

SSL configuration on JBoss EAP 6.4

Contents

- 1 SSL beállítása
 - ◆ 1.1 SSL kulcsok legyártása
 - ◆ 1.2 Aláírás kér? legyártása a titkos kulcsból
 - ◆ 1.3 Cert legyártása
 - ◆ 1.4 PKCS12 keystore legyártása
- 2 Java keystore
 - ◆ 2.1 Keystore létrehozása
 - ◆ 2.2 ca importálása
 - ◆ 2.3 pkcs12 keystore importálása
 - ◆ 2.4 Keystore karbantartás
 - ◇ 2.4.1 Java keystore listázása
 - ◇ 2.4.2 Törlés a keystore-ból
- 3 JBoss beállítások

SSL beállítása

Korábban már létrehoztuk az autentikációs hatóságot (mycompany-ca.pem) ami aláírta az myproject.mycompany.hu és az jenkins.mycompany.hu tanúsítványokat. A lokális szerver példányt is csak https eléréssel lehet futtatni a HTTPs sütik használata miatt. Két lehetőségünk van. Vagy elé teszünk egy apache-t, ami https-en fut, vagy beállítjuk a jboss-ban a https használatát. Én az utóbbit használtam.

Az alternat-ca-t már korábban importáltuk a böngészőbe mint cert hatóság, így minden általa aláírt cert-et el fog fogadni a böngésző, ami különösen Chrome-ban hasznos, mert nem lehet permanensen elfogadni.

SSL kulcsok legyártása

Lokális szerver privát kulcsa

```
$ openssl genrsa -out myproject.mycompany.local-server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
```

Aláírás kér? legyártása a titkos kulcsból

Az aláírás kér? már tartalmazza a domain nevet is, a lényeg itt, hogy az aláíró hatóság azt bizonyítja, hogy a cert a domain névhez tartozik.

Ez a Common Name paraméter, ezt nem szabad elrontani. Az itt megadott névvel lehet csak elérni a szervert (myproject.mycompany.local). Ezt majd fel kell venni a host fájlba, hogy a localhost-ra mutasson.

```
$ openssl req -new -key myproject.mycompany.local-server.key -out myproject.mycompany.local-server.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:HU
State or Province Name (full name) []:BUD
Locality Name (eg, city) [Default City]:BUD
Organization Name (eg, company) [Default Company Ltd]:mycompany Zrt.
Organizational Unit Name (eg, section) []:myproject
Common Name (eg, your name or your server's hostname) []:myproject.mycompany.local <<<----- az egyetlen fontos paraméter
Email Address []:berki.adam@mycompany.hu
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Cert legyártása

Írjuk alá a korábban már használt mycompany-ca -val az aláírás kér?t.

```
$ openssl x509 -req -in myproject.mycompany.local-server.req -CA mycompany-ca.pem -CAkey mycompany-ca.key -set_serial 102 -days 3650 -outform
```

PKCS12 keystore legyártása

A titkos kulcsunkból és a hozzá tartozó cert-ből csinálni kell egy PKCS12 keystore fájlt, ami mind a kettőt tartalmazza, mert csak így lehet a java keystore-ba importálni.



Note

Fontos, hogy adjunk meg jelszót a keystore-hoz, mert mikor majd a java keystore-ba importáljuk, panaszkondi fog, ha nincs jelszó

A PKCS12 keystore legyártásakor a keystore-t el kell nevezni a -name paraméterben. Az itt megadott név fontos lesz a java keystore-ba való importáláskor, ezzel a névvel kell majd rá hivatkozni, máshogy nem lehet importálni.

```
$ openssl pkcs12 -export -name myprojectlocalcert -in myproject.mycompany.local-server.cer -inkey myproject.mycompany.local-server.key -out m
Enter Export Password:
Verifying - Enter Export Password:
```

Java keystore

Keystore létrehozása

Hozzunk létre egy üres keystore-t a JBoss bin mappájában:

```
$ /usr/lib/jvm/jdk1.8.0_45/bin/keytool -genkey -alias jbossStore -keyalg RSA -keystore /home/adam/runable/jboss/EAP-6.4.0_second/bin/myproject
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Adam Berki
What is the name of your organizational unit?
[Unknown]: mycompany Zrt.
What is the name of your organization?
[Unknown]: myproject
What is the name of your City or Locality?
[Unknown]: BUD
What is the name of your State or Province?
[Unknown]: BUD
What is the two-letter country code for this unit?
[Unknown]: HUN
Is CN=Adam Berki, OU=mycompany Zrt., O=myproject, L=BUD, ST=BUD, C=HUN correct?
[no]: yes
Enter key password for <jbossStore>
(RETURN if same as keystore password):
Re-enter new password:
```

ca importálása

Rakjuk be a keystore-a az mycompany-ca cert. hatóságot, hogy a szerverünk is megbízzon mindenkiben akinek a kulcsát ezzel írtuk alá:

```
$ /usr/lib/jvm/jdk1.8.0_45/bin/keytool -import -alias mycompanyAtuth -keystore /home/adam/runable/jboss/EAP-6.4.0_second/bin/myproject.keystore
Enter keystore password:
Owner: EMAILADDRESS=berki.adam@mycompany.hu, CN=ca.mycompany.hu, OU=mycompany-CA Divison, O=mycompany Zrt, L=Budapest, C=HU
Issuer: EMAILADDRESS=berki.adam@mycompany.hu, CN=ca.mycompany.hu, OU=mycompany-CA Divison, O=mycompany Zrt, L=Budapest, C=HU
Serial number: 92484dba84d2d5ee
Valid from: Fri Oct 07 13:26:23 CEST 2016 until: Mon Oct 05 13:26:23 CEST 2026
Certificate fingerprints:
MD5: 3D:BC:11:FC:E2:DD:C4:FE:50:CA:CF:34:B3:84:EF:5C
SHA1: 3C:90:F0:45:F7:EF:37:92:D1:9B:AE:E5:2B:B8:67:26:8F:26:1F:6E
SHA256: 2E:EC:FB:C6:F5:33:0D:6A:43:41:A8:BE:11:A3:E8:A0:3F:21:18:82:CB:89:02:7C:0A:28:76:41:8C:58:AA:94
Signature algorithm name: SHA256withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 6E 60 BB 76 75 06 22 3F D7 6E 63 1B 52 00 F3 2A n`.vu."?.nc.R..*
0010: 83 7A F9 7C .z..
]
]
#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 6E 60 BB 76 75 06 22 3F D7 6E 63 1B 52 00 F3 2A n`.vu."?.nc.R..*
0010: 83 7A F9 7C .z..
]
]
Trust this certificate? [no]: yes
Certificate was added to keystore
```

pkcs12 keystore importálása

Töltsük be a korábban létrehozott pkcs12 keystore-t amiben a myproject.mycompany.local cert-je és titkos kulcsa van.



Note

Fontos hogy az -alias paraméterben azt adjuk meg, amit a pkcs12 létrehozásakor a -name paraméterben megadtunk. Els?ként meg kell adni a pkcs12 kulcsát majd a java keystore kulcsát

```
$ /usr/lib/jvm/jdk1.8.0_45/bin/keytool -importkeystore -destkeystore /home/adam/runable/jboss/EAP-6.4.0_second/bin/myproject.keystore -srckeystore
Enter destination keystore password:
Enter source keystore password:
```

Keystore karbantartás

Java keystore listázása

```
$ /usr/lib/jvm/jdk1.8.0_45/bin/keytool -list -keystore /home/adam/runable/jboss/EAP-6.4.0_second/bin/myproject.keystore
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 3 entries
```

```
mycompanyatuth, Oct 26, 2016, trustedCertEntry,  
Certificate fingerprint (SHA1): 3C:90:F0:45:F7:EF:37:92:D1:9B:AE:E5:2B:B8:67:26:8F:26:1F:6E
```

```
jbossstore, Oct 26, 2016, PrivateKeyEntry,  
Certificate fingerprint (SHA1): 89:B5:FD:07:08:4B:C0:E4:6C:4F:B9:A1:BF:6E:7A:8C:B0:C1:14:92
```

```
myprojectlocalcert, Oct 27, 2016, PrivateKeyEntry,  
Certificate fingerprint (SHA1): 5D:4C:B1:21:48:43:7C:2A:04:DD:E3:BB:B2:FD:34:2E:80:EC:69:EB
```

Törlés a keystore-bol

```
$ /usr/lib/jvm/jdk1.8.0_45/bin/keytool -delete -alias myprojectlocalcert -keystore /home/adam/runable/jboss/EAP-6.4.0_second/bin/myproject.keystore
```

JBoss beállítások

A standalone.xml-ben a **urn:jboss:domain:web:2.2** modult cseréljük ki az alábbira. Fontos, hogy a key-alias paraméterben a pkcs12 kulcs importálásakor megadott alias-t használjuk, hogy a java keystore-bol ki tudja választani a szerver, hogy melyik titkos kulcsot használja. A java keystore jelszavát is meg kell adni, hogy a JBoss tudjon olvasni belőle.

```
<profile>  
  <subsystem xmlns="urn:jboss:domain:web:2.2" default-virtual-server="default-host" native="false">  
    <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http" secure="true"/>  
    <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">  
      <ssl name="https" key-alias="myprojectlocalcert" password="liteon" certificate-key-file="/home/adam/runable/jboss/EAP-6.4.0_s  
    </connector>  
    <virtual-server name="default-host" enable-welcome-root="true">  
      <alias name="myproject.mycompany.local"/>  
    </virtual-server>  
  </subsystem>  
  <subsystem xmlns="urn:jboss:domain:weld:1.0"/>  
</profile>
```

Az alkalmazás itt érhető el: <https://myproject.mycompany.local:8443/myproject/Login/Login.do> A böngészőnek el kell fogadnia a cert-et.