Certificate and revocation Archival for EJBCA

Introduction

From syscheck 1.2 and on there is a script-based archival solution.

New and revoked certificates are stored on local disk in a file-tree and optional remote SSH server.

Setup of syscheck

First we need to configure 917_archive_file.sh that is a general archiving script.
Do that by edit <syscheck>/conf/917.conf, make the directories “InTransitDir” and “ArchiveDir”. Also make sure that users of 917_archive_file.sh can write to those directories. InTransitDir will be used as a temporary location when transferring files to remote hosts. ArchiveDir is the final destination on localhost.

```
# config for 917_archive_file.sh
InTransitDir=/misc/cert-archive/intransit
ArchiveDir=/misc/cert-archive/archive

#OUTFILE="${OUTPATH2}/archived-crl-${DATE}-${CRLLASTUPDATE2}-${CRLISSUER2}"
OUTFILE="${OUTPATH2}/${CRLISSUER2}"
```

Now we'll configure the destinations for cert-, crl- and revocationarchiving.
Edit <syscheck>/config/900.conf with your destinations.

```
# config for related-available/900_export_cert.sh

### config ###
OUTPATH=/misc/cert-archive/local
CERTLOG=${OUTPATH}/exportcert.log
DATE=`date +'%Y-%m-%d_%H.%m.%S'`
DATE2=`date +'%Y/%m/%d'`

OUTPATH2="${OUTPATH}/${DATE2}"

# If you configure one or more REMOTE_HOST:s the archived certificate will also be stored on that host
REMOTE_HOST[0]="192.168.158.131"
REMOTE_USER[0]='htmf'
REMOTE_DIR[0]='/misc/cert-archive/'
SSHKEY[0]='/home/han/.ssh/id_rsa'

REMOTE_HOST[1]="127.0.0.1"
REMOTE_USER[1]='han'
REMOTE_DIR[1]='/misc/cert-archive/'
SSHKEY[1]='/home/han/.ssh/id_rsa'
```

```
### end config ###
```

You can add more destinations just copy the config block and add “1” to the config index.
Like this:

```
REMOTE_HOST[2]="127.0.0.1"
REMOTE_USER[2]='han'
REMOTE_DIR[2]='/misc/cert-archive/'
SSHKEY[2]='/home/han/.ssh/id_rsa'
```

Do the same with
<syscheck>/config/901.conf (config for 901_export_revocation.sh)
and
<syscheck>/config/902.conf (config for 902_export_crl.sh)

Setup of publisher

Go to: EJBCA Adminweb → ”Edit Publishers” → Add new name: ”Archival publisher”

Select/ enter the following:

Publisher Type: ”Custom Publisher”

Class Path: ”org.ejbca.core.model.ca.publisher.GeneralPurposeCustomPublisher”

Properties of Custom Publisher:

crl.application /path/to/syscheck/related-enabled/902_export_crl.sh

crl.failOnStandardError true

crl.failOnErrorCode true

cert.application /path/to/syscheck/related-enabled/900_export_cert.sh

cert.failOnStandardError true

cert.failOnErrorCode true

revoke.application /path/to/syscheck/related-enabled/901_export_revocation.sh

revoke.failOnStandardError true

revoke.failOnErrorCode true

Use the publisher on CA:s

Go to: EJBCA Adminweb → ”Edit Certificate Authorites”

Select the CA you want CRL archival on, then click on edit CA

At ”CRL Publishers”:

Select ”Archival publisher”

Do this for all CA:s you want CRL Archival for.

Use the publisher on Certificate profile:s

Go to: EJBCA Adminweb → ”Edit Certifcate Profiles”

At: ”Publishers”

Select ”Archival publisher”

Do this for all Certificate profiles:s you want Certifcate Archival for.