

Linux

This script automates the re-generation of a keystore file to enable SSL for Tomcat and postfix based on certificates obtained through letsencrypt.

```
#!/bin/bash

if [ ! -f "/etc/cert_gen_tomcat" ]; then
  echo "Config file /etc/cert_gen_tomcat does not exist"
  exit 1;
fi
source /etc/cert_gen_tomcat

if [ ! -f /usr/local/bin/certbot-auto ]; then
  wget -q https://dl.eff.org/certbot-auto >/usr/local/bin/certbot-auto
  chmod a+x /usr/local/bin/certbot-auto
fi

pgrep haproxy 1>/dev/null
HAPROXY=$?
if [ "$HAPROXY" -eq 0 ]; then
  service haproxy stop 1>/dev/null
fi

if [ -d "/opt/apache-tomcat" ]; then
  /opt/apache-tomcat/bin/shutdown.sh 1>/dev/null
else
  service tomcat7 stop 1>/dev/null
fi

#
# Stop if HTTP/HTTPS is already bound (as letsencrypt will start a webserver)
#
netstat -at|grep -q "https.*LISTEN"
if [ $? -eq 0 ]; then
  echo "Port 443 still bound. Exit."
  exit 1
fi
netstat -atn|grep ":80 .*LISTEN"
if [ $? -eq 0 ]; then
  echo "Port 80 still bound. Exit."
  exit 1
fi

#
# letsencrypt will re-generate the certs
#
/usr/local/bin/certbot-auto renew 1>/dev/null

if [ $? -ne 0 ]; then
  echo "letsencrypt failed. Exit."
  exit 2
fi

#
# convert PEM to p12
#
openssl pkcs12 -export -in /etc/letsencrypt/live/$DOMAIN/fullchain.pem \
-inkey /etc/letsencrypt/live/$DOMAIN/privkey.pem \
-passout pass:$PASS > /etc/letsencrypt/live/$DOMAIN/server.p12
```

Linux

```
if [ $? -ne 0 ]; then
    echo "openssl key conversion to pkcs12 failed. Exit."
    exit 3
fi

rm -f /etc/tomcat7/keystore- $\$$ DOMAIN-new 2>/dev/null

#
# create a new keystore file
#
keytool -importkeystore -srckeystore /etc/letsencrypt/live/ $\$$ DOMAIN/server.p12 \
    -destkeystore /etc/tomcat7/keystore- $\$$ DOMAIN-
new -srcstoretype pkcs12 2>/dev/null <<-EOF
$PASS
$PASS
$PASS
EOF

#
# move the new keystore file to the right location
#
if [ $? -eq 0 ]; then
    rm -f /etc/tomcat7/keystore- $\$$ DOMAIN-old 2>/dev/null
    mv /etc/tomcat7/keystore- $\$$ DOMAIN /etc/tomcat7/keystore- $\$$ DOMAIN-old
    mv /etc/tomcat7/keystore- $\$$ DOMAIN-new /etc/tomcat7/keystore- $\$$ DOMAIN

#
# postfix might also use the certificate
#
if [ -f "/etc/postfix/server.pem" ]; then
    cat /etc/letsencrypt/live/ $\$$ DOMAIN/fullchain.pem \
        /etc/letsencrypt/live/ $\$$ DOMAIN/root.pem >/etc/postfix/server.pem
    cat /etc/letsencrypt/live/ $\$$ DOMAIN/privkey.pem >/etc/postfix/privkey.pem

    service postfix restart 1>/dev/null
fi

EXIT_CODE=0
else
    echo "keystore creation failed. Restarting tomcat with old certificate."
    EXIT_CODE=4
fi

if [ "$HAPROXY" -eq 0 ]; then
    service haproxy start 1>/dev/null
fi

if [ -d "/opt/apache-tomcat" ]; then
    /opt/apache-tomcat/bin/startup.sh 1>/dev/null
else
    service tomcat7 start 1>/dev/null
fi

exit  $\$$ EXIT_CODE
```

Linux

Quelle: https://github.com/oglimmer/cert_gen_tomcat/blob/master/cert_gen.sh

Eindeutige ID: #1066

Verfasser: n/a

Letzte Änderung: 2016-07-18 23:14