Certifikathantering i Ladok

Fredrik Domeij
Ladok Operations
2024-02-08

Bakgrund

- Ladoks utvecklings- och driftmiljöer använder knappt 200 unika TLS-certifikat
- Beställning sker idag manuellt via ett shell-script mot Sectigos REST-API
- Certifikaten är giltiga i 12 månader, vi förlänger dom var 6:e månad för att
  - inte få en förskjutning på certifikatsförlängningarna
  - inte glömma hur det går till
  - identifiera vad som behöver automatiseras
- Varje medarbetare inom Ladok Operations har ett eget konto på https://cert-manager.com/customer/sunet
- De flesta certifikaten scriptas in i Ansible vaults eller läggs manuellt in i HashiCorp Vault och levereras ut till servrar via Ansible

Ladok

Beställa certifikat syntax

```
# ./request-certificate.sh --help
Usage: ./request-certificate.sh <cn|file.csr> [subject-alternative-name] ...
Ex:    ./request-certificate.sh ladok00.utv.ladok.se
       ./request-certificate.sh /tmp/play.ladok.se.csr
       ./request-certificate.sh '*.ufhsk.ladok.se' ufhsk.ladok.se

# read API_USER
myusername

# read -s API_PASS
mysecretpassword

# export API_USER API_PASS
```

Ladok

Beställa certifikat kod

```
#!/bin/bash
cn=$1

orgid="11732"           # "Ladok.se"
certtype=9249           # GEANT OV Multi-Domain
api_customeruri=sunet

subject="/C=SE/O=Umea universitet/OU=ITS/CN=$cn"
```

```
mkdir -p "certs/$cn"

file_done=certs/$cn/done
file_sslid=certs/$cn/sslid
file_key=certs/$cn/$cn.key
file_csr=certs/$cn/$cn.csr
file_crt=certs/$cn/$cn.crt
file_chain=certs/$cn/certificate_chain.pem
```

```
openssl genrsa -out "$file_key" 4096
openssl req -new -subj "$subject" -key "$file_key" -out "$file_csr"
```

Ladok

Beställa certifikat kod (forts.)

```
json="{
        \"orgId\" : $orgid,
        \"csr\" : \"$(cat $file_csr)\",
        \"certType\" : $certtype,
        \"numberServers\" : 0,
        \"serverType\" : -1,
        \"term\" : 365
}”
```

```
output=$(curl -s -X POST
    -H "Content-type: application/json”
    -H "login: $api_user”
    -H "password: $api_pass”
    -H "customerUri: $api_customeruri”
    -d "$json”
    https://cert-manager.com/api/ssl/v1/enroll)
```

```
sslid=$(echo "$output" | sed -n 's/^{.*"sslId":\([0-9]*\).*}$/\1/p')
echo "$sslid" > "$file_sslid"
```

Ladok

Beställa certifikat exempel

```
# ./request-certificate.sh testcert.ladok.se
Hello fredrik.domeij@umu.se
Generating RSA private key, 4096 bit long modulus (2 primes)
.........................++++
..............................++++
e is 65537 (0x010001)
testcert.ladok.se SUCCESS
```

Ladok

Hämta certifikat kod

```
#!/bin/bash

for certdir in certs/* ; do
        # Already downloaded?
        test -r "$file_done" && continue

        sslid=$(cat "$file_sslid")

        output=$(curl -s -X GET
            -H "Content-type: application/json"
            -H "login: $api_user"
            -H "password: $api_pass"
            -H "customerUri: $api_customeruri"
            "https://cert-manager.com/api/ssl/v1/collect/$sslid/base64")
```

Ladok

Hämta certifikat kod (forts.)

```
        if echo "$output" | grep -q 'Being processed by Sectigo' ; then
                echo "Order $cn pending"
                continue
        fi

        output=$(echo "$output" | openssl pkcs7 -print_certs)
        echo "$output" | sed '/END CERTIFICATE/q' > "$file_crt"

        echo "$cn OK"
        touch "$file_done"
done
```

Ladok

Hämta certifikat exempel

```
# ./retrieve-certificates.sh
Hello fredrik.domeij@umu.se
Order testcert.ladok.se pending

# ./retrieve-certificates.sh
Hello fredrik.domeij@umu.se
-rw-r--r--. 1 root root 2451  7 feb 15.02 certs/testcert.ladok.se/testcert.ladok.se.crt
-rw-------. 1 root root 3243  7 feb 14.36 certs/testcert.ladok.se/testcert.ladok.se.key
-rw-r--r--. 1 root root 2955  7 feb 15.02 certs/testcert.ladok.se/testcert.ladok.se.pem
testcert.ladok.se OK
```

Ladok

Ladok

Frågor?

Fredrik Domeij
fredrik.domeij@umu.se