

Invalidacija lokalnih kopija CRL



Znamo da Certification Authority može, ako je potrebno, poništiti valjanost izdanog digitalnog certifikata. Znamo i da se informacija o opozvanim certifikatima ugnježđuje u **Certificate Revocation List** (CRL) autoritativnog CA; ova se potom može skinuti, ručno ili aplikativno, s **Certificate Distribution Points** (CDPs) tog CA. Važno je pravovremeno informirati autentikacijske kontrole informatičkih servisa da je neki certifikat obezvrijeđen prije isteka datuma/vremena upisanog u njemu. Mi IT profesionalci sve to znamo ali "vrag je u detalju", u sitnici koja začas izazove glavobolju.

Moderni Windows serverski i desktop operativni sustavi rade tako da povuku CRL s određene CDP, CRL listu spremu lokalno i potom ju rabe 2 - 3 sata. Ovim postupkom windoze omogućuju aplikaciji koja se oslanja na njihov *CryptoAPI* da vrlo brzo obrađuje autentikacijske zahtjeve, rekli bismo, povećava se *response time* konkretnog autentikacijskog rješenja usidrenog u Windows OS. No, kako to u životu često biva, dobijemo na jednoj strani, a izgubimo na drugoj. Evo zašto: kad windoze spremu CRL na disk i nadalje tom lokalnom instancom opslužuju aplikaciju, niti OS niti aplikacija ne znaju da li je nakon skidanja aktualne CRL možda došlo do opoziva jednog ili cijele gomile certifikata, to će saznati tek nakon idućeg skidanja CRL sa iste CDP. A do tada će kao valjane tretirati te opozvane certifikate. Ovo se sigurno neće svjediti osobama odgovornim za čuvanje nekih sigurnosno senzitivnih podataka od neovlaštenog upada, zar ne?!

Srećom, Microsoft nas je opskrbio s par alata kojima možemo nagovoriti Windows OS da u kraćim vremenskim intervalima, recimo, svakih 30 minuta, osvježava lokalne CRL. *Task Schedulerom* složit ćemo *job* (ups!, pardon, *job* slažu linuxaši sa *Cronom*, mi na windozama slažemo *task* ;-)) kojime ćemo obezvrijediti sve CRL na disku i u RAM-u pa će windoze skidati najnovije CRL čim se ukaže potreba za time (tj. kod prve provjere certifikata kojime se netko predstavlja autentikacijskom modulu nekog Internet ili intranet servisa).

Nakon odabira naredbe Create Task u Task Scheduleru, radimo kako slijedi:

* Kartica General - smjernice za konfiguraciju su na nižoj slici.

General Triggers Actions Conditions Settings History

Name: refresh-CRL

Location: \

Author: CORP\Administrator

Description:

Security options

When running the task, use the following user account:

R2HOST\Admin Change User or Group...

Run only when user is logged on

Run whether user is logged on or not

Do not store password. The task will only have access to local computer resources.

Run with highest privileges

Hidden Configure for: Windows Server 2012 R2

* Kartica Triggers – novi okidač složit ćemu kao na nižoj slici.

Begin the task: On a schedule

Settings

One time
 Daily
 Weekly
 Monthly

Start: 3. 3.2014. 6:00:00 Synchronize across time zones

Recur every: 1 days

Advanced settings

Delay task for up to (random delay): 1 hour

Repeat task every: 30 minutes for a duration of: Indefinitely

Stop all running tasks at end of repetition duration

Stop task if it runs longer than: 3 days

Expire: 10. 3.2015. 15:18:29 Synchronize across time zones

Enabled

- * Kartica Actions je najvažnija - odaberemo Start a program, potom u niže polje upišemo c:\windows\system32\certutil.exe a u polje Add arguments upišemo -setreg chain\ChainCacheResyncFiletime @now;
- * Kartica Conditions - sve opcije trebaju biti isključene, amen.
- * Kartica Settings - kao na nižoj slici.

General Triggers Actions Conditions Settings

Specify additional settings that affect the behavior of the task.

- Allow task to be run on demand
 - Run task as soon as possible after a scheduled start is missed
 - If the task fails, restart every:
 - Attempt to restart up to: times
 - Stop the task if it runs longer than:
 - If the running task does not end when requested, force it to stop
 - If the task is not scheduled to run again, delete it after:
- If the task is already running, then the following rule applies:
-

Djeluje li postavljeni zadatak, možemo vidjeti iz Task Schedulera, kartica History odn. iz komandne linije (kao na nižoj slici) jer zadatak upisuje u registry vrijeme zadnje invalidacije svih lokalnih CRL.

```
C:\>certutil -getreg chain\chaincacheresyncfiletime
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\En
ateCertificateChainEngine\Config\ChainCacheResyncFiletime

ChainCacheResyncFiletime REG_BINARY = 11.3.2014. 10:34
CertUtil: -getreg command completed successfully.

C:\>lokalne kopije CRL su poništene u 10:34 :-)
```

* Ako isti task morate primijeniti na nekoliko servera, samo na prvom serveru exportate taj zadatak u XML i importate ga na drugom.

uto, 2014-03-18 10:25 - Ratko ŽižekKuharice: [Windows](#) [1]

Kategorije: [Servisi](#) [2]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1368>

Links

[1] <https://sysportal.carnet.hr/taxonomy/term/18>

[2] <https://sysportal.carnet.hr/taxonomy/term/28>