Dr. Mileff Péter

UNIX/LINUX OPERÁCIÓS RENDSZER ÜZEMELTETÉSE

4. ELŐADÁS

Miskolci Egyetem
Általános Informatikai Tanszék

Chroot

- **Cél:** átmenetileg meg kellene változtatnunk a root jegyzékét egy program lefuttatásának idejére.
- Ennek egyik tipikus esete:
  - Boot loader elromlik. Ekkor felcsatolunk egy root partíciót valamely pontra a jegyzékstruktúrában.
  - Majd ezen a köteten szeretnénk lefuttatni egy programot úgy, hogy az root jegyzéknek a kötet eredeti root jegyzékét lássa.
- Ilyenkor a megoldás a ***chroot*** parancs használata
  - indít egy olyan shell-t, ami a megadott jegyzéket látja root jegyzéknek.

Chroot

chroot <új gyökér könyvtár>

- A másik ok, amiért a gyökér jegyzéket átállíthatjuk:
  - egy program működési területének lekorlátozása.
  - Ha a szolgáltatást fel is törnék
    - úgy gyökérnek megadott aljegyzéknél nem juthatnak feljebb a jegyzékstruktúrában
  - nem szerezhetnek hozzáférést a rendszer kényesebb részeihez.

Példa

1. mkdir /mnt/hda7
2. mount /dev/hda7 /mnt/hda7
3. chroot /mnt/hda7

exit

A fájlok megosztása és átvitele...

5

Fájlok megosztása

- A számítógépek már nagy háttértárolókkal rendelkeznek
  - De még mindig szükség van fájl szerverekre.
- Oka:
  - Fontos információk központi tárolása, mások számára elérhetővé tétele.
  - Az egyes számítógépek különböző veszélyeknek vannak kitéve, vírusok, meghibásodások, emberi hibák.
    - Ezért biztonsági másolatokat helyezhetünk el a központi szerveren.

6

Fájlok megosztása

- A munkaállomások könnyebb adminisztrációja,
- az installációs állományok tárolása,
- a programok központi szerverről való futtatása révén.

- Ismertebb fájlmegosztási módszerek:
  - **FTP,**
  - **SFTP,**
  - **FTPS,**
  - **NFS,**
  - **SAMBA,**
  - **SCP.**

7

FTP...

8

Az FTP (File Transfer Protocol)

- Az állományok megosztásának egyik legrégibb, és manapság is elterjedten használt módja.
- A protokollt 1985-ben rögzítették az **RFC 959** szabványban.
- Megkülönböztetünk:
  - ftp szolgáltatást nyújtó programot (ftp szerver),
  - és az ftp szolgáltatást igénybe vevő programot (ftp kliens).
- A fájl átvitelt a kliens oldalon kell kezdeményezni.
  - **Upload:** A klienstől a szerver felé történő átvitel, a feltöltés.
  - **Download:** a szervertől a kliens felé történő fájlátvitel, a letöltésnek nevezzük.

9

Az FTP működése

- A Linux rendszereken az FTP szerverek több változata is elterjedt.
  - Működésük *daemon* jellegű.
- Az egyik legismertebb a vsftpd *(Very Secure FTP Daemon)* program.
  - (http://vsftpd.beasts.org/)
  - Konfigurációs állománya az /etc/vsftpd/vsftpd.conf

10

Az FTP működése

- Működésük alapján két változatot különböztetünk meg:
- A legáltalánosabban használt:
  - amikor a rendszer felhasználói a nevükkel és jelszavukkal bejelentkezve, a felhasználói jogaikkal látják az állományrendszert.
    - Ilyenkor kezelhetik a saját állományaikat.
- A másik működési mód: amikor publikálunk állományokat.
  - Ekkor a kliens programok azonosítás nélkül, "anonymous"-ként jelentkeznek be.
  - Az *ftp* felhasználó jogaival tevékenykednek, és mozgási területük az *ftp* felhasználó *home* jegyzékére korlátozódik.

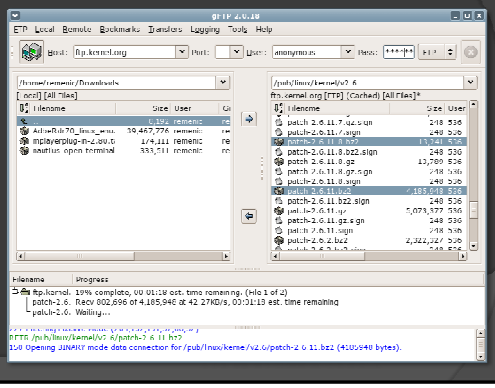
11

Az FTP működése

- Az ***ftpd*** az ftp szolgáltatásért felelős daemon.
- Ő kezeli az ftp kliensektől érkező csatlakozási kéréseket
  - bonyolítja a fájl átvitelt a kliens kérése és a saját beállításai szerint.
- Az ftpd a 21-es portot figyeli.
  - Minden ide érkező kérést az ftp szerverhez irányít.

12

gFTP



NFS...

Az NFS

- Fájlmegosztási protokoll. *(Network File System)*
  - *Unix rendszerek* elterjedt megoldása az állományok megosztására.
- A Linux/Unix rendszerek:
  - üzemelhetnek NFS szerverként is, de klienskent fel is csatolhatjuk más szerverek megosztott jegyzékeit.
- Az NFS szerver implementációja két részre oszlik:
  - Egy kernel modulra,
  - és egy felhasználói módú programra.
  - A felhasználói módban futó folyamat fogadja a kapcsolódási kérelmeket, és indítja a kernel szálakat.

Az NFS szerver

- Elindulása és működése részben különbözik a *daemon*, illetve *inetd* alapú működéstől.
- Oka: **RPC** (Remote Procedure Call) alapú kommunikációra épül.
  - Ezért igényli a működéséhez az RPC kommunikációs rendszert is,
    - amelyhez kapcsolódik a folyamatosan futó daemon jellegű szerver.
  - Az RPC kommunikációs rendszert a ***portmap*** szolgáltatással indíthatjuk el.
  - Ezek után már futtathatjuk az nfs és az nfslock szolgáltatásokat.
- Csomagok: nfs-utils, portmap (vagy rpcbind)
  - Ubuntu:
    - sudo apt-get install nfs-kernel-server nfs-common portmap

Mi is az az inetd?

- Az *inetd* démont gyakran csak „internet szuperszervernek” nevezik.
  - mert a helyi szolgáltatások kapcsolatainak kezeléséért felelős.
- **Működése**: amikor az inetd fogad egy csatlakozási kérelmet:
  - akkor eldönti róla, hogy ez melyik programhoz tartozik,
    - elindít egy példányt belőle,
  - majd átadja neki a socketet
    - (az így meghívott program a szabvány bemenetéhez, kimenetéhez és hibajelzési csatornájához kapja meg a socket leíróit).

17

Mi is az az inetd?

- Az inetd használatával csökkenteni tudjuk a rendszerünk terhelését:
  - a csak alkalmanként meghívott szolgáltatásokat nem futtatjuk teljesen független önálló módban.
- Az inetd démont elsősorban más démonok elindítására használjuk.
- A konfigurációs állománya az /etc/inetd.conf.

18

Az NFS szerver

- A jegyzék megosztások beállítása:
  - **/etc/exports** állomány
- Felépítése:
  - Minden sor elején a megosztott jegyzék szerepel,
  - ezt követi a megosztást elérhető kliensek listája
    - (üres helyekkel elválasztva). Gépnév vagy IP címmel.
    - De megadhatjuk gépek egy csoportját úgy, hogy a név megadásánál használjuk a "*" és "?" karaktereket, vagy IP címtartományt adunk meg
  - Minden kliensnek külön megadhatjuk a hozzáférési jogait zárójelben

19

Az NFS szerver

- Néhány fontosabb paraméter:

Paraméter	Leírás
ro	Csak olvasható a megosztás. (Alapértelmezett)
rw	Olvasható-írható a megosztás.
secure	A kliens kérelmének 1024 alatti portról kell érkeznie, vagyis csak *root* lehet a felhasználó. (Alapértelmezett)
asvnc	Aszinkron módon kezeli a szerver a meghajtót, vagyis hamarabb válaszol, mint hogy letárolta a módosításokat.
all_squash	Minden felhasználót anonymous-ra képez le.

20

/etc/exports

- /files *(ro,sync) # Csak olvasás mindenkinek
- /files 192.168.0.100(rw,sync) # Írás olvasás a 192.168.0.100 kliensnek
- /files 192.168.1.1/24(rw,sync) # Írás, olvasás minden 192.168.1.1 – 192.168.1.255 kliensnek

21

NFS példa

- /pub *.uni-miskolc.hu(rw,all_squash)
  - Itt a /pub jegyzéket tettük elérhetővé a uni-miskolc.hu *domain* minden gépe számára
    - olvasás-írás joggal, és a felhasználók *anonymous*-ra képezésével.
- Egy szerver NFS megosztásainak listázása:

  # showmount –e <gépnév>
- A fejlett disztribúciókban grafikus felületet is biztosítanak az NFS megosztások menedzselésére.

22

NFS megosztás használata

- mount szerver_ip_címe:/megosztani/szánt/jegyzék /ahova/csatolni/szeretnénk/mappa
- Pl.:

  # mount 193.6.5.41:/megosztas /mnt/filmek

23

SAMBA...

24

A SAMBA

- Egy olyan eszközgyűjtemény, amelyek segítségével a hálózaton erőforrások oszthatók meg.
  - Pl.: a nyomtató, fájlok.
- A Samba a Microsoft és az IBM által is elfogadott **Server Message Block** (SMB) protokollt használja
  - **Cél:** TCP/IP hálózaton keresztül alacsony szinten adatokat cserélni a Windows ügyfelek és Unix kiszolgálók között.
- A Samba szabad szoftver így szinte minden platformon megtalálható
  - léteznek kereskedelmi forgalomban kapható változatai is.
- Teljes megoldást kínál a helyi hálózatok számára

25

Mit kínál a Samba?

- Unix fájlokat megosztása Win, OS/2 és más operációs rendszereknek
- Elérhetővé tehetjük a hálózati nyomtatókat a Windows ügyfelek számára
- Névkiszolgálást kínálhatunk (broadcast és WINS).
- Engedélyezhetjük, hogy Windows ügyfelek böngésszék a hálózati erőforrásokat
- Windows munkacsoportokat vagy tartományokat hozhatunk létre.
- Előírhatjuk az ügyfelek felhasználónevének és jelszavának a hitelesítését

26

Az SMB protokoll

- Egy kapcsolat orientált protokoll.
- Működése:
  - Minden kapcsolatra létrehoz egy kapcsolat ID-t „service user ID” (UID)
  - ezen belül pedig minden megosztáshoz létrehoz egy TID és ezen belül minden fájlnak egy FID-t.
  - TID az erőforrás ID-je, amihez kapcsolódni akar a kliens (pl. egy megosztás)
  - a FID pedig azon az erőforráson egy file-hoz kapcsolt ID.

27

A SAMBA működése

- A Samba működése két Unix démon körül forog.
  - megosztott erőforrásokat kínálnak a hálózatba kapcsolódó SMB ügyfeleknek.
- **smbd:**
  - lehetővé teszi fájlok és nyomtatók megosztását SMB hálózatban,
  - és az SMB ügyfelek azonosságának és jogosultságának vizsgálatát.
  - Minden beérkező kérésre új smbd processz indul,
    - amely újraolvassa a konfigurációs fájlokat és kiszolgálja a kérelmet.

28

A SAMBA működése

- **nmbd:**
  - Ez a démon a WINS (Windows Internet Name Service, Windows internet névkiszolgáló) kezeléséről gondoskodik,
  - segítséget nyújt a tallózásban.

29

Samba konfiguráció

- Konfigurációs állományok az **/etc/samba** jegyzékben.
  - Az smb.conf fájl tartalmazza a szerver beállításait.
    - Megosztásokat is ebben az állományban hozhatunk létre.
  - Az lmhosts a hosts fájlhoz hasonlít, a Név - IP cím leképezéseket tartalmazza.
  - Az smbusers az NT felhasználók Linux felhasználó listába való leképezését tartalmazza.
  - Az smbpasswd állomány a Samba felhasználói jelszókat tartalmazza kódolt formában.

Log fájlok: /var/log/samba

30

Egy alap szerver konfiguráció

- Első lépés: beállítjuk a szerver workgroup paraméterét, a leíró szövegét, és esetleg a NetBIOS nevét is.
  - Hálózatban résztvevő minden gépnek van egy netbios neve.
  - Egy NetBIOS név 16 karakterből áll, de ebből csak 15 használható a név megadására,
  - a tizenhatodik byte az erőforrás (pl. megosztás) típusát adja meg)
- /etc/samba/smb.conf-ban

31

Egy alap szerver konfiguráció

- Tehát:

  netbios name = név

  workgroup = CSOPORT

  server string = Ez egy samba szerver
- Következő lépés: lekorlátozzuk a hozzáférést a szerverhez egyes IP cím tartományokra a cím részleges megadásával:

  host allow = 192.168.

32

Authentikációs beállítások

- Az SMB esetében kétféle authentikációs metódust különböztetünk meg:
  - A régi Windows 9x metódust (share)
    - a megosztásokra ad meg jelszavakat
  - A felhasználók azonosításán alapuló metódus
    - Itt 4 különböző megoldás közül is választhatunk az információk ellenőrzésénél:
  - **user:** a Samba szerver fogadja a usernév/jelszó párost és az adatbázisa alapján leellenőrzi.

33

Authentikációs beállítások

- **domain:** ebben az esetben a szerver egy NT domain tagja,
  - rendelkezik egy gép accounttal a domain controllerben.
  - Minden authentikációs információt a domain controller felé továbbít.
- **ADS:** a Samba szerver egy Active Directory domainhez való csatlakozási lehetősége.
- **server:** elavult opció. Régebben még a Samba nem volt képes a domain authentikációra.
  - Lényege: a szerver átveszi a usemevet/jelszót a klienstől majd ezzel megpróbál a domain controllerre belépni.
    - Amennyiben sikerül, akkor elfogadja az authentikációt.

34

Egy alap szerver konfiguráció

- User authentikációs metódus, titkosított jelszókezeléssel:

  security = user
- Ahhoz, hogy a jelszavak a hálózaton biztonságban legyenek,
  - szükséges hogy titkosítva továbbítsuk. Ennek beállítása:

    encrypt passwords = yes

35

Jelszavak tárolása

- A Win és a Unix/Linux rendszerek jelszó kódolási algoritmusa különbözik.
  - A kódolás egyirányú, a titkos jelszóból az eredeti jelszó nem nyerhető vissza.
- Így a Linux jelszavakat nem tudjuk felhasználni a samba authentikációhóz.
  - Vagyis kódolt jelszavak esetén a samba jelszavakat külön meg kell adnunk és tárolnunk.
  - Az állomány, amely a jelszókat tárolja a következő sorral adható meg:

    smb passwd file = /etc/samba/smbpasswd

36

Jelszavak tárolása

- A jelszó beállítása: az **smbpasswd**.
- Ehhez először fel kell vennünk a samba felhasználókat.
  - így az első alkalommal a -a paraméterrel kell meghívnunk:

    smbpasswd -a <felhasználó>
- Ha a Samba felhasználók neve nem egyezik meg a Linux accountokkal:
  - akkor leképezést is megadhatunk a kettő között.
  - Ezt az smbusers állománya tartalmazza. Megadása:

    username map = /etc/samba/smbusers

37

Megosztások kezelése

- Publikus, csak olvasható megosztás:

```
[public]
comment = Publikus
path = /home/samba
public = yes
writable = no
printable = no
```

- Értelmezés:
  - Itt a [] jelek közötti szöveg a megosztás neve
  - A comment a megosztás leírása.
  - A *path* paraméter a megosztott jegyzék.
  - A *public* jellemzővel mindenki számára elérhetővé tesszük.
  - Viszont mivel a *writable* paramétert *no*-ra állítottuk, így csak olvasható lesz.

38

Megosztások kezelése

- Ha azt szeretnénk, hogy a felhasználók egy csoportja írhassa:

  write list = felhasználói felhasználó2 …
- A felhasználók felsorolása helyett megadhatunk csoportot is.
  - Ilyenkor a csoport neve elé be kell írnunk a "@" jelet.
- Log: /var/log/samba/

39

Megosztások elérése

- Több disztribúcióban: smbclient
  - FTP-hez hasonló utility

```
# smbclient //gépnév/megosztás -U <felhasználó>
```

- mount, smbmount:

```
# mount -t smbfs -o username=skywalker //gépnév/megosztás
  /mnt/windóz
```

40


Köszönöm a figyelmet!
41