Fábián Zoltán – Hálózatok elmélet

Operációs rendszerek Jogosultságkezelés

Jogosultságkezelés

- Minden objektumra van jogosultság
  - Könyvtárak
  - Fájlok
  - Device (Printer, scanner, stb...)
  - Alkalmazások
  - Szolgáltatások
- Különböző rendszerek különböző koncepciók
  - Linux
  - Netware
  - Windows NT család

Jogosultságkezelés – közös elvek

- A userek csoportokba szervezhetők
  - Ha egy csoportnak a tagja a user, akkor minden jog, amit a csoport kap, rá is érvényes
  - A csoportok egyes esetekben hierarchiát is alkothatnak
  - Hogyan adjunk jogot?

Hogyan osszuk a jogosultságokat?

1. Feladatok, szervezeti egységek alapján csoportokat alkotunk
2. Megadjuk a csoportoknak a jellemző jogait
3. Felvesszük a felhasználókat
4. Besoroljuk a megfelelő csoportba
5. Megadjuk nekik a saját jogaikat
6. Megadjuk a kivételes tiltásokat

Linux jogosultságkezelése 1

- Istencsászár: root – mindenhez van joga, ezért veszélyes használni
  - Root-tal nem lépünk be távolról
  - Másik usert használunk
- Minden objektum
  - Olvasható (r) - 4
  - Írható (w) - 2
  - Futtatható (x) - 1
- Minden objektumnak van
  - Tulajdonosa
  - Csoportja
  - Mindenki más

Linux jogosultságkezelése 2

- Példa
  - Tulajdonos (rw-) => 6
  - Csoportja (rw-) => 6
  - Mindenki más (r--) => 4
  - => rw-rw-r-- => 664
  - Mit jelent a 775? => rwxrwxrw-
- Chmod – paraméterek
  - Művelet
    - + jog hozzáadás
    - - jog elvétel
    - = engedély beállítása
    - r,w,x jogok fajtái
  - Kinek adjuk a jogot
    - u tulajdonosnak adunk jogot
    - g Csoportnak adunk jogot
    - o mindneki másnak adunk jogot
    - A mindenkinek jogokat adunk
  - -R rekurzív jogok adása

Linux jogosultságkezelése 3 chmod példák

- chmod u+x gyakorlas.txt # Futtatási jogosultságot ad a fájl tulajdonosának.
- chmod go-rx gyakorlas.txt # Visszavonja az olvasási és futtatási jogosultságot a csoport tagjaitól és mindenki mástól.
- chmod a=r gyakorlas.txt # A fájl jogosultságait csak olvashatóra állítja minden felhasználó számára.
- chmod 444 gyakorlas.txt # A fájl jogosultságait csak olvashatóra állítja minden felhasználó számára.

Fájl tulajdonosának módosítása

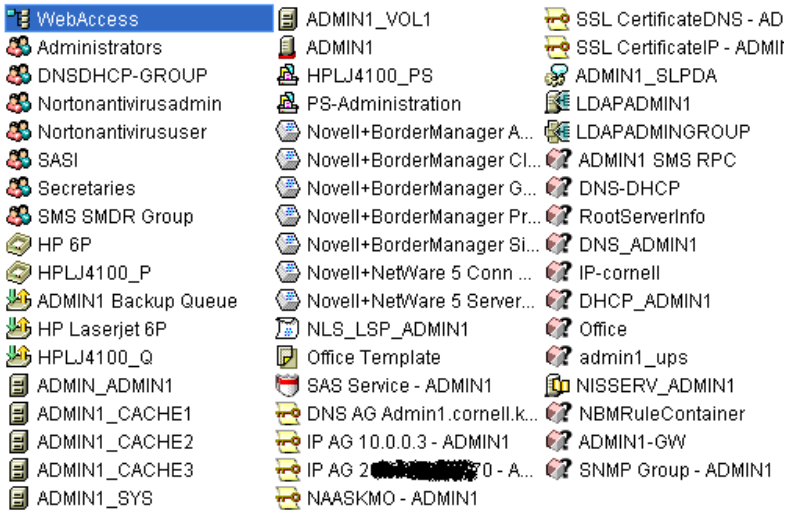
- A fájl tulajdonosának és csoportjának megváltoztatására alkalmas parancsok:
- chown # A fájl tulajdonosát változtatja meg.
- -c # Azon állományok nevét jeleníti meg, melyeknek a tulajdonosa megváltozott.
- -f # Tiltja a hibaüzenetek megjelenítését.
- -R # A fájlok tulajdonosát az alkönyvtárakban is módosítja.
- -v # A módosításokról részletes listát készít.
- Példák:
  - chown zsozso gyakorlas.txt # A fájl “zsozso” tulajdonába kerül.
  - chgrp felhasznalo gyakorlas.txt # A fájl a “felhasznalo” csoportba kerül.
  - chown zsozso:felhasznalo gyakorlas.txt # A fájl “zsozso” tulajdonába és a “felhasznalo” csoportba kerü

Webszerverek jogosultságai

- Root user – nem használjuk
- Apache – user: Futtatja az Apache-ot => php-t
- Xy-user – csak a saját könyvtárstruktúráját láthatja

Netware jogosultságrendszere

- Novell Directory Services – Címtár
  - Jogosultságok kezelése
  - Userek adatai
  - Beléptető, authetnikáló rendszer
  - Elosztott
  - Szinkronizálható több Netware szerver között
  - AD-vel korlátozottan kompatibilis
- Kezelése
  - Régen Windows kliens program
  - Console One kliens



NetWare-ek jogosultságkezelése

- A szerver nem hozzáférhető a userek számára, konzolnak nem kell jogosultságkezelés
- Speciális user: Supervisor = Istencsászár
- Auditáló user = Nem tud semmit csinálni, csak ellenőrzi a többi usert.
- Csak könyvtárakra és fájlokra vonatkozó jogok
  - Read – Olvashat egy fájlt
  - File Scan – Listázhat egy könyvtárat
  - Write – Írhat egy fájlba (könyvtárba)
  - Execute – Futtathat egy fájlt
  - Create – Létrehozhat egy fájlt, könyvtárat
  - Modify – Módosítani lehet egy fájl tartalmát
  - Delete – Fáj(könyvtár) törlési jog
  - Supervisor – Mindenre van joga
  - Access – Másnak átadhatja a felhasználó a jogait
- File-ok saját attribútumai
  - Read only
  - Hidden
  - System
  - Archív
- Userek jogosultságrendszere
  - Userek tagjai lehetnek csoportoknak
  - Csoportok tagjai lehetnek más csoportoknak
  - Userek beállíthatják, hogy más userekkel egyenrangúak legyenek

- Jogosultságok lehetnek az NDS-re is
  - Olvasási
  - Módosítási
  - Létrehozási
  - Auditálása

Windows NT család jogosultságkezelése

- Beépített felhasználók – lokális userek
  - Alapértelmezett felhasználók és csoportok => Demo
  - Administrator = Rendszergazda,
  - Vendég
  - Jogosultsági szintek: Rendszergazdák, Kiemelt felhazsnálók, Felhasználók, Vendégek
- Userek - Profilok
  - Lokális profil
  - Roaming profil - később

Active Directory

- Active Directory = Címtár
  - Tartalma
    - Felhasználók nevei és egyéb adatai,
    - Jelszó
    - Viszonya a rendszerben
    - UID – User ID – ez azonosítja a felhazsnálót
  - DNS-re épülő szolgáltatás
  - Feladatai
    - Bejelentkeztetés – jogosultságkezelés
    - Címtár adatok kiszolgálása különböző alkalmazások részére (pl. Exchange)
  - Gépeket is domainba kell léptetni -> Utána a gépbe belépést az AD engedélyezi
- Active Directory felhasználók
  - Alapértelmezett felhasználók és csoportok => Demo
  - Konténerek – A felhasználók csoportjainak egyedi tárolóhelye
    - Nem lehet két egyforma felhasználói név az AD-ben.
- Gépek beléptetése - hogyan kell?
- Group Policy-k
  - Az AD-ben lévő csoportokra alkalmazható szabályok gyűjteménye
    - Userekre vonatkozhat
    - Munkaállomásokra vonatkozhat
    - Szerverekre vonatkozhat
    - Alkalmazásokra vonatkozhat
    - Eseményekre (pl. belépés, kilépés)

Jogosultságok osztása

- Lokális jogok – engedély, tiltás
  - Fájlokra és könyvtárakra adható jogosultságok (olvasás, írás, módosítás, futtatás, tulajdonos) – Lokális jogok
  - A jogok öröklődnek alapesetben a könyvtárstruktúrában
  - El lehet venni az öröklődést
- Megosztási jogok – engedély, tiltás
  - A jogok öröklődnek
- A kétféle jog eredője lesz az effektív jog

Célszerű kialakítás

- Konténerek tükrözzék a személyek és csoportok kialakítását
- Usernév tükrözze a valódi felhasználót
- A csoportok legyenek a felhasználók tényleges csoportjainak leképezései
- Csak annyi jogot, amennyi kell a munkához, de ahhoz legyen elég
- A csoportok tagjai kapják a megfelelő jogot és csak a specialitások legyenek egyénileg beállítva
- Megosztásokban lévő könyvtárak elérésének finom szabályozása
  - A Megosztási jog: mindent engedélyezzünk
  - Lokális jog: csak azok az engedélyek, amelyek szükségesek
  - Az öröklést a korlátozott könyvtárra nem szabad engedélyezni, de a korlátozott könyvtár jogai tovább öröklődhetnek lefelé

Célszerű tevékenységek, tipikus esetek

- Számítógép beléptetése AD-be
- Meglévő felhasználók gépeinek beléptetése AD-be, profilok átmásolása
- Nagy számú felhasználó létrehozása AD-ben
  - Scriptekkel – Power Shell, VBScript, Jscript