

Központi hitelesítés Kerberos 5-tel (1. rész)

A Kerberos segítségével elfeledhetjük a fiókok felügyeletével kapcsolatos gondjainkat.

Elosztott *UNIX/Linux* alapú környezetben a fiókok kezelése rendkívül összetett és zűrös munka tud lenni, ha kézzel próbáljuk elvégezni. A nagyméretű rendszerekben különleges eszközökkel próbálnak úrrá lenni ezen a problémán. Írásomban ismertetem, hogy egy kisebb, akár egy három gépből álló hálózatban hogyan vehetjük hasznát ugyanezeknek az eszközöknek.

Az elosztott környezetek egyik gondja, hogy a jelszó- és árnyékfájlokat az összes gépen egyenként kell megváltoztatni, ha valamelyik fiók adatai módosulnak. A fiókok adatainak módosulása alatt a jelszóváltoztatásokat, a fiókok hozzáadását és törlését, a névváltozásokat (az *UID/GID* módosítások mindig sok bajjal járnak), az adott gépre szóló bejelentkezési jogok hozzáadását és törlését stb. értjük. Szó lesz arról is, hogy a *Kerberos* terjesztés révén hogyan válaszolhatjuk meg az elosztott számítási környezetekben felmerülő, hitelesítéssel kapcsolatos kérdéseket. A 2. részben a jogosultságkezeléssel kapcsolatos témákat tárgyaljuk.

A felhasználók számítógépekkel szembeni hitelesítését a legtöbb esetben jelszavakkal oldjuk meg, bár más módszerek – intelligens kártyák, biometrikus eljárások – is léteznek. A jelszavakat korábban a */etc/passwd* fájl tárolta, az árnyékjelszavak megjelenése óta pedig a */etc/shadow* fájlban található. Mivel mindkét fájl helyileg tárolódik az egyes gépeken, naprakészen tartásuk sok gonddal jár. Erre a gondra kínálnak megoldást a címtárszolgáltatások, mint a *NIS*, a *NIS+* és az *LDAP*. Használatuk kapcsán ugyanakkor egy újabb probléma vetül fel: működésük a hálózatra alapul, és könnyen elérhetővé teszik a csak gyengén titkosított jelszavakat.

A *Kerberos* által megvalósított hitelesítő protokoll egyszerre biztosítja a hálózati szolgáltatások előnyeit, illetve teszi szükségtelemmé a jelszavak számítógépek közötti továbbítását. Mindehhez két demont kell futtatni egy biztonságos kiszolgálón. A *kulcselosztó központ (Key Distribution Center, KDC)* démon a jelszóellenőrzési kérések kezeléséről és a *Kerberos* hitelesítő adatok, igazolványok előállításáról gondoskodik, ezeket *jegyadó jegyeknek (Ticket Granting Ticket, TGT)* nevezzük. A második démon, a *Kerberos felügyelet (Kerberos Administration)* segítségével távolról, a *Kerberos* démonokat futtató számítógépre való bejelentkezés nélkül is lehetővé válik a fiókok hozzáadása, törlése és módosítása. Ez kezeli a felhasználóktól befutó jelszó-

változtatási kéréseket is. A *Kerberos* használatakor jelszó hálózati továbbítására csak jelszóváltoztatáskor kerül sor, ekkor is erős titkosítás védelme alatt.

A *Kerberos KDC* egy ideiglenes igazolványt, egy *TGT*-t ad a fióknak a felhasználó hitelesítésének folyamata során. Ezeknek az igazolványoknak jellemzően 10 vagy 24 óra az élettartamuk. Az élettartam változtatható, de ne legyen 24 óránál hosszabb. Ugyanis, ha ellopják a *TGT*-t, a tolvaj az élettartam fennmaradó részében fel tudja használni. Az igazolványok érvényességének lejárása semmilyen gonddal nem jár, ha a *Kerberos* kizárólag hitelesítésre használjuk, ahogy írásomban ezt feltételezem. Ha viszont *Kerberos* alapú, „kerberizált” szolgáltatásokat használunk, akkor meg kell tanítanunk a felhasználóknak, hogy igazolványuk érvényességének lejártakor újat kell kérniük, függetlenül attól, hogy folyamatosan be voltak jelentkezve a rendszerbe.

A *Kerberos* alapjául szolgáló ötlet az *MIT*-n született. A *Kerberos* legújabb változata az 5-ös, leírása az *RFC 1510* dokumentumban található. Jelenleg két *Kerberos*-megvalósítás érhető el szabadon. (Lásd az internetes forrásokat.) A *MIT Kerberos 5* a *Red Hat Linux* része, a *Heimdal* pedig a *SuSE* és a *Debian Linuxban* található meg. A *Kerberos 5* megvalósításai a *Microsoft Windowsba (Windows 2000* és újabb kiadások), a *Sun Solarisába (SEAM, Solaris 2.6* és újabbak) és az *Apple Mac OS X* operációs rendszerébe is bekerültek. Írásomban az *MIT Kerberos* terjesztésének használatát veszem alapul, ez ugyanis alapesetben is egyszerű jelszóminőség-ellenőrzést, jelszó-előregedést és jelszótörténetet biztosít.

Előfeltételek

A *Kerberos* alapú hitelesítésre két előfeltétel teljesítésével térhetünk át. Az első, hogy a *Kerberos* bevezetése által érintett gépek óráját kivétel nélkül a *KDC*-t futtató gép órájához kell szinkronizálni. Ennek legegyszerűbb módja a *Network Time Protocol (hálózati időprotokoll, NTP)* telepítése az összes gépre.

A második feltételt már nehezebb teljesíteni. Minden fióknévnek, *UID*-nek és *GID*-nek azonosnak kell lennie az összes gépen. Erre azért van szükség, mert minden fiók új és független *Kerberos*-fiókká változik, ezeket *főfióknak (principal)* nevezzük. Meg kell tehát vizsgálnunk az összes helyi */etc/passwd* fájlt, és ellenőriznünk kell, hogy teljesül-

ez a feltétel. Ha nem, akkor egységesíteniünk kell a fiókokat. Ha *Windows* vagy *Mac OS X* alapú gépeket is be akarunk vonni, akkor ezeken a gépeken is át kell néznünk a fiókokat. Ha saját Linux-terjesztésünk *Kerberos*-ának használata mellett döntünk, akkor egyszerűen telepítsük a megfelelő csomagot. Ha viszont magunk akarjuk elvégezni a *Kerberos* lefordítását, akkor kövessük az alábbi útmutatót.

Az MIT Kerberos lefordítása és telepítése

1) Az internetes források között megadott URL-ek valamelyikéről töltsük le a forrást. Töltsük le a forrás csomag *PGP*-aláírását is, és az alábbi paranccsal ellenőrizzük a forrás csomag sértetlenségét:

```
% gpg --verify krb5-1.3.4.targz.asc
```

2) Bontsuk ki a csomagot:

```
% tar zxvf krb5-1.3.4.tar.gz
```

3) Lépünk át a forrás könyvtárba:

```
% cd krb5-1.3.4/src
```

4) Adjuk ki a következő parancsot:

```
% ./configure --help
```

Ezzel megtudhatjuk, hogy rendszerünkben milyen különleges beállításokat kell használnunk. Az alapértelmezett telepítési könyvtár a */usr/local/*. Ha más könyvtárba szeretnénk végrehajtani a telepítést, akkor a következő lépésnél használjuk a *--prefix=/új/könyvtár/elérési/útja* jelzőt.

5) A legtöbb esetben az alapértelmezett könyvtár tökéletesen megfelel:

```
% ./configure
```

6) Fordítsuk le a csomagot:

```
% make
```

Nálam volt valami gond a *krb5-1.3.4/src/kadmin/testing/util* könyvtár egyik fájljával, ezt azonban nyugodtan figyelmen kívül hagyhatjuk. Ha ilyen hibába ütköznénk, a *% make -i* paranccsal indítsuk újra a fordítást.

7) Ellenőrizzük, hogy minden rendben lezajlott-e:

```
% make check
```

8) Ha igen, telepítsük a csomagot:

```
% sudo make install
```

A fordítást soha ne végezzük rootként. A root jogosultságait csak akkor vegyük igénybe, amikor valóban szükséges, például a telepítési lépések során.

Ezzel telepítettük az *MIT Krb5* csomagját a */usr/local/* könyvtárba. Néhány további könyvtárat is létre kell hoznunk, illetve be kell állítanunk a rájuk vonatkozó engedélyeket:

```
% sudo mkdir -p /usr/local/var/krb5kdc
% sudo chown root /usr/local/var/krb5kdc
% sudo chmod 700 /usr/local/var/krb5kdc
```

Ha saját *PAM*-modult szeretnénk fordítani, illetve feltétlenül szükségünk van rá, akkor a *Red Hat* által biztosított modul az alábbi lépésekkel bírhatjuk munkára. Töltsük le a forrást (lásd az internetes forrásokat), majd bontsuk ki:

```
% tar xzf pam_krb5-1.3-rc7.tar.gz
% cd pam_krb5-1.3-rc7
```

A *\$PATH* környezeti változónak az általunk elsődlegesnek kiválasztott *Kerberos*-terjesztés elérési útját kell tartalmaznia, ha valamiért több változat is telepítve lenne a gépen. Például:

```
% PATH=/usr/local/bin:$PATH
```

(Feltéve, hogy a telepítést a */usr/local* könyvtárba végeztük.) Ezután futtassuk az alábbi parancsot:

```
% ./configure
```

Záró lépésként az alábbi parancsokkal fordítsuk le és telepítsük a csomagot:

```
% make
% sudo make install
```

A tartomány létrehozása

A *Kerberos* tartomány (*realm, birodalom*) egy saját *Kerberos* adatbázissal rendelkező felügyeleti tartomány. Minden *Kerberos* tartomány saját *Kerberos* kiszolgálókkal rendelkezik. Tartományunk neve bármi lehet, ám tükröznie kell a DNS alapú világban elfoglalt helyünket. Ha az új *Kerberos* tartományt teljes *pelda.com* DNS-tartományunk számára hozzuk létre, akkor *Kerberos* tartományunknak is azonos nevet adjunk: *PELDA.COM*; csupa nagybetűvel, követve a kerberosos hagyományokat. Ha az új tartomány például a tervezési osztályt fogja lefedni, akkor válasszuk a *TERVEZES.PELDA.COM* nevet.

A tartomány létrehozásának első lépése a */etc/krb5.conf* fájl létrehozása, ez tartalmaz minden a tartománnyal kapcsolatos adatot. A *krb5.conf* fájlban minden olyan számítógépen jelen kell lennie, amelyről el szeretnénk érni a *Kerberos* tartományt. A fájl tartalma a *PELDA.COM* tartomány esetében a következő lesz, feltételezve, hogy a KDC és a felügyeleti kiszolgáló egyaránt a *kdc.pelda.com* címen fut:

```
[libdefaults]
# alapértelmezett tartománynév
default_realm = PELDA.COM

[realms]
PELDA.COM = {
# kiszolgálók elérhetőségének megadása
# valamint annak, hogy mely kapukon
# fogadják a kéréseket
# a szabványos kapuk a 88 és a 749
kdc = kdc.pelda.com:88
```

```

        admin_server = kdc.pelda.com:749
    }
[domain_realm]
    # a DNS tartománynév megfeleltetése a Kerberos
    # tartománynévnek
    .pelda.com = PELDA.COM
[logging]
    # megadja, hogy az egyes szolgáltatásoknak
    # hova kell
    # írniuk naplózási adataikat
    kdc = SYSLOG:INFO:DAEMON
    admin_server = SYSLOG:INFO:DAEMON
    default = SYSLOG:INFO:DAEMON

```

A következő fájl, a `/usr/local/var/krb5kdc/kdc.conf` a **KDC**-kiszolgáló beállításait tartalmazza. Ennek csak a **KDC**-démont futtató gépen kell jelen lennie. Mindegyik beállításnak ésszerű alapértéke van, ezért a legtöbb esetben egy üres fájl létrehozása is elegendő.

```
% sudo touch /usr/local/var/krb5kdc/kdc.conf
```

Az alábbi parancsokat a **KDC** szerepét játszó számítógépen kell kiadni. A

```
% sudo /usr/local/sbin/kdb5_util create -s
```

paranccsal létrehozuk az új tartomány kezdeti **Kerberos** adatbázisát. A parancs bekéri az új tartomány adatbázisának fő jelszavát, majd a `/usr/local/var/krb5kdc/.k5.PELDA.COM` fájlba írja. A parancs hatására a **Kerberos 5** fiókadatbázisban létrejön a főfiókok kezdő halmaza is. Ezeket a következő parancsokkal tudjuk kilistázni:

```
% sudo /usr/local/sbin/kadmin.local
```

A `kadmin.local`: parancssorba a `listprincs` parancsot kell beírunk. A megjelenő lista a következő:

```

K/M@PELDA.COM
kadmin/admin@PELDA.COM
kadmin/changepw@PELDA.COM
kadmin/history@PELDA.COM
krbtgt/PELDA.COM@PELDA.COM

```

Pillanatnyilag még nem tudjuk használni a **kadmin** eszköz távoli változatát.

Mielőtt elkezdenénk létrehozni új tartományunk főfiókjait, meg kell adnunk a jelszavak kezelésére vonatkozó házirendet:

```

kadmin.local: add_policy -maxlife 180days -minlife
??days -minlength 8 -minclasses 3
?-history 10 default

```

A fentiekkel megadtuk az ezt követően létrejövő főfiókok mindegyikére érvényes alapértelmezett házirendet. A jelszavak maximális élettartama 180, minimális élettartama pedig 2 nap lett. Minden jelszónak legalább nyolc karakter

hosszúnak kell lennie, és ezeknek a karaktereknek a következő öt osztály közül legalább háromból kell kikerülniük: kisbetűk, nagybetűk, számok, írásjelek, egyéb karakterek. A rendszer az utolsó tíz jelszót jegyzi fel, megelőzve az ismételt felhasználást. Ha a jelszavakat valamilyen szótár alapján is ellenőrizni szeretnénk, akkor egy `dict_file` értéket kell megadnunk:

```

[realms]
    PELDA.COM = {
        dict_file = /usr/share/dict/words
    }

```

A beállítás a `kdc.conf` fájlba kerül.

Készen állunk arra, hogy létrehozuk saját felügyeleti főfiókjunkat:

```
kadmin.local: addprinc janos/admin
```

A név természetesen saját nevünkkel egyezzen meg, a **/admin** részt viszont hagyjuk változatlanul. Ezután kétszer be kell írunk a főfiók jelszavát. Az új fiókot a következő paranccsal vizsgálhatjuk meg:

```
kadmin.local: getprinc janos/admin
```

A kimenet az alábbihoz fog hasonlítani:

```

Principal: janos/admin@PELDA.COM
Expiration date: [never]
Last password change: wed Dec 24 09:55:17 PST 2003
Password expiration date: Mon Jun 21 10:55:17 PDT
↳ 2004
Maximum ticket life: 1 day 00:00:00
Maximum renewable life: 0 days 00:00:00
Last modified: wed Dec 24 09:55:17 PST 2003
↳ (root/admin@PELDA.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, Triple DES cbc mode with HMAC/sha1,
↳ no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Attributes:
Policy: default

```

A `quit` paranccsal lépünk ki a `kadmin.local` programból, majd az alábbi utasítással indítsuk el a **KDC** démont:

```
% sudo /usr/local/sbin/krb5kdc
```

Az alábbi paranccsal kérjük egy **Kerberos 5 TGT**-t:

```
% /usr/local/bin/kinit janos/admin@PELDA.COM
```

Majd vizsgáljuk meg a kapott TGT-t:

```

% /usr/local/bin/klint
Ticket cache: FILE:/tmp/krb5cc_5828

```

```
Default principal: janos/admin@PELDA.COM
Valid starting Expires Service principal
12/23/03 14:15:39 12/24/03 14:15:39
↳ krbtgt/PELDA.COM@PELDA.COM
```

Gratulálok! Sikeresen túlestünk első *Kerberos* alapú hitelesítésünkön!

Most meg kell adnunk, hogy a felügyeleti fiók milyen jogosultságokat kapjon. Ezt a */usr/local/var/krb5kdc/kadm5.acl* fájlban található bejegyzések szabják meg. A *janos/admin* fióknak az alábbi sorral adhatunk felügyeleti jogot az összes főfiókra. A főfiókokat a * helyettesítő maszkkal jelezzük:

```
janos/admin@PELDA.COM *
```

Mielőtt elkezdhetnénk hálózaton keresztül használni a felügyeleti démont (kadmind), készítenünk kell egy *keytab* fájlt, amely a tartomány létrehozásakor megadott *kadmin* főfiókok egyikének kulcsát tartalmazza:

```
kadmin.local: ktadd -k /usr/local/var/krb5kdc/
?kadm5.keytab kadmin/changepw
```

Ezzel minden készen áll a *Kerberos* felügyeleti démon indításához. Indítása a következő paranccsal történik:

```
% sudo /usr/local/sbin/kadmind
```

A démon közreműködésével, a *kadmin* ügyfélprogrammal távolról is tudjuk kezelni *Kerberos* főfiókjainkat, nem kell bejelentkeznünk a *KDC*-re. Ha *Kerberos* démonjainkat a rendszerindításkor önműködően szeretnénk indítani, akkor adjuk hozzá őket a *KDC/etc/rc* fájljaihoz. A korábban kapott *Kerberos TGT*-vel indítsuk el a távfelügyeleti programot:

```
% /usr/local/sbin/kadmin
Authenticating as principal janos/admin@PELDA.COM
with password.
Password for janos/admin@PELDA.COM:
```

Új fiókok hozzáadása

Az új fiókokat továbbra is hozzá kell adni a *shadow* fájlhoz vagy a jelszótérképhez. A titkosított jelszavak viszont nem ide kerülnek, ehelyett mindig egy új *Kerberos* főfiókot kell létrehozunk, a jelszót pedig a *KDC*-be kell mentenünk. A *kadmin* segédeszközzel:

```
% /usr/local/sbin/kadmin
```

egy normál felhasználó főfiókját a következő módon hozhatjuk létre:

```
kadmin: addprinc janos
NOTICE: no policy specified for janos@PELDA.COM;
assigning "default"
Enter password for principal "janos@PELDA.COM":
Re-enter password for principal "janos@PELDA.COM":
Principal "janos@PELDA.COM" created.
```

A főfiók létrehozása során megadott jelszó lesz az, amelyet Jánosnak be kell írnia ahhoz, hogy egy *Kerberos TGT*-hez jusson, vagy bejelentkezzen egy a *Kerberos 5* tartományba tartozó gépre.

Most az egyes fiókokhoz tartozó főfiókokat kézzel is létrehozhatjuk, de alkalmazhatjuk a lenti, áttérésről szóló részben ismertetett eljárást is.

Szolga KDC-k hozzáadása

Ha a *Kerberos*t éles környezetben szeretnénk használni, akkor a rendszer hibatűrését további, szolgálként üzemelő *KDC*-k hozzáadásával fokozhatjuk. Ehhez a mester *KDC*-nek egy további, terjesztő szolgáltatásra van szüksége, amely mindig továbbítja a szolga kiszolgálók felé a *KDC* adatbázis frissített változatát. A szolga kiszolgálókra a terjesztő szolgáltatás fogadó oldalát kell telepíteni. A telepítéseket, beállításokat az MIT-s leírás tárgyalja bővebben.

Az ügyfelek beállítása

Egy számítógépet a legegyszerűbben egy *csatlakoztatható hitelesítő modullal (pluggable authentication module, PAM)* tehetünk képessé a *Kerberos* alapú hitelesítésre. Mivel ez *Kerberos API* hívásokat használ, működő */etc/krb5.conf* fájlra van szüksége. Az első lépés tehát a */etc/krb5.conf* fájl átmásolása a *KDC*-ről az egyes ügyfélgépekre. A *Kerberos*t nemcsak felhasználók, de számítógépek hitelesítésére is használjuk, ezzel például megakadályozhatjuk, hogy hamis IP-című gépre jelentkezünk be. Mindez csak akkor működik, ha mindegyik számítógép saját *Kerberos* főfiókkal rendelkezik, amelynek kulcsa, vagyis jelszava egy fájlba, pontosabban egy *keytab* fájlba kerül. A számítógépek főfiókjai különleges formátumúak:

```
host/<állomasnev>.pelda.com@PELDA.COM.
```

Első lépésként az összes ügyfélgéphez létre kell hoznunk egy-egy új főfiókot. Az alábbi parancsokban az *ugyfe11*-et használjuk számítógépnévként. Helyette értelemszerűen mindig az adott ügyfélgép állomásnevét kell alkalmazni. Lépünk be az egyes ügyfélgépekre, majd adjuk ki az alábbi parancsokat:

```
% sudo /usr/local/sbin/kadmin
kadmin: addprinc -randkey host/
?ugyfe11.pelda.com@PELDA.COM
```

Ezzel az új főfiók véletlenszerű jelszót kap. Ezután írjuk ki a kulcsot egy *keytab* fájlba:

```
kadmin: ktadd host/ugyfe11.pelda.com@PELDA.COM
```

A parancs hatására létrejön a */etc/krb5.keytab* fájl. A */etc/* könyvtárhoz csak akkor kapunk írási engedélyt, ha a *kadmin* parancsot *sudo*-val futtatjuk. Ha csupán egy új főfiókot akarunk létrehozni, akkor nincs szükségünk kiemelt jogosultságokra. Ellenőrizzük a */etc/krb5.keytab* fájl tulajdonjogát és a rá vonatkozó engedélyeket. Írására csak a root kapjon jogot, ellenkező esetben sérül a gép biztonsága. Többféle *Kerberos 5 PAM*-modul is létezik, nevük egységesen *pam_krb5*. Nagy részük az MIT *Kerberos 5 1.3*-as válto-

zatának kiadásakor az *API*-t érintően végrehajtott módosítások miatt ma már nem működik. A legjobban úgy járunk, ha a saját *Linux* terjesztésünkhöz tartozó *PAM*-modult használjuk. A *Kerberos 5 PAM*-modulok forrásból végzett fordításáról már ejtettünk szót. Most adjuk hozzá az új *PAM*-modult a rendszer hitelesítési készletéhez. Ezt – legalábbis *Red Hat* rendszereken – a `/etc/pam.d/system-auth` fájl átírásával tehetjük meg. A fájlban szereplő bejegyzéseknek az alábbiakhoz kell hasonlítaniuk:

```
auth required /lib/security/$ISA/
↳ pam_env.so
auth sufficient /lib/security/$ISA/pam_unix.so
↳ likeauth nullok
auth sufficient /lib/security/$ISA/pam_krb5.so
↳ use_first_pass
auth required /lib/security/$ISA/
↳ pam_deny.so
account required /lib/security/$ISA/
↳ pam_unix.so
account [default=bad success=ok
↳ user_unknown=ignore
?service_err=ignore system_err=ignore]
?/lib/security/$ISA/pam_krb5.so
password required /lib/security/$ISA/
↳ pam_cracklib.so
?retry=3 type=
password sufficient /lib/security/$ISA/
↳ pam_unix.so
?nullok use_authtok md5 shadow
password sufficient /lib/security/$ISA/
↳ pam_krb5.so
?use_authtok
password required /lib/security/$ISA/
↳ pam_deny.so
session required /lib/security/$ISA/
↳ pam_limits.so
session required /lib/security/$ISA/
↳ pam_unix.so
session optional /lib/security/$ISA/
↳ pam_krb5.so
```

A módosítások elvégzése után minden olyan program, amelynek *PAM* beállító fájljában a `system-auth PAM`-készlet szerepel – lásd a `/etc/pam.d/` könyvtár egyéb fájljait – *Kerberos*t fog használni a hitelesítési feladatokra.

Együttműködés nem Linux alapú ügyfelekkel

Ha már rendelkezünk működő *Windows Active Directory (AD) KDC* telepítéssel, akkor ezt is használhatjuk mester *KDC*-ként a *Linux/UNIX* alapú gépek számára. Ebben az esetben a teljes kiszolgálótelepítést elhagyhatjuk, elég az ügyfelek telepítésére szorítkoznunk, illetve a `/etc/krb5.conf` fájlban a *Windows* alapú *KDC*-t kell megadni a *UNIX* alapú *KDC* helyett. A *keytab* fájlok létrehozásáról és másolásáról bővebben az internetes források tájékoztatnak.

Ha a csoportban *Windows* gépek is vannak, természetesen ezekkel is csatlakozhatunk a *UNIX* alapú *KDC*-hez, ám csak akkor, ha a gépek még nem tartoznak *Kerberos* használó *Windows* *AD* tartományba, valamint a *Kerberos* és

a *Windows* alatti fióknevek megegyeznek. Erről bővebben az internetes anyagokban lehet olvasni.

A *Mac OS X* alapú ügyfelek használata a *Kerberos 5* tartományban egyszerű, ahogy a *UNIX* alapú *KDC*-k nevének megadása is a *Mac* gépeken. A fiókneveknek ebben az esetben is egyezniük kell.

Áttérés helyi jelszavakról vagy NIS/LDAP alapú rendszerről Kerberosra

Van egy működő *Kerberos 5* tartományunk és beállítottuk az ügyfeleket – a következő lépés a felhasználói fiókok áttelepítése. Eddig a fiókokhoz tartozó jelszavakat az egyes gépek a helyi `/etc/shadow` fájlban vagy egy *NIS/LDAP* jelszó-térképben tárolták. Ezek a jelszavak egyirányú kivonatoló algoritmussal vannak titkosítva, mely lehetetlenné, de legalábbis a gyakorlatban a szuperszámítógéppel nem rendelkezők számára nehezen kivitelezhetővé teszi a jelszavak feltörését, illetve a teljes átalakítást *Kerberos 5* formátumra. A *Kerberos* alá történő áttelepítés elvégzésére kiváló megoldás a `pam_krb5_migrate` használata. (Lásd a forrásokat.) Ez egy veremlhető *PAM*-modul, fel kell telepíteni néhány gépre, és minden alkalommal, amikor valaki bejelentkezik, a fiók aktuális jelszavával létrehoz egy új főfiókot a *Kerberos 5 KDC*-ben.

Miután mindenki bejelentkezett ezekre a gépekre, az összes felhasználónak lesz egy *Kerberos 5* főfiókja. Ekkor a helyi fájlokban vagy a *NIS/LDAP* jelszó-térképben található jelszavakat lecserélhetjük egy helyőrzőre, mint például `krb5`. Ettől a pillanattól kezdve a *Kerberos PAM*-modul végzi a felhasználók hitelesítését. Az áttérést segítő gépekről eltávolíthatjuk a `pam_krb5_migrate` modult.

Kerberizált alkalmazások

Sikeresen életre hívtuk a *Kerberos*t, tehát elkezdhetünk rá támaszkodó szolgáltatásokat használni. Telepíthetnénk például *Kerberos* alapú *telnet*-et és *FTP*-t, de ezek helyett használjunk inkább *SSH*-t. Kerberizálhatjuk *Apache* webkiszolgálónkat és Mozilla böngészőnket is. A *Kerberos* alkalmazása előtt ezen szolgáltatások igénybe vételekor mindig jelszót kellett megadnunk, most azonban lehetővé vált, hogy mindezek az alkalmazások az elmentett *Kerberos* igazolványokat használják fel a megfelelő szolgáltatásoknál végzett hitelesítésre. Ezt a megoldást szokták egyszeri bejelentkezésnek nevezni (*single-sign-on*).

Linux Journal 2005. február, 130. szám

A cikkhez tartozó források elérhetősége:

➔ www.linuxjournal.com/article/7706



Dr. Alf Wachsmann 1999 óta a Stanford Linear Accelerator Center (SLAC) munkatársa. Ő felelős az önműködő *Linux* telepítések minden mozzanatáért, egyaránt ide értve a farmok csomópontjainak, a kiszolgálóknak és az asztali gépeknek a kezelését. Munkája során elsősorban az aktív fájlkészletek (AFS) támogatásával, a *Kerberos 5*-re való áttéréssel, egy felhasználónyilvántartó tervezettel és felhasználói tanácsadással foglalkozik.