ZENTRO / DMSop / Zugriff per TLS(https) absichern (Teil 5)

Erstellt von: Jan Reichelt
Geändert am: Mi, 10 Mai, 2023 um 2:00 NACHMITTAGS

****
* Changelog:
* 20230509 csgjr: Entwurf
****

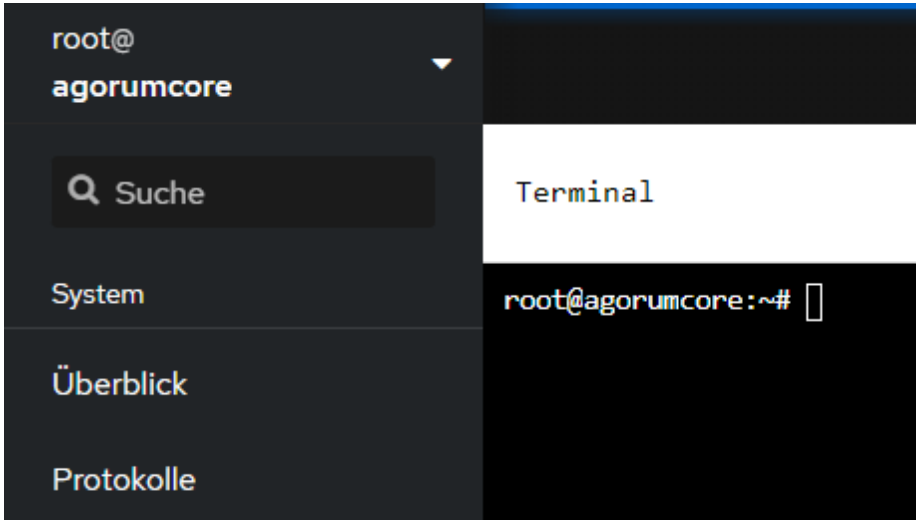
Quelle:
https://www.youtube.com/watch?v=VjMRfF7hXIg (https://www.youtube.com/watch?v=VjMRfF7hXIg)
https://community.agorum.com/forum/index.php?thread/122-agorum-core-open-mit-zertifikat-versehen-let-s-encrypt (https://community.agorum.com/forum/index.php?thread/122-agorum-core-open-mit-zertifikat-versehen-let-s-encrypt)

Um den Zugriff auf das DMS per Browser abzusichern (und der Ignoranz gegenüber https-Warnmeldungen keinen vermeidbaren Vortrieb zu gewähren) erstellen wir mittel DNS und CertBot ein Let's-Encrypt-Zertifikat.

1. Definition einer **Subdomain** (oder Domain) als FQDN und Anlage im **lokalen und öffentlichen DNS** (hier **dms.**[redacted]).
2. Verweisen des **lokalen Host-Eintrages zur IP** im DNS (hier dms.[redacted] -> 172.16.0.13):

```
C:\Users\jan01>nslookup dms.[redacted]
Server:  UnKnown
Address:  172.16.3.253

Nicht autorisierende Antwort:
Name:    dms.[redacted]
Address:  172.16.0.13
```

3. **LogIn** als root per ssh/Terminal:



4. **sudo** mittels des Befehls **apt-get install sudo** installieren:

Terminal

```
root@agorumcore:~# apt-get install sudo
Paketlisten werden gelesen… Fertig
Abhängigkeitsbaum wird aufgebaut… Fertig
Statusinformationen werden eingelesen… Fertig
Die folgenden Pakete wurden automatisch installiert und werden nicht mehr benötigt:
  linux-image-4.19.0-21-amd64 linux-image-5.10.0-18-amd64
Verwenden Sie »apt autoremove«, um sie zu entfernen.
Die folgenden NEUEN Pakete werden installiert:
  sudo
0 aktualisiert, 1 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 1.061 kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 4.699 kB Plattenplatz zusätzlich benutzt.
Holen:1 http://ftp.de.debian.org/debian bullseye/main amd64 sudo amd64 1.9.5p2-3+deb11u1 [1.061 kB]
Es wurden 1.061 kB in 1 s geholt (945 kB/s).
Vormals nicht ausgewähltes Paket sudo wird gewählt.
(Lese Datenbank ... 77823 Dateien und Verzeichnisse sind derzeit installiert.)
Vorbereitung zum Entpacken von .../sudo_1.9.5p2-3+deb11u1_amd64.deb ...
Entpacken von sudo (1.9.5p2-3+deb11u1) ...
sudo (1.9.5p2-3+deb11u1) wird eingerichtet ...
Trigger für man-db (2.9.4-2) werden verarbeitet ...
root@agorumcore:~#
```

5. **CertBot** mittels Befehl **apt install certbot** installieren:

Terminal

```
root@agorumcore:~# apt install certbot
Paketlisten werden gelesen… Fertig
Abhängigkeitsbaum wird aufgebaut… Fertig
Statusinformationen werden eingelesen… Fertig
Die folgenden Pakete wurden automatisch installiert und werden nicht mehr benötigt:
  linux-image-4.19.0-21-amd64 linux-image-5.10.0-18-amd64
Verwenden Sie »apt autoremove«, um sie zu entfernen.
Vorgeschlagene Pakete:
  python3-certbot-apache python3-certbot-nginx python-certbot-doc
Die folgenden NEUEN Pakete werden installiert:
  certbot
0 aktualisiert, 1 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 49,7 kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 89,1 kB Plattenplatz zusätzlich benutzt.
Holen:1 http://ftp.de.debian.org/debian bullseye/main amd64 certbot all 1.12.0-2 [49,7 kB]
Es wurden 49,7 kB in 0 s geholt (214 kB/s).
Vorkonfiguration der Pakete ...
Vormals nicht ausgewähltes Paket certbot wird gewählt.
(Lese Datenbank ... 77811 Dateien und Verzeichnisse sind derzeit installiert.)
Vorbereitung zum Entpacken von .../certbot_1.12.0-2_all.deb ...
Entpacken von certbot (1.12.0-2) ...
certbot (1.12.0-2) wird eingerichtet ...
Trigger für man-db (2.9.4-2) werden verarbeitet ...
root@agorumcore:~#
```

6. Ausführen des Befehls **certbot --manual --preferred-challenges dns certonly -d dms.[redacted]** zur Zertifikats-Konfiguration mittels CertBot:

Terminal

```
root@agorumcore:~# certbot --manual --preferred-challenges dns certonly -d dms.[redacted]
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
```

7. Eingabe einer **gültigen Mailadresse** für Systemmeldungen von CertBot und **Akzeptieren der Terms of Service**:

```
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): [redacted]

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
```

8. **Ablehnen** der **Weitergabe der E-Mail-Adresse** an die EFF:

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: N
```

9. Ausgabe der **benötigten Informationen** durch CertBot für die **DNS-Validierung**:

```
Requesting a certificate for dms.[redacted]
Performing the following challenges:
dns-01 challenge for dms.[redacted]

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.dms.[redacted] with the following value:

[redacted]C9N3N7GlP6E

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

10. **Anlage** des Eintrages im **öffentlichen (!) DNS**:

9	☑	_acme-challenge.dms	TXT	[redacted]C9N3N7GlP6E

11. **Testen**, dass der **Eintrag aktualisiert/gesetzt** wurde mittels nslookup:

```
C:\Users\jan01>nslookup -q=TXT _acme-challenge.dms.[redacted] 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Nicht autorisierende Antwort:
_acme-challenge.dms.[redacted]    text =

        "[redacted]C9N3N7GlP6E"
```

12. Im **CertBot-Dialog** weiter mit **ENTER** und Bestätigung der **erfolgreichen Anlage** abwarten:

```
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/dms.[redacted]/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/dms.[redacted]/privkey.pem
   Your certificate will expire on 2023-08-07. 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

root@agorumcore:~#
```

13. **Mit dem Befehl cd /etc/letsencrypt/live/dms.[redacted]/ in das entsprechende Verzeichnis wechseln:**

Terminal

```
root@agorumcore:/# cd /etc/letsencrypt/live/dms.[redacted]/
root@agorumcore:/etc/letsencrypt/live/dms.[redacted]#
```

14. Das bestehende **PEM** mit dem Befehl **openssl pkcs12 -inkey privkey.pem -in fullchain.pem -export -out fullchain.pfx** in **PFX konvertieren** und ein Kennwort dafür vergeben (temp. dokumentieren!):

```
root@agorumcore:/etc/letsencrypt/live/dms.[redacted]# openssl pkcs12 -inkey privkey.pem -in fullchain.pem -export -out fullchain.pfx
Enter Export Password:
Verifying - Enter Export Password:
root@agorumcore:/etc/letsencrypt/live/dms.[redacted]# ls
cert.pem  chain.pem  fullchain.pem  fullchain.pfx  privkey.pem  README
root@agorumcore:/etc/letsencrypt/live/dms.[redacted]#
```

15. Zu **/opt/agorum/agorumcore/scripts** wechseln und den **Server stoppen** (./agorumcore stop) (Achtung: Verbindung zum DMS wird unterbrochen!):

```
root@agorumcore:/opt/agorum/agorumcore/scripts# ./agorumcore stop

Stopping agorumcore
Shutting down MySQL..
root@agorumcore:/opt/agorum/agorumcore/scripts#
```

16. **Wechsel** in den Pfad **/opt/agorum/agorumcore/java/bin**:

```
root@agorumcore:/opt/agorum/agorumcore/java/bin#
```

17. Das neu erstellte **Zertifikat importieren** mittels **./keytool -importkeystore -srckeystore /etc/letsencrypt/live/dms.[redacted]/fullchain.pfx -srcstoretype pkcs12 -destkeystore /root/.keystore**. Dabei als **Ziel-Keystore-Kennwort** den Default **changeit** von agorum nutzen. Und als **Quell-Keystore-Kennwort** das zuvor bei der PFX-Konvertierung gesetzte Kennwort:

```
root@agorumcore:/opt/agorum/agorumcore/java/bin# ./keytool -importkeystore -srckeystore /etc/letsencrypt/live/dms.[redacted]/fullchain.pfx -srcstoretype pkcs12 -destkeystore /root/.keystore
Keystore /etc/letsencrypt/live/dms.[redacted]/fullchain.pfx wird in /root/.keystore importiert...
Ziel Keystore Kennwort eingeben:
Quell-Keystore-Kennwort eingeben:
Eintrag für Alias 1 erfolgreich importiert.
Importbefehl abgeschlossen: 1 Einträge erfolgreich importiert, 0 Einträge nicht erfolgreich oder abgebrochen

Warning:
Der JKS-Keystore verwendet ein proprietäres Format. Es wird empfohlen, auf PKCS12 zu migrieren, das ein Industriestandardformat mit "keytool -importkeystore -srckeystore /root/.keystore -destkeystore /root/
keystore -deststoretype pkcs12" ist.
root@agorumcore:/opt/agorum/agorumcore/java/bin#
```

18. Altes Zertifikat mittels **./keytool -delete -alias tomcat -keystore /root/.keystore** und dem Keystore-Kennwort **changeit** löschen:

```
root@agorumcore:/opt/agorum/agorumcore/java/bin# ./keytool -delete -alias tomcat -keystore /root/.keystore
Keystore-Kennwort eingeben:

Warning:
Der JKS-Keystore verwendet ein proprietäres Format. Es wird empfohlen, auf PKCS12 zu migrieren, das ein Industriestandardformat mit "keytool -importkeystore -srckeystore /root/.keystore -destkeystore /root/
keystore -deststoretype pkcs12" ist.
root@agorumcore:/opt/agorum/agorumcore/java/bin#
```

19. Das zuvor beim Import erzeugte Alias (hier 1) zum **Ziel-Alias tomcat** mit dem Befehl **./keytool -changealias -alias 1 -destalias tomcat -keystore /root/.keystore** ändern. Dabei als **Keystore-Kennwort** wieder **changeit** und als **Schlüsselkennwort für das Alias** wieder das **zuvor defnierte Kennwort** nutzen:

```
root@agorumcore:/opt/agorum/agorumcore/java/bin# ./keytool -changealias -alias 1 -destalias tomcat -keystore /root/.keystore
Keystore-Kennwort eingeben:
Schlüsselkennwort für <1> eingeben

Warning:
Der JKS Keystore verwendet ein proprietäres Format. Es wird empfohlen, auf PKCS12 zu migrieren, das ein Industriestandardformat mit "keytool -importkeystore -srckeystore /root/.keystore -destkeystore /root/
keystore -deststoretype pkcs12" ist.
root@agorumcore:/opt/agorum/agorumcore/java/bin#
```

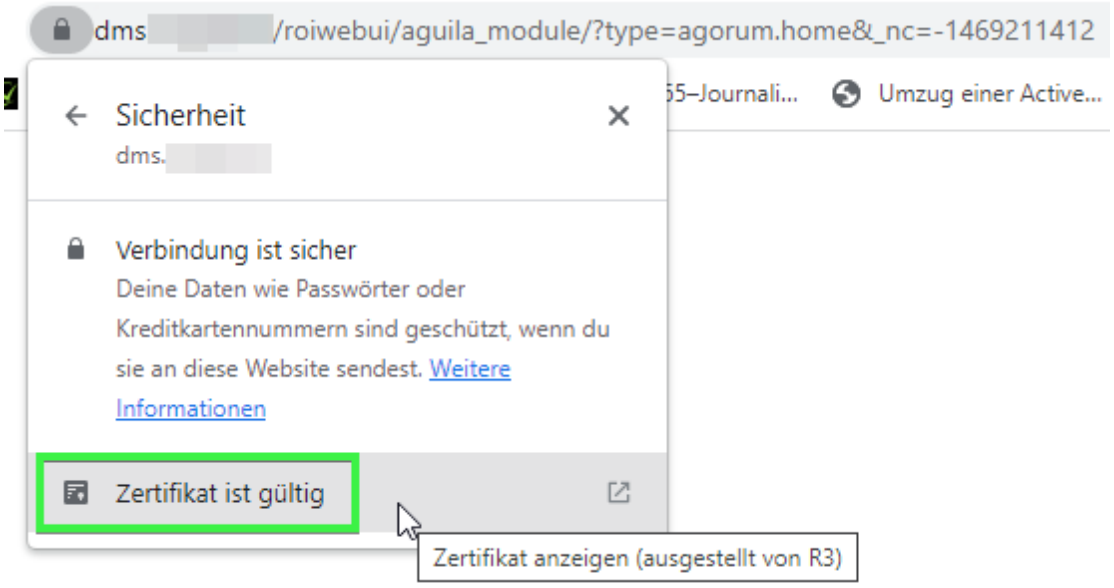
20. Mittels des Befehls **.\keytool -keypasswd -alias tomcat -keystore /root/.keystore** das Kennwort wieder auf **changeit** ändern. Dafür **changeit** für den **Keystore** nutzen. Als **Schlüsselkennwort für tomcat** das zuvor definierte. Und nun eben dieses durch die **zweimalige Eingabe** von **changeit** wieder auf den **Defaultwert zurücksetzen**:

```
root@agorumcore:/opt/agorum/agorumcore/java/bin# ./keytool -keypasswd -alias tomcat -keystore /root/.keystore
Keystore-Kennwort eingeben:
Schlüsselkennwort für <tomcat> eingeben
Neues Schlüsselkennwort für <tomcat>:
Neues Schlüsselkennwort für <tomcat> erneut eingeben:

Warning:
Der JKS-Keystore verwendet ein proprietäres Format. Es wird empfohlen, auf PKCS12 zu migrieren, das ein Industriestandardformat mit "keytool -importkeystore -srckeystore /root/.keystore -destkeystore /root/.
keystore -deststoretype pkcs12" ist.
root@agorumcore:/opt/agorum/agorumcore/java/bin#
```

21. Wechsel in das Skript-Verzeichnis mit dem Befehl **cd /opt/agorum/agorumcore/scripts** und starten von agorumcore mittels **./agorumcore start** :

```
root@agorumcore:/opt/agorum/agorumcore/java/bin# cd /opt/agorum/agorumcore/scripts
root@agorumcore:/opt/agorum/agorumcore/scripts# ./agorumcore start
Starting agorumcore
Starting MySQL.

Starting agorum core...
```

22. Ruft man jetzt die Seite auf, ist die Verbindung offiziell via Let's Encrypt für weitere 90 Tage gesichert:



J Jan ist der Autor dieses Lösungsartikels.