

lab10 - Feature #1

Set up letsencrypt certs (for https) auto-renewal

06.09.2016 11:40 - didi

Status: New	Due date:
Priority: Normal	
Assignee: didi	
Target version:	
Description	
<p>Status quo: redmine.d10r.net is served via Apache reverse proxy on h1.d10r.net, where the https config is also located. The certificate is from "letsencrypt": https://letsencrypt.org/. Setup was done using the cli tool <i>letsencrypt</i> installed via Debian package. Note that the package is flagged as obsolete due to the renaming of the tool to <i>certbot</i>, however this package can't be installed for unknown reason:</p> <p>The following packages have unmet dependencies: certbot : Depends: python-certbot (= 0.8.1-2~bpo8+1) but it is not going to be installed</p> <p>Thus for now I just keep using the <i>letsencrypt</i> command.</p> <p>In theory the tool can adjust the Apache config itself. However I use Apache Macros for the proxy config files, which the tool can't handle. Thus I used manual mode for renewing:</p> <pre>letsencrypt renew --manual</pre> <p>This is now also added ad a cronjob (executed monthly). For now the only purpose of that cronjob is to trigger an email notification if anything is written to stderr. Once that happens, check if/how it can be further automated.</p> <p>The manual method authorizes a domain by checking the existence of a specific file, e.g. in this case http://redmine.d10r.net/~well-known/acme-challenge/p3-78vilmHKLSR0lKeqnhk_TQ3A0ee43V6U1QpQ1Z0. Needs to be seen if this file / its contents need to be changed for renewal. The Apache config needs no update on renewal. Probably a reload of the Apache daemon is needed in order to read the updated pem file (<i>service apache2 reload</i>).</p>	

History

#1 - 15.03.2017 23:08 - didi

- Project changed from 3 to lab10

#2 - 12.04.2017 23:22 - didi

```
letsencrypt certonly --manual -d sub.lab10.io --standalone-supported-challenges http-01
```

#3 - 11.07.2017 11:38 - didi

auto renew failed for chat.lab10.io and code.lab10.io.
Trying with `letsencrypt certonly -d chat.lab10.io --preferred-challenges dns --manual`
Not sure if renew will work for that.
Btw. the `--post-hook` argument may be useful for deploying certs.

letsencrypt certs expire after 90 days (can't be changed).

wildcard certs are announced for 2018.