Hálózati operációs rendszerek II.

eDirectory menedzsment

eDirectory alapok

- Jellemzők
  - Novell hálózat alapvető szolgáltatása
  - Erőforrások, felhasználók, stb. információit, jogosultságait tárolja
  - Hierarchikus fa szerkezetű
  - Egy egységbe foglalja az inkompatibilis rendszereket
  - A felhasználóknak szabályozott hozzáférést biztosít az erőforrásokhoz
  - Központosítja a hálózati menedzsmentet
  - Felépítése részben tükrözheti egy vállalat szerkezeti felépítését

eDirectory alapok

- eDirectory felépítése, fogalmak
  - Hierarchikus struktúra → fájlrendszerhez hasonló felépítés
  - ***„Tree”***, ***„konténer”*** és ***„levél”*** objektumok
    - legalább egy konténer objektum a ***„tree”*** alatt
  - Objektumosztályok
    - objektumok definíciójára épül az ***„eDirectory”***
      - ***„hálózati erőforrás”*** objektumok
      - ***„strukturális (konténer)”*** objektumok
      - ***„felhasználók és kapcsolódó”*** objektumok
    - Attribútumok
      - objektumok **tulajdonságait** (paramétereit) definiálja
      - ***„eDirectory sémában”*** tárolják az objektum-osztályokkal együtt

eDirectory alapok

- eDirectory felépítése, fogalmak
  - Hierarchikus struktúra
    - ***„Tree”*** objektum
      - legfelső szintű (gyökér) objektum
      - az eDirectory-val együtt jön létre
    - „Konténer” objektumok
      - ***„Security”***
        - speciális, hálózati biztonsággal kapcsolatos objektumok tárolója (Certificate Authority, NMAS)
        - „*Tree*” objektum alatt hozható létre
      - ***„Organization”***
        - vállalatot, szervezetet, telephelyet jeleníti meg
        - „*Tree*” és „*Country*” objektum alatt létezhet
      - ***„Country”***
        - országnév megjelenítése a címtárban (X.500)
        - egy „*Organization*” objektumot tartalmazhat és a „*Tree*” alatt létezhet csak

eDirectory alapok

- eDirectory felépítése, fogalmak
  - Hierarchikus struktúra
    - „Konténer” objektumok
      - ***„Organizational Unit”***
        - szervezeti egységek, osztályok megjelenítése
        - *„Organization”* vagy *„Organization Unit”* alatt létezhet
      - ***„License Container”***
        - OES licenceket tárolja
        - *„Organization”* vagy *„Organization Unit”* alatt létezhet
      - ***„RBS Container”***
        - iManager RBS konfigurálásához
        - *„Organization”* vagy *„Organization Unit”* alatt létezhet
      - „***Domain”***
        - DNS domain-ek megjelenítése (X.500)
        - nem túl gyakori, bárhol létezhet a címtárfában

eDirectory alapok

- eDirectory felépítése, fogalmak
  - Hierarchikus struktúra
    - „Konténer” objektumok
      - ***„Locality”***
        - kiemelt hely megjelenítése, nem túl gyakori
        - *„Organization”* vagy *„Organization Unit”* alatt létezhet
    - „Levél” objektumok
      - ***„Alias”***
        - egy másik objektumra mutat a címtárfában
      - ***„Application”***
        - hálózati alkalmazás
      - ***„Directory Map”***
        - egy szerver fájlrendszerén belül lévő könyvtárra mutat
      - ***„Group”***
        - felhasználói csoport (munkacsoport)

eDirectory alapok

- eDirectory felépítése, fogalmak
  - Hierarchikus struktúra
    - „Levél” objektumok
      - ***„LDAP Server”***
        - LDAP szerver címtárfa objektuma
      - ***„LDAP Group”***
        - LDAP szerverek csoportosítása
      - ***„License Cerificate”***
        - telepített licencekkel kapcsolatos információkat tárolja
      - ***„Organizational Role”***
        - egy kitüntetett vállalati szerepet (beosztást) jelenít meg
      - ***„Print Queue”***
        - nyomtatási sor céljára használt könyvtár a fájlrendszeren belül
      - ***„Profile”***
        - *„login script”* a felhasználók egy csoportjának

eDirectory alapok

- Directory felépítése, fogalmak
  - Hierarchikus struktúra
    - „Levél” objektumok
      - ***„Volume”***
        - a fájlrendszer egy kötetét jeleníti meg
  - Objektum nevek, hivatkozások
    - Két objektum neve azonos is lehet a címtárfában
    - Abszolút hivatkozás
      - típus nélküli hivatkozás esetén mindig ponttal kezdődik a név pl.: ***„.xy.cd.ab”*** vagy ***„.xy.fd.ab”***
      - típus jelölésével is megadhatók a nevek pl.: ***„.cn=xy.ou=cd.o=ab”***
      - típusok jelölése: ***O*** *(Organization),* ***OU*** *(Organization Unit),* ***C*** *(Country),* ***DC*** *(Domain)*
      - *LDAP esetén csak típusjelöléses hivatkozás létezik:* ***„cn=xy,ou=cd,o=ab”***

eDirectory alapok

- Directory felépítése, fogalmak
  - Objektum nevek, hivatkozások
    - Abszolút hivatkozás
      - típus jelölése esetén nem kötelező ponttal kezdeni a hivatkozást
      - hivatkozásban ***balról-jobbra olvasás*** a címtárfában ***alulról-felfelé haladást*** jelent
      - *„eDirectory”*-ban ponttal, míg *„LDAP”*-ban vesszővel választjuk el a hivatkozásban az objektumokat egymástól
    - Relatív hivatkozás
      - hivatkozás az aktuális kontextushoz képest
      - *„Windows”*-os gépek esetében ***„cx”*** paranccsal lehet az aktuális kontextust váltani
      - Hibázás kockázata miatt nem ajánlott

eDirectory alapok

- eDirectory alapú authentikáció
  - „eDirectory” másik fontos, központi szereppel bíró feladata
    - Felhasználó „okmánya” alapján ellenőrzik az erőforráshoz való hozzáférés jogosságát
      - az ***„okmány”*** és a ***„hitelesítő aláírás”*** létrehozása bejelentkezés után
      - felhasználó hozzá akar férni valamilyen szolgáltatáshoz
      - kapcsolatfelvétel, véletlen szám generálása és küldése a felhasználónak (titkosítva a ***publikus*** kulcsával)
      - ***„lenyomat”*** előállítása a titkosított véletlen szám dekódolásával (szolgáltatás hitelesítése)
      - felhasználó visszaküldi a ***véletlen számot,*** a ***„hitelesítő aláírást”*** és az ***„okmányt”*** (felhasználó hitelesítése)
      - ha minden rendben, felhasználó hozzáférhet a szolgáltatáshoz

eDirectory alapok

- eDirectory adatbázis
  - Rejtett könyvtárban található: SYS:_NETWARE
  - Több különböző, egymással szoros kapcsolatban álló fájlból áll össze
    - Naplózó (log) fájlok a tranzakciók követésére
      - NDS.DB: adatbázis vezérlője, befejezetlen tranzakciók naplózása
    - NDS.01 (max. 4GB): adatbázis rekordok és néhány index fájl
    - XY.NDS: stream típusú attribútumok tárolása
      - pl.: login script, print job configuration
  - Indítás, leállítás
    - Konzolon
      - Indítás: ds
      - Leállítás: unload ds.nlm

Időszinkronizáció

- Jellemzők
  - Szoros kapcsolat az eDirectory adatbázissal
    - Objektumukon végzett műveleteket időbélyeggel látják el
  - Szervereknek ugyanazt az időt kell látniuk
    - Időszinkronizáció nélkül nem lehetséges
  - Adatbázis szinkronizálásánál alapvető jelentőségű
- NTP (Network Time Protocol)
  - TCP/IP-t használó rendszerekben alapszolgáltatás
  - Hierarchikus (stratum) típusú szinkronizáció
  - Universal Time Coordinated (UTC) időt

Időszinkronizáció

- NTP (Network Time Protocol)
  - Időszinkronizáció beállítása
    - Maximális időkülönbség a szerverek órái között: 1000s
    - Első alkalommal összes szerver szinkronizálása egy internetes szerverhez
      - „ntpdate x.x.x.x” futtatása
    - NTP.CONF módosítása
      - server 127.127.1.0
      - fudge 127.127.1.0 stratum 10
      - server 10.0.0.1
    - NTP.CONF biztonsági beállításai
      - restrict default noquery nomotify
      - restrict 127.0.0.1
      - restrict 192.168.0.0 mask 255.255.255.0
    - NTP indítása
      - XNTPD.NLM betöltése a szerver konzolon (OES-Netware esetén)

Partíciók

- Mikor van szükség több partícióra?
  - Túl sok objektum egy partícióban
  - Több telephely lassú WAN kapcsolatokkal
  - Felhasználók „***elkülönítése”*** biztonsági okokból
- Partíciók
  - Replikákban tárolja a rendszer
    - ***master, read/write, read-only,*** stb.
  - Hibatűrés
    - ***minimum 3*** replika minden partícióról
  - Partíciók kezelése (l. gyakorlati bemutató)
    - létrehozás, mozgatás, összefűzés

Replikák

- Replikatípusok
  - ***„Master”***
    - egy partíció első replikája
    - legmagasabb szintű replika-műveletek
      - szerver hozzáadás/elvétel
      - replika vagy partíció hozzáadás
  - ***„Read/Write”***
    - Teljes másolata (írható/olvasható) a ***„master”*** replikának
    - Objektum-műveletek ezen a replikán is végrehajthatók
    - ***minimum 3***, de ***maximum 8 „read/write”*** replika egy partícióról

Replikák

- Replikatípusok
  - ***„Read-Only”***
    - hasonló, mint a ***„read/write”*** replika, de csak olvasható
      - ritkán használják
    - eDirectory keresések gyorsíthatók valamint a hibatűrés növelhető
  - ***„Filtered”***
    - szerverenként szűrhető a replikált objektumok és tulajdonságaik típusa
    - szerver objektum tulajdonsága
  - ***„Subordinate reference”***
    - nem igazi replika, ***„csak egy mutató”***
    - a rendszer automatikusan hozza létre ill. törli

Replikák

- Replikák kezelése
  - Létrehozás, törlés, replikaállapot ellenőrzés
    - lásd gyakorlati bemutató
- eDirectory címtárfa tervezése
  - kis és közepes méretű cégek
    - jellemzően egy telephely, néhányszor tíz felhasználó
    - különböző típusú objektumok külön konténerbe
  - közepes méretű cégek
    - jellemzően több telephely, lassú WAN kapcsolatok
      - esetleg egy nagy telephely gyors WAN összeköttetések
    - decentralizált rendszerfelügyelet
    - alsó rétegek kialakítása
      - közös erőforrások és projektek, szervezeti struktúra alsóbb szintjei alapján

Replikák

- eDirectory címtárfa tervezése
  - Nagyvállalatok
    - földrajzi kiterjedés, telephelyek száma, távolsága
    - vállalat irányítási struktúrája
    - WAN kapcsolatok mennyisége, sebessége
    - telephelyek helyi hálózata
    - objektumok száma és eloszlása
  - Skálázhatóság, hibatűrés, erőforrások elérése
    - WAN forgalom optimalizálása
      - partíciók földrajzi elhelyezkedés alapján
      - partíciók ne tartalmazzanak lassú WAN kapcsolatokat
    - legalább két replika minden partícióról
    - ***„master”*** replikák közel az ***„admin”***-hoz
    - replikákat közel a felhasználókhoz