Setup Grafana on Ubuntu 18.04 with LetsEncrypt

MAY 13, 2019 | IN DEBIAN, LINUX | BY ORI

In this article I will show you how to get the data visualisation solution Grafana to work with clean HTTPS on Ubuntu 18.04.
As alwaysI recommend not running the service natively on your server but rather to run it in a VM.

See: virtualization with KVM

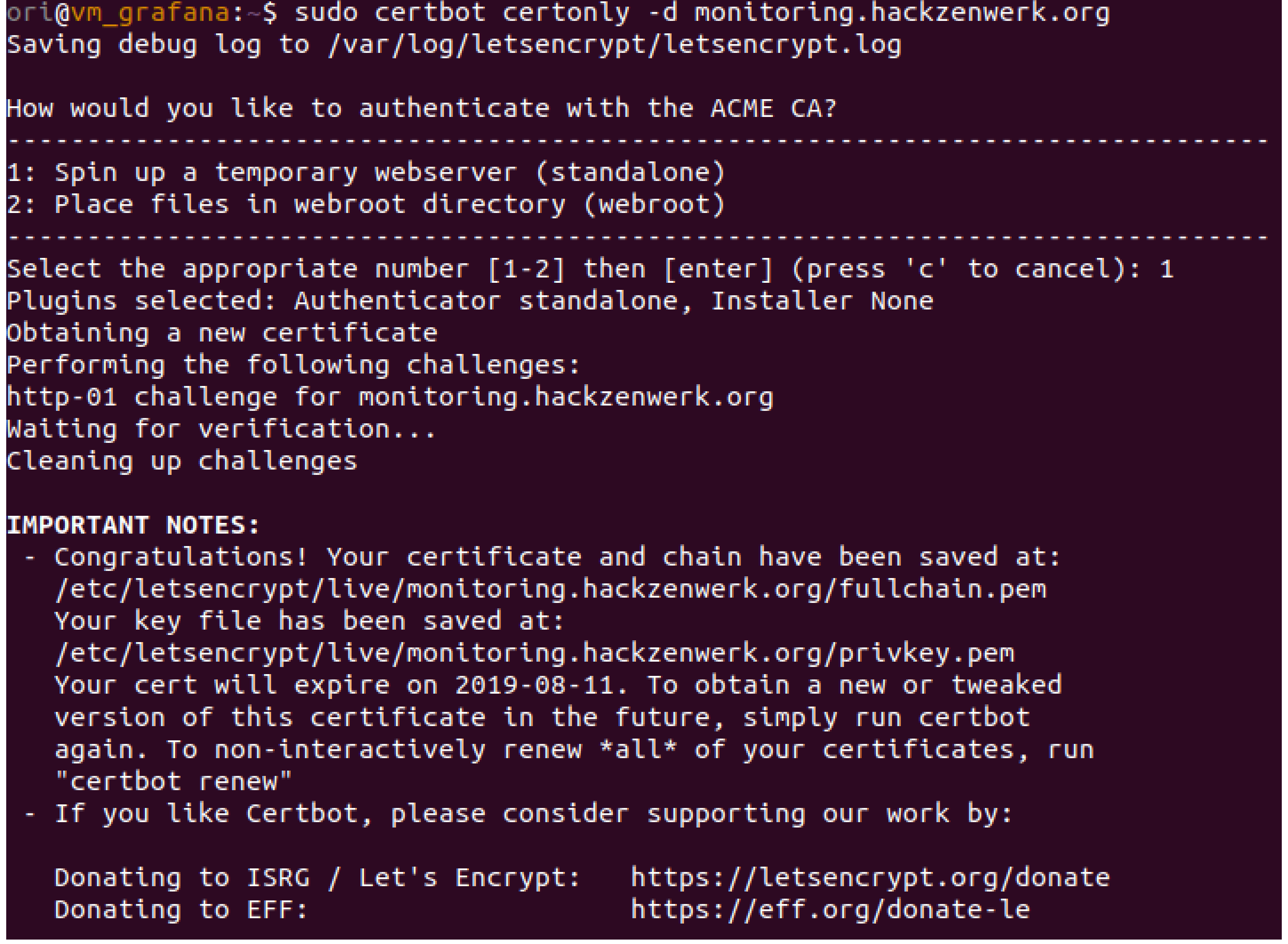
Installation

Simply follow along the instructions of the official guide on the Grafana website.

LetsEncrypt

To secure our webserver with valid SSL certificates we generate an certificate using LetsEncrypt
Ubuntu comes with certbot installed nativley.

```
sudo certbot certonly -d your.website
```



```
ori@vm_grafana:~$ sudo certbot certonly -d monitoring.hackzenwerk.org
Saving debug log to /var/log/letsencrypt/letsencrypt.log

How would you like to authenticate with the ACME CA?
-------------------------------------------------------------------------------
1: Spin up a temporary webserver (standalone)
2: Place files in webroot directory (webroot)
-------------------------------------------------------------------------------
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Plugins selected: Authenticator standalone, Installer None
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for monitoring.hackzenwerk.org
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/monitoring.hackzenwerk.org/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/monitoring.hackzenwerk.org/privkey.pem
   Your cert will expire on 2019-08-11. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

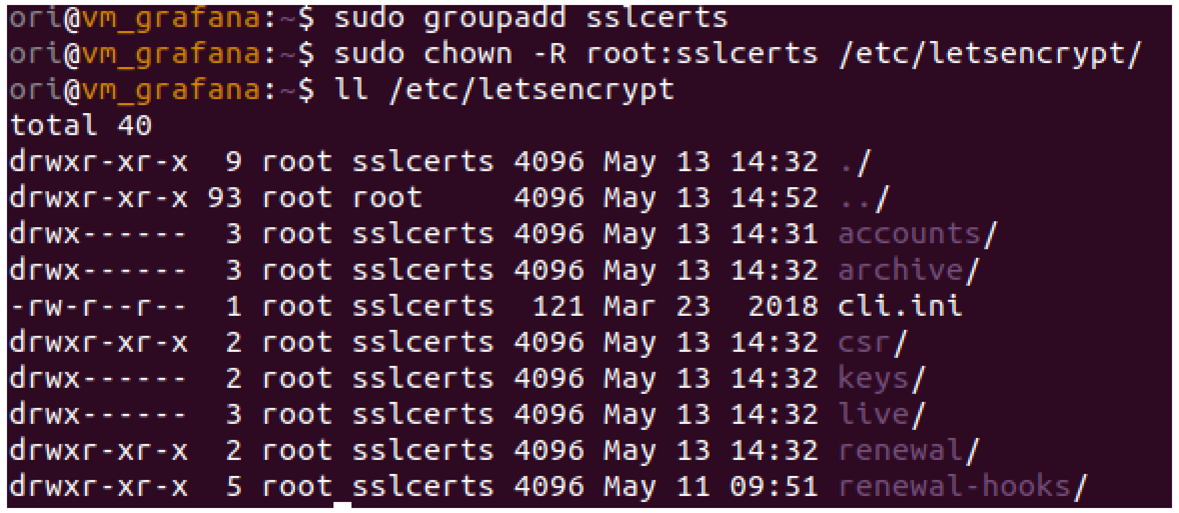
Write down the fullchain.pem and privkey.pem path.
You will later put that into the grafana.ini configuration file.

Before we do that, we have to make sure grafana can access these certificates.
To do that we create a new group.

```
sudo groupadd sslcerts
```

/etc/letsencrypt is owned by the user root and the group root.
We will change the group ownership recursivley to sslcerts.

```
user chown -R root:sslcerts /etc/letsencrypt/
```



```
ori@vm_grafana:~$ sudo groupadd sslcerts
ori@vm_grafana:~$ sudo chown -R root:sslcerts /etc/letsencrypt/
ori@vm_grafana:~$ ll /etc/letsencrypt
total 40
drwxr-xr-x  9 root sslcerts 4096 May 13 14:32 ./
drwxr-xr-x 93 root root     4096 May 13 14:52 ../
drwx------  3 root sslcerts 4096 May 13 14:31 accounts/
drwx------  3 root sslcerts 4096 May 13 14:32 archive/
-rw-r--r--  1 root sslcerts  121 Mar 23  2018 cli.ini
drwxr-xr-x  2 root sslcerts 4096 May 13 14:32 csr/
drwx------  2 root sslcerts 4096 May 13 14:32 keys/
drwx------  3 root sslcerts 4096 May 13 14:32 live/
drwxr-xr-x  2 root sslcerts 4096 May 13 14:32 renewal/
drwxr-xr-x  5 root sslcerts 4096 May 11 09:51 renewal-hooks/
```

Now we will add the user grafana (added when installing grafana) to this grop.

Now we will have to adjust the permissions of /etc/letsencrypt/live and /etc/letsencrypt/archive

```
sudo chmod 755 /etc/letsencrypt/live
sudo chmod 755 /etc/letsencrypt/archive
```

Editing the configfile /etc/grafana/grafana.ini

You will have to change the following lines:

```
30 [server]
31 # Protocol (http, https, socket)
32 protocol = https
```

```
37 # The http port to use
38 http_port = 443
```

```
40 # The public facing domain name used to access grafana from a browser
41 domain = your.grafana.url
```

```
47 # The full public facing url you use in browser, used for redirects and emails
48 # If you use reverse proxy and sub path specify full url (with sub path)
49 root_url = https://your.grafana.url
```

```
60 # https certs & key file
61 cert_file = /etc/letsencrypt/live/your.grafana.url/fullchain.pem
62 cert_key = /etc/letsencrypt/live/your.grafana.url/privkey.pem
```

Empowering Grafana to bind 443

The grafana service is not running as root.
This is why in the default configuration a ein highport is beeing used for the webserver.

But we want to use 443…

To do this without granting grafana super user, we explicitly allow it to bind ports below 1024 using setcap.

```
sudo setcap 'cap_net_bind_service=+ep' /usr/sbin/grafana-server
```

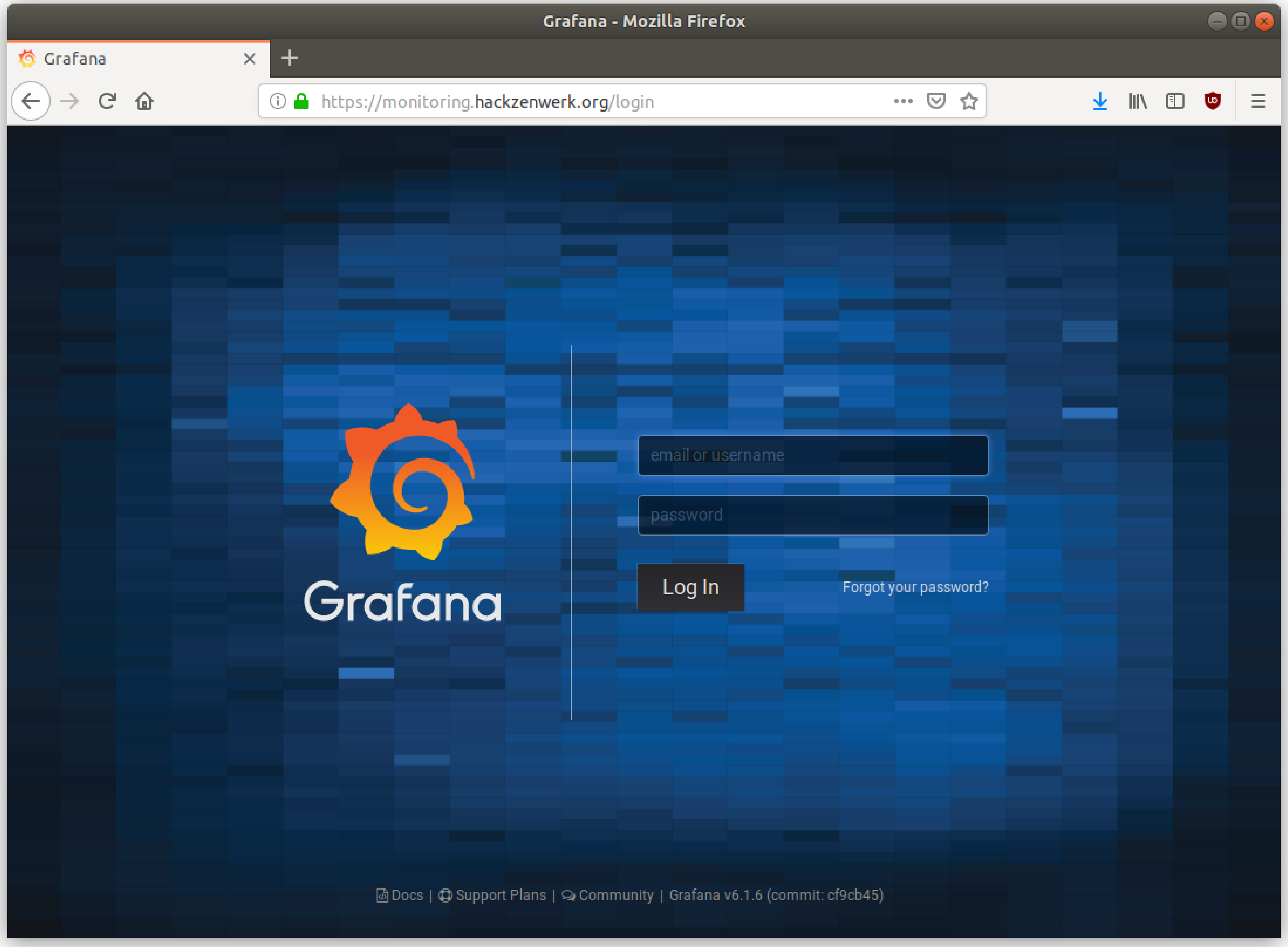
Further read:
https://wiki.apache.org/httpd/NonRootPortBinding
https://wiki.archlinux.org/index.php/Capabilities

Now, finally, restart the grafana service.

```
sudo systemctl restart grafana-server.service
```

If you have done everything right, a clean HTTPS should be greeting you.
If it does not work, a look into the logfile can be quite helpful.

```
sudo tail -f /var/log/grafana/grafana.log
```


Grafana - Mozilla Firefox
Grafana
https://monitoring.hackzenwerk.org/login
Grafana
email or username
password
Log In
Forgot your password?
Docs | Support Plans | Community | Grafana v6.1.6 (commit: cf9cb45)

At this webinterface you can now login using admin admin.
You will be asked to change that password on the first login.

Now you can carry on using this guid: https://grafana.com/docs/guides/getting_started/

Cheers,
Ori

3 COMMENTS

Thomas

REPLY

Was looking for these instructions hish and low to tighten up Grafana running on AWS. No issue following your excellent guide. However the server doesn’t start aparently because of permission issues

sanitised the URL to Grafana

```
ubuntu@ip-172-31-14-87:~$ sudo tail -f /var/log/grafana/grafana.log
t=2020-06-06T02:59:19+0000 lvl=info msg=”Writing PID file” logger=server path=/var/run/grafana/grafana-server.pid
pid=35125
t=2020-06-06T02:59:19+0000 lvl=info msg=”Connecting to DB” logger=sqlstore dbtype=sqlite3
t=2020-06-06T02:59:19+0000 lvl=info msg=”Starting DB migration” logger=migrator
t=2020-06-06T02:59:19+0000 lvl=info msg=”Starting plugin search” logger=plugins
t=2020-06-06T02:59:19+0000 lvl=info msg=”Registering plugin” logger=plugins name=”Direct Input”
t=2020-06-06T02:59:19+0000 lvl=info msg=”Registering plugin” logger=plugins name=Histogram
t=2020-06-06T02:59:19+0000 lvl=info msg=”HTTP Server Listen” logger=http.server address=[::]:443 protocol=https
subUrl= socket=
t=2020-06-06T02:59:19+0000 lvl=eror msg=”Stopped HTTPServer” logger=server reason=”open /etc/letsencrypt/live/
—————/privkey.pem: permission denied”
t=2020-06-06T02:59:19+0000 lvl=eror msg=”A service failed” logger=server err=”open /etc/letsencrypt/live/
—————/privkey.pem: permission denied”
t=2020-06-06T02:59:19+0000 lvl=eror msg=”Server shutdown” logger=server reason=”open /etc/letsencrypt/live/
—————/privkey.pem: permission denied”
```

which is strange as the permissions look alright – sanitised the URL to Grafana

```
ubuntu@ip-172-31-14-87:~$ ll /etc/letsencrypt/live/—————
total 12
drwxr-xr-x 2 root sslcerts 4096 Jun 6 02:11 ./
drwxr-xr-x 3 root sslcerts 4096 Jun 6 02:11 ../
-rw-r–r– 1 root sslcerts 692 Jun 6 02:11 README
lrwxrwxrwx 1 root sslcerts 44 Jun 6 02:11 cert.pem -> ../../archive/—————/cert1.pem
lrwxrwxrwx 1 root sslcerts 45 Jun 6 02:11 chain.pem -> ../../archive/—————/chain1.pem
lrwxrwxrwx 1 root sslcerts 49 Jun 6 02:11 fullchain.pem -> ../../archive/—————/fullchain1.pem
lrwxrwxrwx 1 root sslcerts 47 Jun 6 02:11 privkey.pem -> ../../archive/—————/privkey1.pem
ubuntu@ip-172-31-14-87:~$
```

However if I look at the archive directory I get a different set of permissions eventhough this would have been addressed via the command ‘sudo chmod 755 /etc/letsencrypt/archive

```
ubuntu@ip-172-31-14-87:~$ ll /etc/letsencrypt/archive/—————
total 24
drwxr-xr-x 2 root sslcerts 4096 Jun 6 02:11 ./
drwxr-xr-x 3 root sslcerts 4096 Jun 6 02:11 ../
-rw-r–r– 1 root sslcerts 1923 Jun 6 02:11 cert1.pem
-rw-r–r– 1 root sslcerts 1647 Jun 6 02:11 chain1.pem
-rw-r–r– 1 root sslcerts 3570 Jun 6 02:11 fullchain1.pem
-rw——- 1 root sslcerts 1704 Jun 6 02:11 privkey1.pem
ubuntu@ip-172-31-14-87:~$
ubuntu@ip-172-31-14-87:~$
```

Ori

REPLY

June 23, 2020, 8:40 am

Hello,

sorry for the delayed response.
Don’t check this block that often anymore.

Having the the certs readable by sslcerts should be enaugh.
Did you verify that your grafana user is a member of that group?

Dsfds

REPLY

June 19, 2020, 10:27 am

```
# Change ownership of the directory the certificates are stored in to the root user and the grafana users’ group.
sudo chown -R root:grafana /etc/letsencrypt/live/blabla.com
# Allow the group which owns the directory to open and list the content of the directory.
sudo chmod 750 /etc/letsencrypt/live/blabla.com
# Grant reading-rights for all certificates inside of the blabla.com directory to the group.
sudo chmod 640 /etc/letsencrypt/live/blabla.com/*
```

ADD COMMENT

Name *

Email *

Website

POST COMMENT

PREV NEXT