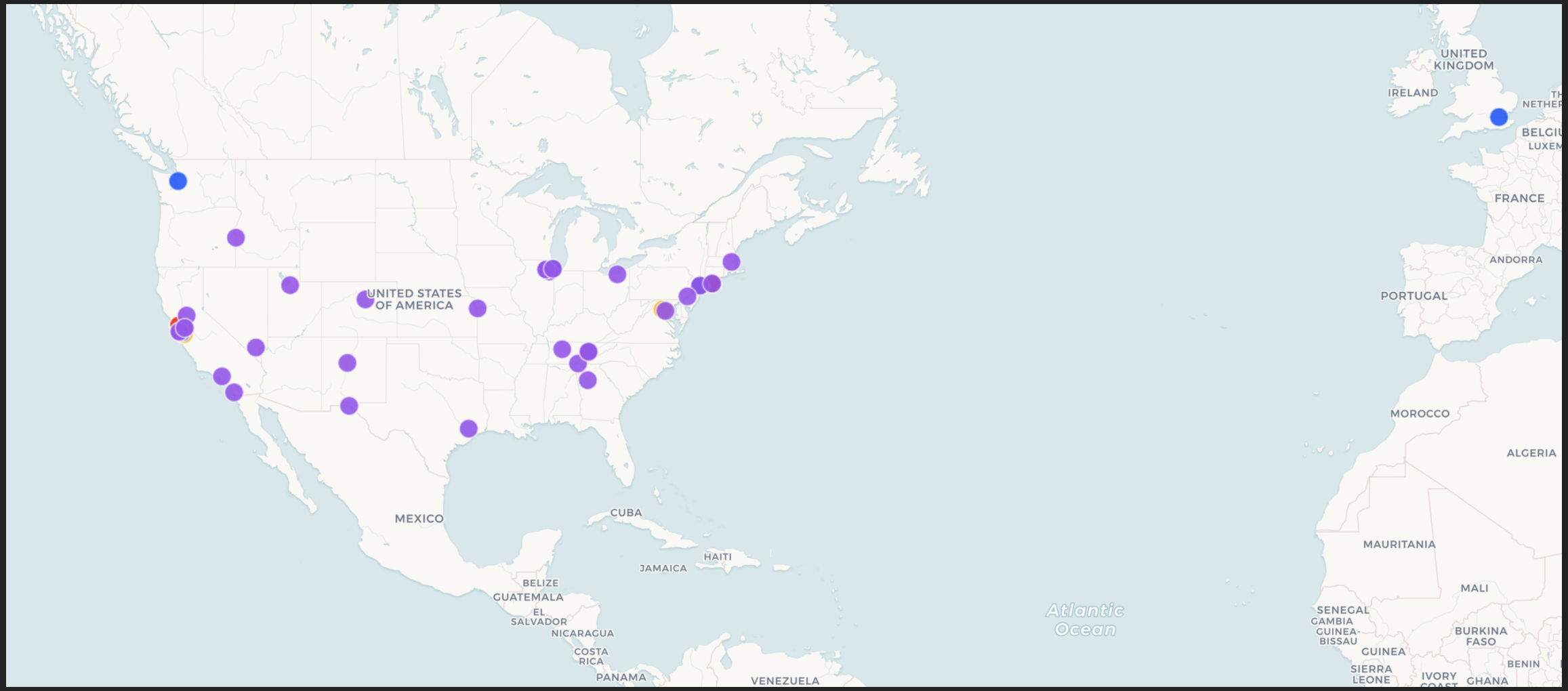
- A bleeding-edge network that connects national labs, CERN, NASA, etc.
- Enabling "science in the cloud."
- ISP for thousands of users

Challenges

“ Data rates of around 40Tb/s going into the ATLAS, CMS, and LHCb software triggers imply an overall volume of around 60 exabytes of data to be processed per year…

- 950 lit 100 Gbps ports
- 3 PB of ingress traffic/day
- 10x growth every 47 months
- 400 locations in the US & Europe
- Requirement: 99.999% uptime

Goal: Config Management



Goal: Config Management

10:54 **Gitlab-Bro** APP Michael Dopheide (dopheide) opened !21 **Add sites.dat for use by zeek_add-site-data** in security/esnet-bro

Samson Hille (samson) approved !21 **Add sites.dat for use by zeek_add-site-data** in security/esnet-bro

> security/esnet-bro: Pipeline #980 of branch topic/dopheide/sites by Michael Dopheide (dopheide) passed in 03:51

11:02 **Gitlab-Bro** APP Michael Dopheide (dopheide) merged !21 **Add sites.dat for use by zeek_add-site-data** in security/esnet-bro

> security/esnet-bro: Pipeline #981 of branch master by Michael Dopheide (dopheide) passed in 03:47

Goal: Policy/Script

```
1 event http_request(c: connection, method: string, original_URI: string,
2                    unescaped_URI: string, version: string) &priority=3
3         {
4         if ( sensitive_URIs in unescaped_URI )
5                 {
6                 NOTICE([$note=HTTP_SensitiveURI, $msg=message, ...);
7                 }
```

Goal: Policy/Script

```
redef sensitive_URIs +=
        /.*Copy_of_UPS_Label\.zip/|
        /.*Delivery_Information.*\.zip/|
        /.*Label_Copy_UPS\.zip/|
        /.*qiss\.ucoz\.com.*/|
        /.*semtex\.c/|
        /\?-s\+%3d/|
        /\?-d\+auto_prepend_file/|
        /\.\.%2Fetc%2Fpasswd/|
        /\.\.%2Fboot\.ini/|
        /\.\.\/\.\.\/proc\/self\/fd/|
        /\.\.\/\.\.\/proc\/self\/version/|
        /\.\.\\\.\.\\windows\\win\.ini/|
        /\.\.\/boot\.ini/|
        /\.\.\/etc\/httpd\/logs\/error\.log/|
        /\.\.\/etc\/httpd\/logs\/error_log/|
        /\.\.\/var\/log\/apache\/error\.log/|
        /\.\.\/var\/log\/apache2\/error\.log/|
        /\.\.\\windows\\win.ini/|
        /\.\.\/windows\/iis6\.log/|
        /\.\.\/windows\/iis6\.log/|
        /\/admin-console/|
        /boot\.ini/|
        /\/(cmd|root|tftp)\.exe/|
        /c99.php/|
        /c99shell.php/|
        /\.htaccess\/sh/|
        /index.php\?-s/|
        /index.php?session_to_unset=/|
        /index.php\?-dsafe_mode/|
        /index.php\?-dallow_url_include/|
        /open_basedir=none/|
        /php:\/\/input\+-d\+cgi\.force_redirect/|
        /php.cgi\?-d\+allow_url_include/|
        /ppcrlconfig.bin/|
```

Goal: Policy/Script

```
$ fgrep '/|' esnet-http.zeek
218
$ egrep -c '.' esnet-http.zeek
316
```

```
redef sensitive_URIs +=
        /.*Copy_of_UPS_Label\.zip/|
        /.*Delivery_Information.*\.zip/|
        /.*Label_Copy_UPS\.zip/|
        /.*qiss\.ucoz\.com.*/|
        /.*semtex\.c/|
        /\?-s\+%3d/|
        /\?-d\+auto_prepend_file/|
        /\.\.%2Fetc%2Fpasswd/|
        /\.\.%2Fboot\.ini/|
        /\.\.\/\.\.\/proc\/self\/fd/|
        /\.\.\/\.\.\/proc\/self\/version/|
        /\.\.\\\.\.\\windows\\win\.ini/|
        /\.\.\/boot\.ini/|
        /\.\.\/etc\/httpd\/logs\/error\.log/|
        /\.\.\/etc\/httpd\/logs\/error_log/|
        /\.\.\/var\/log\/apache\/error\.log/|
        /\.\.\/var\/log\/apache2\/error\.log/|
        /\.\.\\windows\\win.ini/|
        /\.\.\/windows\/iis6\.log/|
        /\.\.\/windows\/iis6\.log/|
        /\/admin-console/|
        /boot\.ini/|
        /\/(cmd|root|tftp)\.exe/|
        /c99.php/|
        /c99shell.php/|
        /\.htaccess\/sh/|
        /index.php\?-s/|
        /index.php?session_to_unset=/|
        /index.php\?-dsafe_mode/|
        /index.php\?-dallow_url_include/|
        /open_basedir=none/|
        /php:\/\/input\+-d\+cgi\.force_redirect/|
        /php.cgi\?-d\+allow_url_include/|
        /ppcrlconfig.bin/|
```

Goal: Policy/Script

```
1          if(! Site::is_neighbor_addr(c$id$orig_h) && ! Site::is_local_addr(c$id$orig_h)){
2               if(!(c$id$orig_h in rdp_whitelist && rdp_whitelist[c$id$orig_h] == c$id$resp_h) &&
3                  !(c$id$orig_h in rdp_friendly_nets)){
4                    NOTICE([$note=ESnet::External_Desktop_Threshold,
```

https://nsmdb-east.es.net/ez/

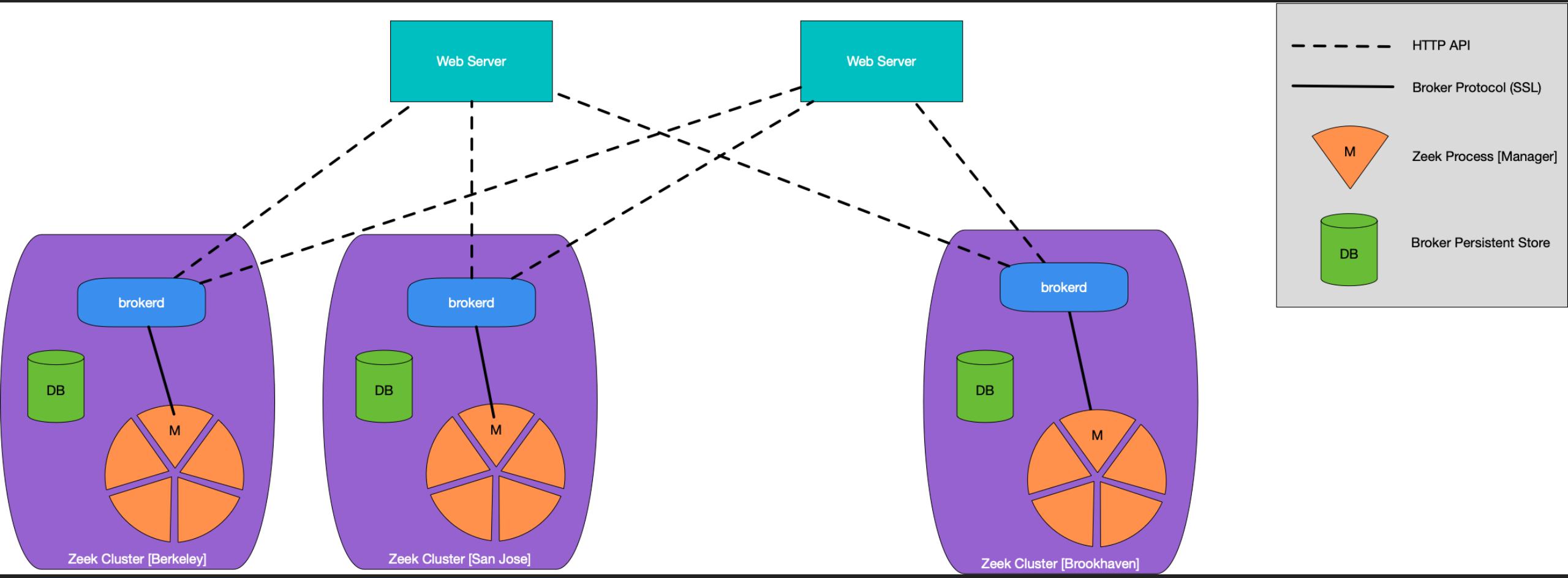
eZeeKonfigurator Features

- Quickly push out changes to any number of Zeek clusters
- Be able to set **any** type of option
- Change tracking
- Auditing
- Document "magic" values

eZeeKonfigurator Applications

- Notice policy configuration package
  - Quick and easy to set notice policy.
- Zeek Exporter package
  - Measure the impact of a change
- *Log filter package*
- *SumStat policy configuration package*

Architecture



FEMA Region 9
@FEMARegion9

Follow

A @PGE4Me Power Shutoff is planned for early Wednesday morning until mid-day Thursday due to a #RedFlagWarning. Around 775,000 customers in 39 counties may be impacted.

Visit here to learn more: pge.com

Prepare for a power outage: ready.gov/power-outages

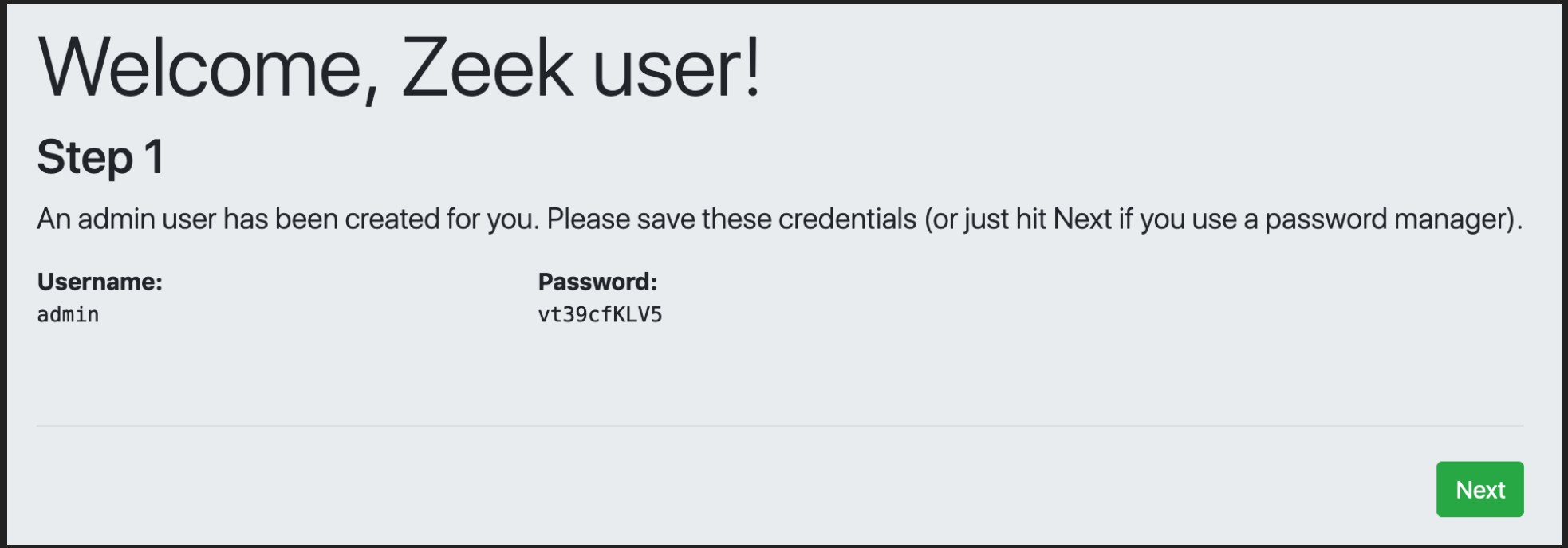
2:42 PM - 8 Oct 2019

TODO

- Expiration
- RBAC
- Better type safety:
  - enum existence
  - set uniqueness
- Better UI for configuring sensor groups

Install: Server

```
pip install https://github.com/esnet/eZeeKonfigurator
daphne eZeeKonfigurator.asgi:application
```



Install: Client

```
zkg install ezk_client
zeekctl deploy
```

```
1 The following packages will be INSTALLED:
2   ezk_client (0.1)
3
4 Proceed? [Y/n] Y
5 ezk_client asks for EZK_URL (web server URL) ? [http://localhost:8000]
```

What Can I Do?

- Publish packages
  - ...using options
- Try eZeeKonfigurator
  - Fork it, help develop!
  - ...or just loudly complain via GitHub issues

OK, I'm in!

- Server:

https://github.com/esnet/eZeeKonfigurator

- Client:

https://github.com/esnet/ezk_client

- Presentation:

https://software.es.net/eZeeKonfigurator/