Graylog <> MongoDB | X.509 Zertifikat erneuern

Dieses How To bezieht sich auf Graylog Server, die sich per Zertifikat an einer (oder mehreren) MongoDB (im TLS / SSL Modus) authentifizieren!

> Es wird der vorhandene private Key des "OPENSEARCH-ADMIN" sowie die RootCA benötigt (wenn PKI Infrastruktur vorliegt).

> Das Zertifikat wird hier per Windows PKI ausgestellt

1. **per OpenSSL eine CSR von vorigen Zertifikat erstellen**

OPENSEARCH-ADMIN openssl.cnf Vorlage (Anpassung erforderlich!):

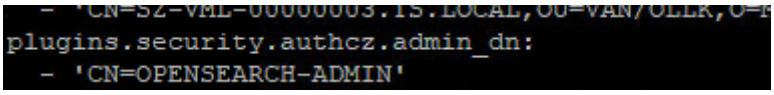
```
[ req ]
default_bits        = 2048
default_md          = sha256
prompt              = no
distinguished_name  = req_distinguished_name
req_extensions      = req_ext

[ req_distinguished_name ]
CN = OPENSEARCH-ADMIN

[ req_ext ]
extendedKeyUsage    = clientAuth, serverAuth
```

> Die CSR kann für die Zertifikatsanforderung nun genutzt werden

> Der DN muss mit dem vorigen DN übereinstimmen! Kann hier gefunden werden: /etc/opensearch/opensearch.conf

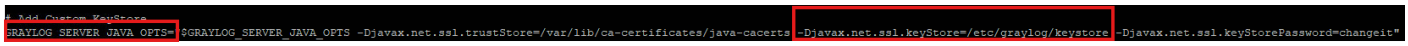


> openssl req -new -key SERVER1-privatekey.pem -out SERVER1-certRequest.csr -config openssl.cnf

> Das Zertifikat muss als BASE64 / X.509 vorliegen und darf nicht verschlüsselt sein!

2. JAVA KEYSTORE von Graylog / Opensearch finden

```
cat /etc/sysconfig/graylog-server
```



Das neue Zertifikat muss nun auf den Server kopiert werden (öffnen per **Texteditor / Notepad** und kopieren des Inhalts aus der frisch erstellten ***.cer**). Danach kann der Inhalt per ***vim / nano*** auf dem Graylog Server in die neue Datei **admin-cert.pem** eingefügt werden)

3. PKCS12 Datei erstellen, um diese in KEYSTORE hinzuzufügen

```
openssl pkcs12 -export \
    -out admin.p12 \
    -inkey admin-key.pem \
    -in admin-cert.pem \
    -certfile root-ca.pem  # Optional, wenn du ein CA-Bundle hast
```

> Das Kennwort der PKCS12 Datei muss gleich dem JAVA KEYSTORE sein!

4. p12 Datei in JAVA KEYSTORE importieren

```
sudo keytool -importkeystore \
    -srckeystore admin.p12 \
    -srcstoretype PKCS12 \
    -destkeystore /etc/graylog/keystore \
    -deststoretype JKS \
    -storepass changeit
```

>

> Server neustarten, danach ist das Zertifikat erneuert :)

Revision #15
Created 2024-09-24 10:30:08 UTC by Tom Behrendt
Updated 2024-09-24 12:14:32 UTC by Tom Behrendt