Invalidacija lokalnih kopija CRL

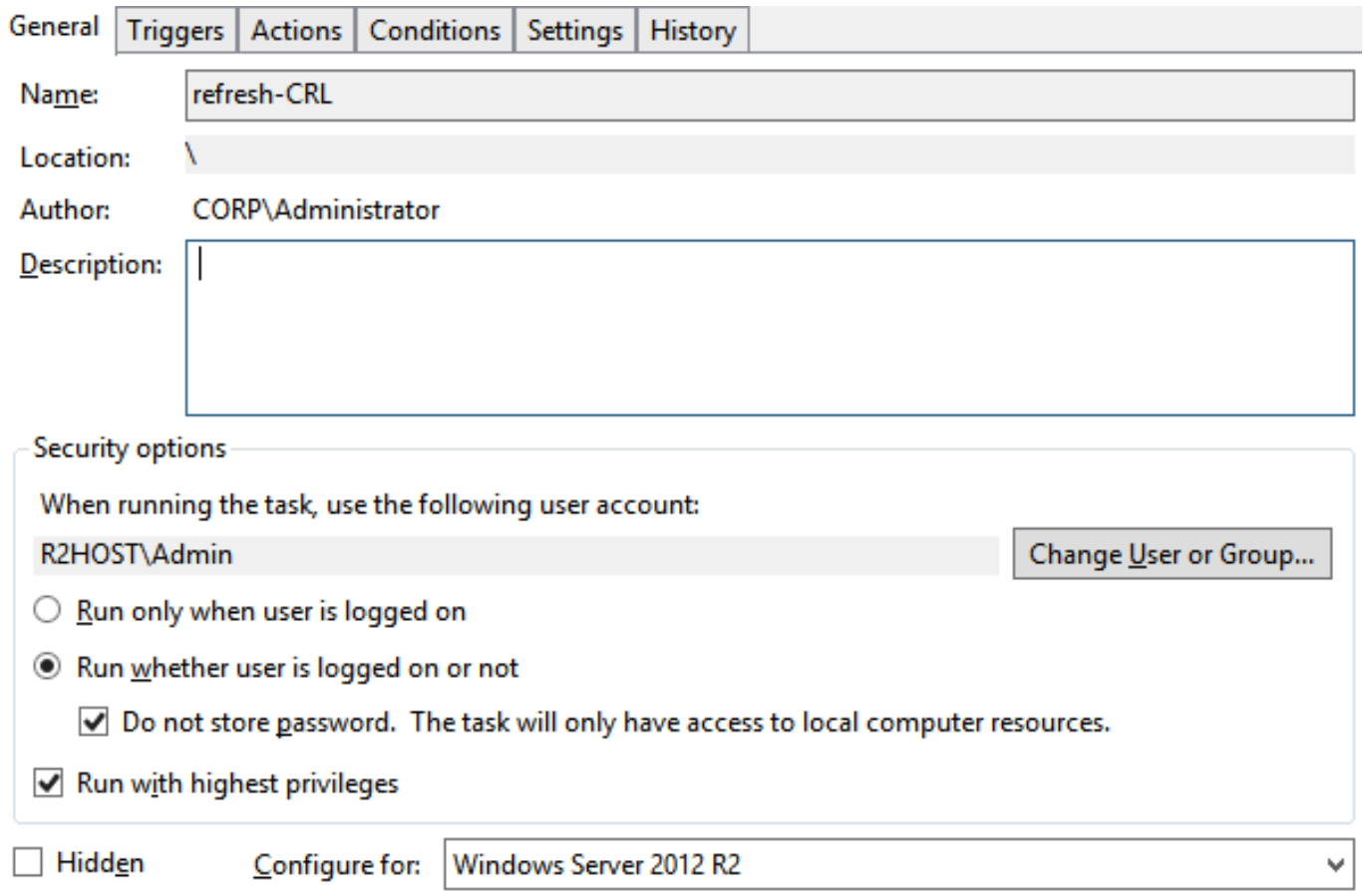

Znamo da Certification Authority može, ako je potrebno, poništiti valjanost izdanog digitalnog certifikata. Znamo i da se informacija o opozvanim certifikatima ugnježđuje u ***Certificate Revocation List*** (CRL) autoritativnog CA; ova se potom može skinuti, ručno ili aplikativno, s ***Certificate Distribution 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 spreme 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 spreme 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 certifkate. Ovo se sigurno neće svidjeti 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).

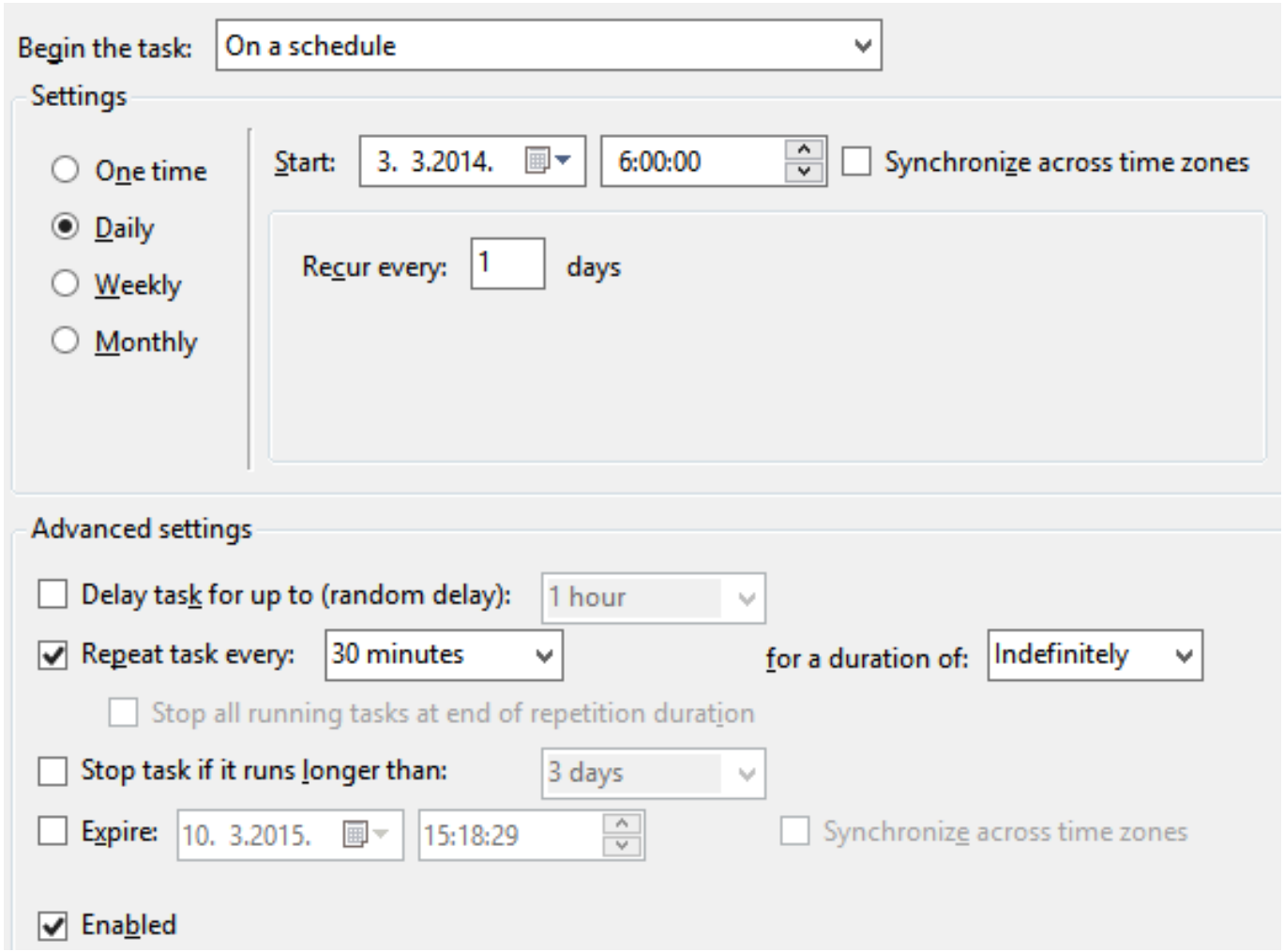
Nakon odabira naredbe Create Task u Task Scheduleru, radimo kako slijedi:
* Kartica General – smjernice za konfiguraciju su na nižoj slici.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



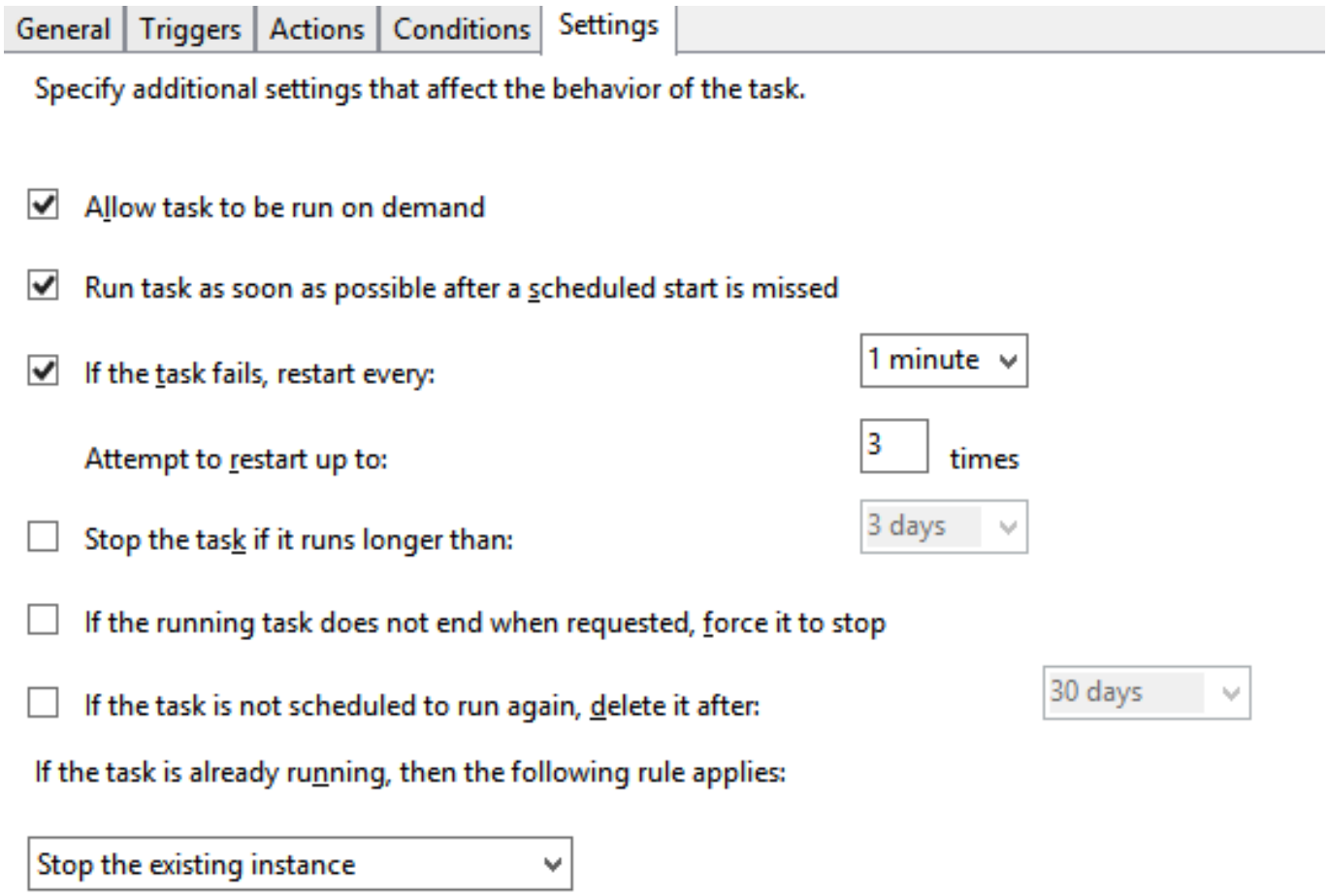
* Kartica Triggers – novi okidač složit ćemu kao na nižoj slici.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

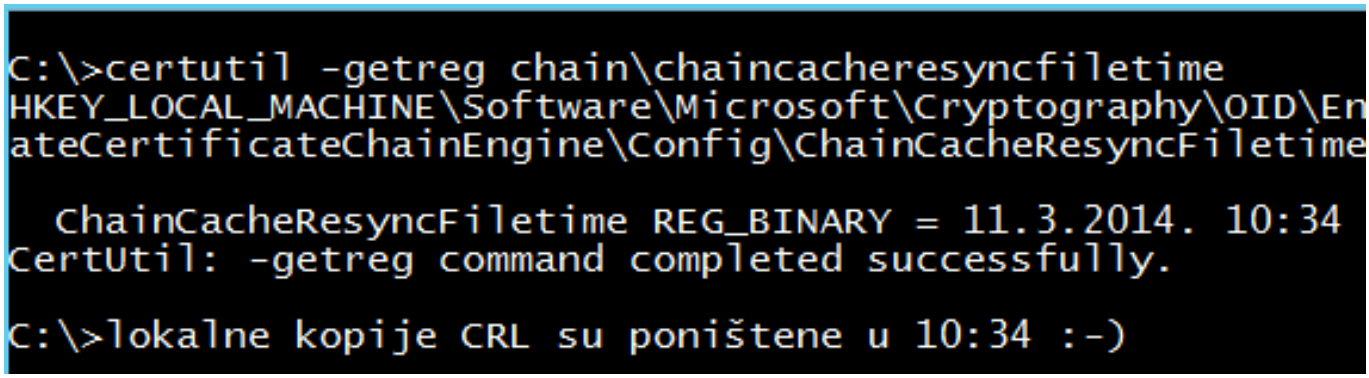


* Kartica Actions je najvažnija – odaberemo Start a program, potom u niže polje upišemo c:\windows\system32\certutil.exe a u polje Add arguments upišemo -setreg chain\ChainCacheResyncFiletime @now;
* Kartica Conditions – sve opcije trebaju biti isključene, amen.
* Kartica Settings – kao na nižoj slici.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



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.



* 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 Žižek**Kuharice:** Windows [1]
Kategorije: Servisi [2]
Vote: 0

No votes yet

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

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

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr