Időszinkronizáció

Szabad szoftver keretrendszer

Készítette a Közigazgatási és Igazságügyi minisztérium E-közigazgatási Szabad Szoftver Kompetencia Központja, Budapest, 2013

Kódszám: EKOP–1.2.15 – Ez a Mű a Creative Commons Nevezd meg! Így add tovább! 3.0 Unported License feltételeinek megfelelően szabadon felhasználható.
A dokumentum legfrissebb változata letölthető a honlapunkról:
http://szabadszoftver.kormany.hu/szabad-szoftver-keretrendszer/

Tartalomjegyzék

Történeti áttekintés

A számítógépes hálózatok korai időszakában a gépek órájának szinkronban tartására egyszerű eszközöket használtak. Mivel sok gép nem tartalmazott beépített órát, a gép bekapcsolásakor az automatikusan lefutó alkalmazások egyike a rendszergazdától megkérdezte a helyi időt, és a továbbiakban az adatot begépelő személy karórájától függött a pontosság. Ez meglehetős pontatlanságot eredményezett. (Ráadásul az idő múlását az operációs rendszer tartotta számon, ami szintén okozhatott időcsúszást.)

MAGYARORSZÁG MEGÚJUL

Viszonylag hamar kitaláltak olyan megoldást (RFC-868[1] [2]), amely TCP/IP protokollt használó gépek számára akár TCP, akár UDP használatával lehetővé tette egy központi géptől a pontos idő lekérdezését. Ez az idő már nem lokális, hanem a Greenwich-i középidő (GMT) szerinti volt, ezt kellett a helyi gépnek az időzóna információ helyes beállításával korrigáltan mutatni a felhasználók számára.[3] Ez másodperc pontosságot biztosított, és a használt adatformátum miatt 2036-ig nyújt lehetőséget a használatra. Ez a megoldás már 1-2-re csökkentette egy hálózat esetén a kézzel beállítandó gépek számát, és növelte a pontosságot. Mivel a TCP/IP hálózat UNIX-rendszerekbe integrálásának kezdete óta a legtöbb rendszeren alapértelmezetten volt és futott ez

[1] http://tools.ietf.org/html/rfc868

[2] Párja volt az RFC-867, (daytime) mely a helyi időt szöveges formában tette távolról lekérdezhetővé. De mivel a formátumra csak ajánlás szerepelt a szövegben, így használata inkább hibakeresésre korlátozódott

[3] Ma a Unix és Unix-szerű (például Linux) rendszerek használata esetén kifejezetten javasolt a gép fizikai óráját a régebben GMT, újabban UTC néven emlegetett - nem-lokális - idő szerint beállítani. Ha egy gép órája helyi idő szerint jár, az az időzónák, illetve a téli-nyári óraátállítás miatt problémákat vet fel.

az időszerver szolgáltatás (tipikusan az inetd nevű eszköz nyújtotta time néven), elterjedt volt a gépek szinkronizálása egy rdate nevű parancs segítségével; használata például rdate time.kfki.hu formában történt.

Ez a megoldás több problémát is felvet[4]. Ezért újabb protokoll-leírás jött létre (RFC-958[5], RFC-1059[6] NTP - azaz Network Time Protocol néven), amit hamarosan több másik követett (RFC-1119, RFC-1305, RFC-1361, RFC-1769, RFC-2030, RFC-4330, RFC-5905) - egyrészt a különféle továbbfejlesztett verziók (jelenleg v4-nél tartunk), illetve az NTP részhalmazát leíró SNTP (Simple Network Time Protocol). Az NTP segítségével lokális hálózaton akár 1 milliszekundumos pontosság is elérhető, interneten keresztüli szinkronizáció esetén ez a 10 msec nagyságrendű pontosságra csökkenhet.

Fentebb emlegetett (S)NTP kliens oldali megvalósítására bizonyos rendszereken használható az előzőek-

[4] A protokoll nem veszi figyelembe az adatcsomag áthaladásának időtartamát - ez főleg távoli szerverek, lassú adatátvitel esetén jelenthet problémát; a 2036. év utáni időre nem nyújt megoldást - ez nyilván ma még nem kritikus, de foglalkozni kellett vele; és végül a másodperces pontosság sok esetben már nem elegendő.

[5] http://tools.ietf.org/html/rfc958

[6] http://tools.ietf.org/html/rfc1059

ben már emlegetett rdate parancs a kifejezetten erre szolgáló „-n” opció segítségével (http://www.openbsd.org/cgi-bin/man.cgi?query=rdate&sektion=8), ellenben Linux rendszereken az rdate ezen funkciója hiányzik.

Döntési mechanizmus

Gyakorlatilag nincs választási lehetőség, minden ma elterjedt rendszer (S)NTP-t használ. Két elterjedt megvalósítása a http://www.ntp.org/ referenciaszoftvere, illetve az OpenBSD csapat által fejlesztett OpenNTP (http://www.openntpd.org/). Ez utóbbinak a fejlesztése az utóbbi 2-3 évben meglehetősen lelassult, ráadásul a legtöbb Linux-terjesztés az ntp.org-félét kínálja fel alapértelmezetten, e mellett maradtunk.

Használat

Ma már a hálózatba kötött számítógépek óráját javasolt (bizonyos helyen kötelező) szinkronban tartani.

Ugyan ma már a legtöbb számítógép rendelkezik beépített óracsippel, de ezek az órák meglehetősen nagy szórást mutatnak a minőség tekintetében. Így az általában használt megoldás az, hogy kis számú gép esetén 1, nagyobb géppark esetén 2 esetleg 3 központi gép órájához igazítjuk a hálózat többi gépét. A szinkronizálást ma már általában a fent említett NTP segítségével oldják meg.

Kliens

Kliens oldalról két elterjedt módszert szoktak használni:

– a napi rendszerességgel ki- és bekapcsolt gépek esetén, közelítőleg megfelelő eredményt érhetünk el egy a gép bekapcsolásakor automatikusan lefutó, a gép óráját a központi órához igazító parancs segítségével. Ez az ntpdate parancs, használata: ntpdate -b time.kfki.hu Míg a „-b” opció[7] használata javasolt,

[7] jelenleg a „-b” opció által kért funkció az alapértelmezett, így akár el is hagyható, de hosszú távon preferált a használata (láttunk már szoftverben alapértelmezést megváltozni, kicsit sűrűbben, mint opciót)

addig a time.kfki.hu helyett inkább válasszunk valami nekünk megfelelőt, ilyen lehet például a hu.pool.ntp.org (Magyarországról - más ország esetén javasolt azon ország országkódját használni a „hu” helyett).

– amennyiben a gép folyamatos üzemben működik (a szerverek tipikusan ilyenek, de kényelmi okokból sokan a munkaállomásokat se kapcsolgatják), a bekapcsoláskor történő órabeállítás kevés lehet. Jellemzően a gépek órája sietni, vagy késni fog egy idő után. Ebben az esetben a javasolt használat az, hogy az órát folyamatosan igazítsuk a központi órához. Ellenben az, hogy meghatározott időnként (például óránként, naponta) **át**állítjuk a gép óráját, felvet egy nagyon súlyos problémát - ilyen esetben elveszítjük az idő egy vagy több fontos jellemzőjét - a folytonosságot, illetve a monotonitást. Azaz vagy „luk” keletkezik - kimaradó időpont; vagy ugyanaz az időpont többször is bekövetkezik. Ezért a bevált módszer a régi vekkerórákban alkalmazott „óralassítás” / „óragyorsítás”. Azaz lekérdezzük a központi gép óráját, és ha a miénk késést mutat, akkor felgyorsítjuk, ha pedig a miénk siet, akkor lelassítjuk azt.

– Ezt szintén megtehetjük az ntpdate parancs segítségével, ekkor ki kell hagyni a fent említett „-b” opciót, helyette a „-B” használandó: ntpdate -B time.kfki.hu és ezt a parancsot kell óránként / napi rendszerességgel lefuttatni (tipikusan **cron**-ból időzítve). Ily módon futtatva az ntpdate-et, a gép szépen lassan „hozzákésik/hozzásiet” a központi időhöz.

– Komplexebb konfigurációt igényel az ntpd (régebben xntpd) nevű szoftver, ami elindítása után folyamatosan fut, és rendszeresen (alapból 64 másodpercenként, ez 16 másodperc és 36,4 óra között változtatható) lekérdezi a pontos időt, majd az előbb tárgyalt módon, a gép belső órájának felgyorsításával/lelassításával hozza összhangba a gép óráját a külvilágéval. Működéséhez viszont szükséges létrehozni egy konfigurációs fájlt (tipikusan /etc/ntp.conf néven létezik), amelyben minimálisan a lekérdezendő szerver(ek) nevét kell megadni, „server time.kfki.hu” formában.

Nem árt tudni, hogy jópár szoftver (például a Dovecot IMAP-szerver, vagy általában az adatbázis-kezelők)

rendkívül zokon veszi az „időugrást” – ezek miatt szintén nem javasolt az a fajta óraállítás.

Megjegyzendő, hogy az óra folyamatos szinkronban tartásának két módja (ntpdate -B vs ntpd) biztonsági szempontból is különbözik. ntpdate használatakor csak a parancs futtatásakor lesz egy rövid ideig tartó hálózati forgalom, míg ntpd használata esetén az ntpd szerverprogram folyamatosan fut és a 123-as UDP porton keresztül elérhető. (Természetesen ez utóbbi használat esetén van lehetőség a kliensek korlátozására.)

Szerver

Szerver, amelyikhez a többi gépet szinkronizáljuk. Ezen gép órájának pontos beállítására több módszert használhatunk. A leggyakoribb, hogy megkérdezzük valamely másik szervert. Ehhez bevezetünk egy hierarchiát. A hierarchia csúcsán álló gép műholdaktól, célhardver segítségével kapja a pontos időt. Ezeket a gépeket Stratum-0 pontosságú szervernek hívjuk; azok a gépek, amelyek ezektől kapják a pontos időt, azok a Stratum-1-es szerverek. Tőlük kapják az időt a Stratum-2-esek, és í. t. (Noha a szabvány elvileg megkülön-

böztet 256 szintet, a gyakorlatban már egy Stratum-15-ös gépet is nem-szinkronizált órájúnak tekintjük.) Az időinformációt a szerverek TCP/IP protokollon broadcast vagy multicast címeket használva szórják a hálózatban, illetve lehet kérdezni is a szervereket. Attól függően, hogy mi kérdezzük a szervert, vagy csak hallgatni akarjuk a tőle érkező szórt információt, változik a konfiguráció a /etc/ntp.conf fájlban. (A következő példákban feltételezzük, hogy a 192.168.1.42.0/24-es hálózatban dolgozunk, ahol az NTP-szerver a 192.168.42.1-es címen érhető el.)

– üzenetszórásos szerver, hallgatózó kliensekkel

Itt a szerver konfigja:

```
szerver$ cat /etc/ntp.conf
server hu.pool.ntp.org
broadcast 192.168.42.255
```

Itt a kliens konfigja:

```
kliens$ cat /etc/ntp.conf
broadcastclient yes
```

– lekérdezős szerver, kérdezősködő klienssel

Itt a szerver konfigja:

```
szerver$ cat /etc/ntp.conf
```

```
server hu.pool.ntp.org
```

Itt a kliens konfigja:

```
kliens$ cat /etc/ntp.conf
server 192.168.42.1
```

Nagyon sok helyen megelégednek azzal, hogy valamely gépet kinevezik óraszervernek, ennek a belső hardveróráját kézzel beállítják, és ehhez szinkronizálják az összes többit. Ebben az esetben például ez a megfelelő beállítás:

```
gép.belső.órájáról.szinkronizáló.szerver$
  cat /etc/ntp.conf
server 127.127.1.0
fudge 127.127.1.0 stratum 10
```

Látható, hogy a szervergépen egy elég furcsa, normálisan nem használatos IP-címet adtunk meg az idő forrásaként. A 127.127.T.U típusú címet a szoftver speciálisan kezeli és azt jelenti, hogy valamilyen hardveren keresztül kapja meg a pontos időt (típusát és a konkrét darabot adják az IP-címbeli számok: T - typeID, U - unitnumber). A „fudge” sor pedig azt jelzi, hogy az alapértelmezett 0-s stratum szint helyett ennél jóval alacsonyabb pontosságúnak minősítjük az idő forrását (és ennek következtében alacsony pontosságúként hirdet-

jük) - ezzel elérve azt, hogy ha egy kliens gép rajtunk kívül valahonnan máshonnan is kapna pontosabb időinformációt, ne a pontatlan időt használja.

Az NTP protokoll nagyon sok lehetőséggel rendelkezik, mint korábban utaltunk rá, például a kliensek és szerverek a kommunikáció során akár azonosíthatják is egymást. Ez biztonsági szempontól nem elhanyagolható lehetőség, hisz e nélkül könnyen lehetne hamis információkkal megzavarni a rendszer működését. A további információk, az egyes beállítások a használt szoftver kézikönyvében megtalálhatók.