Előszó

Ezt a kidolgozást a 2009 őszén leadott anyag alapján csináltam. Felhasználtam a korábbi kidolgozásokat, a saját jegyzetet és mindenféle netes, Microsoft-os, technetes anyagot, amit találtam.

Ha hibát találtok benne, kérlek javítsátok ki!

Kántor,

cantor@sch.bme.hu

1. Az Active Directory logikai felépítése

A **logikai** felépítés, az AD-ben megjelenő logikai komponensek szerinti felépítés, felhasználói szempontból érdekes, szolgáltatásokat kezeljük vele. (*Kezelésére az Administrative Tools-on belül az Active Directory Domain and Trusts és Active Directory User and Computers szolgál*), hierarchikus felépítés jellemzi:
erdő → tartományi fa → tartomány (ábrákon háromszöggel jelölve), → szervezeti egységek (körrel jelölve az ábrákon, pl. könyvtárak, háttértárak). → objektumok, ezeken kívül a logikai felépítés részét képezik a bizalmi kapcsolatok és a séma.

AD DS Objektumok

- objektumok: sémában definiált tulajdonságok alapján **attribútumok** vagy **paraméterek** csoportja tartozik hozzájuk, ezekből épülnek fel.
- Legfontosabb objektumok: PC,felhasználó,nyomtató,megosztott könyvtár,csoportok,névjegy, InetOrgPerson (szabványos felhasználó, ami más címtárakkal is kompatibilis).

Szervezeti egysége

- objektum tárolók, objektumokat lehet szervezeti egységekbe csoportosítani, osztályozni
- hierarchikusan egymásba ágyazhatók,
- csoportházirendek vonatkozhatnak rájuk
- tartományok alapegységei

Tartomány

- Az AD alapegységei (házirendek, a replikáció és biztonság szempontból). Egy mindenképpen van!
  - **adminisztrációs szempontból** alapegység mert alapértelmezetten a tartományi adminisztrátorok azok akik foglalkoznak a rendszer üzemeltetésével, nekik van jogosultságuk további jogosultságok osztogatására
  - **házirendek szempontjából,** mert a csoportházirendek tartományokon érvényesek.
  - **biztonsági szempontból** is alapegység, mert a biztonsági beállítások is a tartományi házirendeken keresztül állíthatóak be.
  - **replikációs szempontból** is alapegység, mert a logikai partíciók közül (alkalmazási, tartományi, konfigurációs, séma) a tartományi partíció mindenhol azonos tartományon belül, ennek a változásai automatikusan átvezetődnek.

Tartományi Fastruktúra

- egy névteret szimbolizál,
- fentről lefelé lehet felépíteni.
- szülő gyerek viszony alakítható ki a tartományok között.

Kapcsolatok

- bizalmi (trust) kapcsolatok a tartományok és erdők között (bizalmi, mert megbíznak egymás azonosítási rendszerében),
- lehet egy vagy két irányú (trusting és trusted),
- lehet tranzitív vagy nem (többlépéses).

Erdő

- több tartomány összefogására
- egységes logikai partíció, egy és oszthatatlan a séma van,
- közös globális katalógus,
- Enterprise Admin (csak ő hozhat létre erdőket)

Séma (*MMC-s használatához: regsvr32 schmmgmt.dll parancsot kel kiadni a parancssorban)*

- ez az adatbázis definíció helye, az adatbázis szerkezetét adja meg.
- tartalmazza objektum osztályok és attribútumok definícióját tartalmazza.
- pontosan megadja, hogy az egyes objektumok milyen attribútumokból állnak.
- bővíthető (új objektum osztályok is létrehozhatók, örököltethetők egymásból), de törölni nem lehet, csak tiltani
- egész erdőben tovább replikálódnak az itt tárolt adatok
- Schema Admin (sémák kezelése).

2. Az Active Directory fizikai felépítése

F**izikai** felépítés, tényleges fizikai eszközök szerinti felépítés, inkább adminisztrátori, üzemeltetői szempontból érdekes. (*Az Administrative Tools-on belül az Active Directory Sites And Services-szel lehet kezelni*) részei:

- tartomány vezérlő szerver,
- telephely,
- adatbázis,
- globális katalógus (tartomány vezérlőkön bekapcsolható szolgáltatás, ekkor a teljes erdő legfontosabb adatait tárolják a tartományi vezérlők),
- Read-Only Domain Controller.

Tartományvezérlők

- AD alapegysége: az AD működéséért fellelnek, tárolják a tartományi információkat.
- Kötelező TCP/IP hálózat támogatás és DNS!
- Egyszerre csak egy tartománynak lehet a része.
- Többet érdemes használni (terhelés eloszlás és rendelkezésre állás miatt), ezek egymással replikálnak

Telephelyek

- Olyan alhálózatok, amik általában fizikailag is különböző helyeken vannak, osztályozásuk:
    - Kicsi telephely: nincs szerver, csak nagy sávszélesség (nincs szerverüzemeltetés, védelem, stb.).
    - Közepes: DC van, de GC nincsen, ekkor jó a cachelés (erdő szintű replikáció nincs).
    - Nagy telephely: DC és GC is van (védelem is van és van erdőszintű replikáció).
- Belül nagy sebesség a tartományvezérlők és a számítógépek között (automatikus replikáció, multimaster-es), de kifelé lassú WAN kapcsolat (telephelyek között nincs automatikus replikáció)
- egy tartományhoz több telephely, egy telephelyhez több tartomány tartozhat.
- automatikus beállítások és az egyszerűbb kezelés miatt érdemes létrehozni (vagy a földrajzi jellemzők miatt)
- DS (Distributed Filesystem) szolgáltatásnál is figyelembe veszik(hetik) a felhasználók a telephely konfigurációt;
- **infrastruktúra szolgáltatásokra** is lehet használni ,minden kliens a saját telephelyén belül veszi igénybe szolgáltatásokat, pl helyben nyomtat és nem a világ másik felén
- telephelyek SiteLinkek-kel vannak összekapcsolva
    - **SiteLink**: rögzíti, hogy milyen szabályokkal tud két telephely replikálni, a rendszergazdák ezeket a szabályokat adják meg. (Beállítások: milyen időzítéssel és milyen protokollt használjon, de hogy merre menjen, azt az IP beállításoknál kell megadni (mert nem mindegy, ha pl. van egy bérelt vonal, akkor ténylegesen azon megy-e az információ) ez a költség beállítása). Lehetőséges protokollok:
        - IP (RPC) alapértelmezetten, nem tűzfal barát, de szinkron
        - SMTP tűzfalbarát, de aszinkron

Adatbázis (bővebben a13-as tétel)

- **NTDS** (NT Directory Service) mappa (a Windows mappán belül) tartalma:
    - az ntds.dit maga az adatbázis,
    - .jrs-ek a tartalék naplók,
    - edb.log a napló fájl.
- **SYSVOL** mappa (a Windows mappán belül)
    - tartalmazza a házirendeket (globális egyedi azonosítókkal 31 és a 6a a két alapvető házirend),
    - tartalmazza a replikálandó fájlokat.

RODC (bővebben 15-ös tétel)

Csak olvasható tartományvezérlő.

Globális katalógus (bővebben a 11-es tétel)

Erdőre jellemző adatokat tároló DC.

3. DNS és Active Directory

A Windows DNS adatbázis és névszolgáltatás az Active Directory működésének alapja! DNS tönkremegy, akkor az AD is elromlik.

Tulajdonságok:

- TCP / IP-s elnevezési konvenció jellemzi aWindows DNS neveket.
- DNS szintaktikának megfelelő névtereket adunk a tartományoknak. Megjegyzés: erdőnek (is) ajánlott, hogy kéttagú neve legyen, mert sok szolgáltatás ezt várja el (pl. az Exchange Server)
- AD specifikus SRV rekordok használata kötelező (service location rekordok: tárolják hogy pl. milyen protokollon érhetők el az adott szolgáltatások), ezeket is a DNS szerverek tárolják.
- SRV rekord szintakszis és példa:

szolgáltatás	protokoll	név	TTL	osztály	típus	prioritás	súly	port	számítógépnév
_ldap.	_tcp.	contoso.msft		600	IN	SRV	0	100	389 den-dc1.contoso.msft

- prioritás és súly rekordok a terhelés eloszláshoz kellenek (alacsonyabb prioritású, magasabb súlyú a fontosabb)
- Adminisztrálás a DNS Manager-rel.
- Netlogon service végez minden fontos DNS-sel kapcsolatos feladatot.
- *netlogon.dns* fájl-ban lévő információkat kell átvezetni (ha nincs bekapcsolva az automatikus átvezetés)
- *(-ipconfig /registerdns dinamikus regisztráció frissítése, vagy a netlogon servcie újraindítás SRV esetén)*
- *(-nslookup-pal lehet a DNS szervereket megtalálni, kapcsolókkal távoli szerverek is menedzselhetőek)*
- **DNS zóna**: DNS tartomány névtere, vagy annak egy része.

AD DS integrált zónák

Az AD DS adatbázisban is lehet tárolni zóna információkat, ezek az AD DS integrált zónák. Mivel a DNS rekordok a címtárban tárolódnak, így lehetőség van kihasználni annak előnyeit:

- az AD DS replikációja változásokat, DNS replikációt is végez
- multimasteres DNS lehetőség (több DNS szerver is lehet)
- növeli biztonságot (secure dynamic update bekapcsolásával a DNS szemetelőket ki lehet szűrni)
- támogatja a korosodást (dinamikus DNS-nél az információkat mikor lehet megújítani) és a takarítást (az érvénytelen zóna információk törlése automatikusan)

Adattárolás megvalósítása

- A Windows Server 2000 tartományi információk közt tárolta, 2003 óta alkalmazás partíciók vannak
- Alkalmazás partíciók: domainDNSZone, ForestDNSZone (erdőn belül csak oda replikálódik ahol van DNS, automatikusan kezeli, de lehet sajátot is csinálni)

Dinamikus frissítés: Az a lényeg, hogy először a DC-hez fordul a DNS ügyfél a regisztrációjával vagy frissítési kérésével, majd ha attól megkapott minden fontos (DNS szerverre vonatkozó) információt, akkor fordul a DNS-hez.

Kapcsolódó egyéb fogalma:

Biztonságos dinamikus frissítés: AD DS autencikáció előzi meg a frissítést, csak akkor enged frissíteni, ha ehhez joga van.

Stub DNS zóna: zóna adatait másolja, de csak a SOA rekordot, az NS rekordokat (name szerver információkat) és alias rekordokat, ez azért jó, mert a DNS szerver ez alapján is megtalálható és kevesebb replikációra van szükség.

Condtitional forwarding opció: hasonló az előzőhöz, de a stub zóna dinamikus változásokat is viszi és a regisztrált NS rekordjait tárolja, mást nem.

Reverse zónát (emlékeztető: a reverse look up a címhez találja meg a DNS nevet) is mindenképpen érdemes csinálni, hogy a kliensek kéréseit helyben vissza lehessen utasítani és ne kóválygojanak a kérések a hálózaton összevissza

Háttér zóna betöltés: hatékonyság növelés érdekében a Server 2008-ban vezették be. A service indítása után, már betöltés közben is tud válaszolni a klienseknek a korábbi bejegyzésekből.

Read Only DNS zóna

- RODC támogatja létrehozását.
- Mindegyik alkalmazás partíció replikálódik a RODC-be.
- Nem lehet írni, ezért nehezebb támadni.
- A bejegyzési kéréseket tovább küldi egy írhatónak, semmilyen módon nem lehet ezeket módosítani.

4. Szervezeti egységek

- **Objektumtárolók.**
- A tartomány alapegységei, segítségükkel az objektumokat lehet csoportosítani. Ahhoz hasonlítható a működése, mint amikor a háttértáron mappákat hozunk létre fájlok csoportosítására. Ehhez hasonlóan szervezeti egységekbe szervezhetjük az Active Directory objekutomokat. ennek megfelelően, a belerakott objektumok öröklik a szervezeti egységre vonatkozó jogosultsági beállításokat és a szervezeti egységekre vonatkozó házirendek is vonatkoznak rájuk (hasonlóan, mint amikor egy mappát írásvédetté teszünk, akkor a benne lévő fájlok sem módosíthatók).
- Mappákhoz hasonlóan egymásba ágyazhatók, így változatos hierarchia alakítható ki használatukkal. Természetesen a tartalmazott szervezeti egységek öröklik a szülők beállításait.
- Fentiek jelentik egyben a szervezeti egységek használatának előnyeit, mert segítségükkel az objektumokat rendszerezhetjük, közösen állíthatjuk be a rá vonatkozó jogosultságokat, stb. Csoportházirendeket állíthatunk be rájuk. Ezenkívül használatukkal átláthatóbb rendszert alakíthatunk ki (a fájlokat is szívesen rakja mappákba az ember).
- Telepítés után létrejön egy alapértelmezett hierarchia. Az alapértelmezett tároló struktúrában egyetlen egy „igazi” szervezeti egység a Domain Controllers Organizational Unit van amibe a tartományvezérlő számítógépek kerülnek be. A többi tároló nem igazi szervezeti egység, ők egy container típusú objektumok. Elvileg lehet ilyen tároló (container) típusú objektumokat a későbbiekben is létrehozni, de ezek kerülni kell, a szervezeti egységeket érdemes használni.
- A csoportok is csoportosító objektumok mégis jelentős különbségek vannak a szervezeti egységek és a csoportok között:
    - Egy objektum több csoportba tartozhat, de csak egyetlen szervezeti egységbe (mint ahogy egy fájl csak egy mappába).
    - Beállíthatók rájuk csoportházirendek, míg csoportokra nem.
    - Kezelő személy(zetet) is beállíthatunk a szervezeti egységekhez, míg csoportokhoz nem.
- Egyszerre érdemes őket használni: **Shadowgroup**-okat alakítunk ki, vagyis minden szervezeti egységhez létrehozunk egy csoportot és ebbe kerülnek a felhasználók. Így egyszerre kezelhetjük őket csoporttagokként és szervezeti egység objektumaiként.
- Használatukkal kapcsolatban ajánlások:
    - (jogosultságokra) a szervezeti egység szintjén állítsuk be a jogosultságokat automatikusan öröklődni fognak; természetesen az egyes objektumokra lehet külön-külön jogosultságokat megadni => menedzselés bonyolultabb
    - (házirendekre) az általános szolgáltatásokat használjuk inkább, minél kevesebb kivételes konfigurációs dolgokat (pl. block inheritance, enforcement) áttekinthetőbb lesz a rendszer
- Használatuknál (hierarchia kialakításánál) érdemes mérlegelni a meglévő adminisztrációs struktúrát, milyen részlegek vannak, a feladatköröket, a földrajzi adatságokat. Összesen 12 szintig ágyazhatók egymásba, de az ajánlás, hogy 3 fölé ne menjünk.
- Lehetséges plussz beállítás a szervezeti egységekre az auditálás vagyis naplózás.
- *Kezelésük az Administrative Tools-on belül a Users And Computers-szel történhet.*

5. Csoportok kezelése

A csoportok a **group objektumok** az AD-ben. A csoportok használatával az adminisztráció megkönnyíthető, jogosultságokat a benne lévő objektumok is megkapják.

Típusai

- **terjesztési** (kommunikációs alkalmazásoknál, email közös küldése), nincs biztonsági azonosítójuk,
- **biztonsági** (jogosultság kezelés, security principal-ja van!), a funkcionalitási szint meghatározza, hogy milyen lehet.

Érvényességi körök (honnan tartalmazhatnak tagokat és hol lehet őket használni):

- globális tartományon belülről tartalmazhat felhasználókat és bárhol felhasználható)
- tartomány-lokális (tartományon kívülről tartalmaz tagokat, de csak az adott tartományon használható fel)
- lokális (ez kilóg, mert ez a munka állomáson a helyi objektum, AD-ben nem használják),
- univerzális(bárhol felhasználható és bárhol kaphat jogosultságot, emiatt a GC tárolja a tagságot)

Alapértelmezett csoportok (alap jogosultságok definiálva vannak az AD-ben rájuk):

- account operátorok (objektum kezelők)
- admin: atyaúristen után a második, mindenhez joga van
- back up operátor (biztonsági mentés kezelése, nincs mindenre olvasási joguk, csak megfelelő függvény hívásokon át.)
- Incoming Forest Trust buliders (erdők összekapcsolására)
- performancelog, performance monitor users
- preWS2000 compatible acces (nem kerberos-os)
- network config operátor
- replikátor
- remote desktop
- server operátor (szerver szolgáltatások kezelése)
- fehasználók
- nyomtató operátorok

Speciális azonosságok (dinamikus csoportok, de a csoporttagságot automatikusan kezeli a rendszer):

- anonymous logon
- autentikált felhasználók
- Objektum létrehozója
- objektum tulajdonosa
- Betárcsázós felhasználó
- Mindenki
- Interactive (aki éppen dolgozik)
- Local System
- Network
- Service
- Terminal Server users
- This Organization
- Other Organization

AGDLP

Csoporthasználat ajánlás: **A**(ccount) **G**(lobal group) **D**(omain)**L**(ocal) **P**(ermission),
Afiókokból globális csoportokat hozunk létre. Az erőforrások jogosultságaihoz domain lokális csoportokat tudunk létrehozni (pl. nyomtatót használó felhasználók). Globális csoportokat összepárosítjuk a domain lokális csoportokkal. (Több tartományos rendszerben a G és DL közt van a határ.)

DomainLocal: más tartományból is tartalmazhat tagokat, de csak az adott tartomány erőforrására érvényesek a jogosultságai. **Global:** csak a saját tartományából beletett tagokat tartalmazza, viszont bárhol felhasználható.
Ajánlás: nagy rendszerek esetén a négyszintű osztályozás túl bonyolult, ekkor érdemes felhasználni az univerzális csoportot, ezt a G és D közé érdemes berakni, ezután az egyes csoportok egymásba ágyazhatók.

Csoport használati stratégia

- minimális jogosultságokat adjuk meg (ehhez érdemes ajánlást készíteni)
- kevés felhasználó esetén ACL (objektum-hozzáférési) listára lehet őket rakni, egyébként érdemes csoportosítani

Egyszerre érdemes őket használni a szervezeti egységekkel: Shadowgroup-okat alakítunk ki, vagyis minden szervezeti egységhez létrehozunk egy csoportot és ebbe kerülnek a felhasználók. Így egyszerre kezelhetjük őket csoporttagokként és szervezeti egység objektumaiként

6. Csoportos házirendek szolgáltatás működése

Házirendek csoportosítása

- **Csoport házirend**
  - ennek segítségével a számítógép és a felhasználó objektum bealításait adhatjuk meg központilag, különböző szinteken (tartományok, szervezeti egységek)
  - milyen konfigurációval működjön a rendszer (mindkét objektum oldalán lehet érdekes),
  - szoftver terjesztésre, telítésre,
  - biztonsági beállítások is.
- **Helyi házirend / lokális házirend**
  - adott számítógép konfigurációja

Csoport házirendek csoportosítása

- **felhasználó**i házirendek: beállítások vonatkoznak a szoftverekre, windowsra, biztonságra, desktopra
- **számítógépre vonatkozó**: beállíthatók a szoftver, az operációs rendszer, a biztonság *mmc-ben kell hozzáadni a policy management editor-t szerkesztéshez.*

Házirendekek működése

1. Bekapcsoláskor azonosítás után lekéri a gépre vonatkozó házirendet és azt érvényre jutatja, később 90+-(30) percenként ellenőrzi, hogy történt-e változás
2. Bejelentkezéskor jutnak a felhasználói házirendek is érvényre, itt is 90(-+30) percenként frissítés, Vistan és Xp-n a helyi cache-ből egy gyorsabb bejelentkezés is történhet (ebből következik, hogy a házirendek csak a második bejelentkezéskor jutnak érvényre)
3. Kijelentkezéskor / kikapcsoláskor lefutnak a házirendben definiált scriptek.

Tulajdonságok

- Több mint 2000 beállítási lehetőség.
- **Group policy (Administrative) template** (házirend sablon): .admx (.adm Xp-ben) sablon fájlok. XML alapú szintaxis jellemzi, alapvető házirend beállításokat tartalmaz és megadja registry-beli beállítás helyét is.
- **Central store mappa**: admx (adml) fájlok repository-ja (innen töltik le a többiek), a SYSVOL mappa tartalmazza, manuálisan kell létrehozni, a Vista és a S2008 automatikusan észreveszi ha van, ez tovább replikálódik a többi tartományi vezérlőre.
- **Group policy object** (házirend objektum): megmondja, hogy hol kell alkalmazni és mit
- **Group polcy container** (házirend konténer): milyen szabályok szerint kell alkalmazni a kész szabályokat.
- GPO tartalmaz GPC(Site, domain, OU)-ket, az pedig GPT(ADMX)-ket,
- A tartomány vezérlő tartalmazza, hogy milyen verziójú házirend érvényes és az hol érvényes (a verziót azért menti el, hogy 90 perces frissítésnél összetudja hasonlítani őket).
- Érdekesség: Házirendeket is házirendeken keresztül lehet konfigurálni.
- Kiértékelési sorrend:
  1. Local Group policy (install) – helyi beállítások
  2. Site policy – telephelyi beállítások
  3. Domain policy – tartományi beállítások
  4. OU policy – szervezeti egység beállítások
  - Ami később jön, az felülírja az általános beállításokat
- Úgy érdemes használni, hogy "házirend csoportokat" érdemes létrehozni és ezekbe érdemes a felhasználókat pakolni.
- A SYSVOL mappából olvassa ki a házirendeket a rendszer.
- Helyi házirend lehetőségek Vista-tól vannak (korábban csak egy volt mindenkire): adminok, nem adminok, és felhasználó specifikus helyi házirendek készíthetők.
- Slow Network Connection: a csoportházirend kapcsolat küszöb értéke 500 kb/s, ezt a Network Location Awareness service ellenőrzi (korábban ICMP-s pingelés ment). Ha nincs meg ez a kapcsolat, akkor nem minden házirendet tölt le.
- Active Directory további lehetőségeket nyújt a házirendeknél arra nézve, hogy mi az, ami érvényre jut és mi az, ami nem egy adott számítógép vagy felhasználó esetében (de az ajánlás, hogy ezeket ne nagyon használjuk):
  - **Block inheritance**: el lehet vágni az öröklődési sort.
  - **Enforcement (no override):** erőszakosan alkalmazott házirend (pl. egy házirendre bealítjuk, hogy erődszakos legyen, ilyenkor, a benne lévő paramétereket beírja a rendszer konfigurációba

és írásvédetté(!) is teszi őket. Ez tovább jut a block inheritance-n is. Általában biztonsági beállításokra használják.
    - **Wmi szűrő** (dinamikus érvényesítési lehetőség): szűrési feltételt adunk meg (pl. processszorra, memóriára), ez alapján alkalmazza a házirendet, ez jól jön pl. telepítéséknél (pl. photoshop)
    - **Házirend letiltás**: átmenetileg le lehet tiltani házirendeket.
    - **Loopback processing:** olyan számítógép konfigurálás, amikor nem érdekes hogy ki használja a gépet. Közösen használt számítógépeknél alkalmazzák.
    - **Security filtering**: arra érvényes a házirend, akinek jogosultsága van rá (alapból authenticated users).
    - **Csatolási sorrend:** több házirend esetén kiértékelés sorban, ajánlás: a csatolási sorrend ne számítson
- Több házirendet érdemes használni, de nagyon sokat ne, mert sok idő megy el a kiértékeléssel.

Házirendek Kezelése

- *Group Policy management eszköz, group policy management editor*
- *group policy modelling (reporting) lehetőség: modellezhetjük a házirendek működését a saját rendszerünkön*
- *gpupdate, gpresult parancssoros eszközök*

7. Csoportos házirendek felhasználói környezet beállítására

Csoport házirend

- ennek segítségével a számítógép és a felhasználó objektum bealításait adhatjuk meg központilag, különböző szinteken (tartományok, szervezeti egységek)
- milyen konfigurációval működjön a rendszer (mindkét objektum oldalán lehet érdekes),
- szoftver terjesztésre, telítésre,
- biztonsági beállítások is.

Csoport házirendek csoportosítása

- **felhasználó**i házirendek: beállítások vonatkoznak a szoftverekre, windowsra, biztonságra, desktopra
- **számítógépre vonatkozó**: beállíthatók a szoftver, az operációs rendszer, a biztonság

Házirendekek működése

1. Bekapcsoláskor azonosítás után lekéri a gépre vonatkozó házirendet és azt érvényre jutatja, később 90+-(30) percenként ellenőrzi, hogy történt-e változás
2. Bejelentkezéskor jutnak a felhasználói házirendek is érvényre, itt is 90(-+30) percenként frissítés, Vistan és xp-n a helyi cache-ből egy gyorsabb bejelentkezés is történhet (ebből következik, hogy a házirendek csak a második bejelentkezéskor jutnak érvényre)
3. Kijelentkezéskor / kikapcsoláskor lefutnak a házirendben definiált scriptek.

Beállítási lehetőségek

- több mint 2000 beállítás
- *Group Policy Manager-rel és a Group Policy Management Editor-ral lehet kezelni.*
- hasonlók a felhasználó és számítógépek esetében a beállítások, de vannak különbségek is
- Hasonlóságok
  - Mindkét esetben megadhatók a szoftver terjesztésre vonatkozó beállítások.
  - Mindkét esetben beállíthatók a szoftver tiltások.
  - Mindkét esetben beállíthatók scriptek (ezek beállítástól függően bekapcsoláskor, bejelentkezéskor, kijelentkezéskor, kikapcsoláskor futnak le)
  - Mindkét esetben beállíthatók **Administrative Templatek**: felügyeleti sablonok (admx) fájlok, ezeket is fel lehet használni (ezek tartalmaznak alapvető a házirend beállításokat és a hozzá kapcsolódó registry beállításokat is, objektum típusától függően a HKEY_LOCAL_MACHINE vagy HKEY_CURRENT_USER registry beállíátsok)
- **Különbségek**
  - Főleg az operációs rendszerhez kapcsolódó beállítások különböznek,
  - Számítógép esetében megadhatjuk:
    - Eseménynaplók házirendjeit
    - Korlátozott csoportokat (kötelező tagságot ír elő, illetve tilt felhasználókat)
    - Registry házirendet
    - Fiók és helyi házirend (ezek a biztonsági beállítások is egyben, pl. jelszóházirend ebben van benne)
    - Fájlrendszer házirendet
    - Hálózat és vezeték nélküli hálózat házirendjeit
    - Nyilvános kulcsokra vonatkozó beállításokat
  - Felhasználók esetében beállíthatjuk
    - Milyen oprendszer specifikus programokat indíthat el (pl. Control Panel, parancssor, regedit)
    - Hogyan néz ki a felhasználói felület (asztal, start menü, stb)
    - Felhasználók esetében adható meg a **mappa átirányítás**: ekkor az Active Directory központilag tárolja az AppData és a Dokumentumok mappákat, illetve a start menü és a desktop tulajdonságait. Így központilag kezelhetők, illetve központilag védve vannak ezek.
    - Másik lehetőség a **profil megadás**, valamelyik gépen Documents And Settings/felhasználónév-et hozzárendeljük a felhasználóhoz, és ha más géphez ül le, akkor ez replikálódik át óda bejelentkezéskor (sok ideig tart, nem célszerű használni)
- Mindkét esetben beállíthatók a **group policy prefences** is, ezek ajánlások, nem kikényszerítettek (viszont tetszetős targeting lehetőségeket kínál fel).

8. Csoportos házirendek szolgáltatásai szoftverek telepítéséhez

Csoport házirend

- ennek segítségével a számítógép és a felhasználó objektum bealításait adhatjuk meg központilag, különböző szinteken (tartományok, szervezeti egységek)
- milyen konfigurációval működjön a rendszer (mindkét objektum oldalán lehet érdekes),
- szoftver terjesztésre, telítésre,
- biztonsági beállítások is.

Szoftver életciklus

1. felkészülés (szükség van rá...) a bevezetésre,
2. bevezetés,
3. karbantartási fázis,
4. eltávolítás.

Tulajdonságok

- A házirendes szoftver terjesztéshez MSI csomagok kellenek, amiket a Windows Installer tud telepíteni, előnyei:
  - **egyedi telepítéseket** lehet csinálni (igény szerinti telepítés: nem minden komponens kell (pl. Office-nál nem kell Acces és Outlook)),
  - **resilient alkalmazások** (öngyógyító képességek, pl. töröljük le a word.exe-t)
  - **tiszta eltávolítás** (minden letöröl maga után ahogy illik)
- Használatához kell egy disztribúciós pont (rejtett fájl megosztás).
- *Group Policy Manager-rel és a Group Policy Management Editor-ral lehet kezelni.*

Lehetőségek

- **Assign**: gép-re alkalmazott házirend esetben, indításnál, az adott felhasználónál mindent előkészít, de nem telepít, csak első indításnál. Előnye az, hogy követi a felhasználót. User-re alkalmazva automatikusan települ.
- **Publish**: gép-re alkalmazott házirend esetében használható, dokumentum típusánál regisztrálás, hogy mivel nyissa meg és első megnyitáskor telepíti. Felhasználói házirend esetében: Add Remove Programs-nál add new programs és a felhasználó telepíti őket, de ehhez kell a vezérlőpult hozzáférés, legalább, az, hogy ehhez a mini alkalmazáshoz hozzáférjen (és természetesen unalmában a felhasználó telepíti az összes lehetséges programot ☺).

További tulajdonságok

- MST fájlok segítségével lehet finom hangolni a telepítést, pl script-tel.
- Frissítések: lehet kötelező, opcionális, ki lehet jelölni bizonyos felhasználókat is frissítésre (csak náluk frissít).
- Házirendek segítségével lehet uninstallálni is.
- Fontos, hogy a telepítő készletek folyamatosan rendelkezésre kell álljanak (rejtett fálj dollárral a végén).
- Komolyabb szoftve terjesztésre a System Center Essentials (configuration manager) program csomag ajánlott. Nem csak MSI állományokat kezel, van benne szoftver leltár, tárolja a licenszek számát, szoftverhasználatot mér, stb.
- Házirendes megoldás hátrányai: nem lehet megelőzni, hogy ne reggel kilenckor kezdjen el telepíteni, ami kellemetlen lehet, ha akkor kezdődne a munka.

9. Active Directory replikáció telephelyen belül

Multimasteres replikáció: minden tartományi vezérlő írható és olvasható és a változások automatikusan átvezetődnek a tartományvezérlők között.

Replikációs Tulajdonságok

- **Push** és **pull** típusú replikáció (a másod példány kéri le a változásokat, de van, hogy a forrás kezdeményez).
- **Store and forward** (több tartományon kell végig terjedni, akkor az több lépésben, nem egy helyről)
- Replikáció során lehetnek átmeneti állapotok (**convergence érték**: mennyi időbe telik, amíg valamilyen változás teljesen átmegy)
- Új információ, vagy attribútum megváltozás értelemszerűen replikációt kezdeményez és a törlés is replikációt von maga után. Törlés működése: először törlésre jelöli (sírkő), ez lesz az új információ, amit replikál, ezután a valódi törlés a helyi adatbázis karbantartás során történik (alapból a sírkő 60 napig él))

Feltételezések:

- állandó nagy sávszélességű kapcsolat,
- annyi hálózati erőforrás van, amennyi csak kell.

Fentiek miatt mindig mindenki elér mindent.

Tulajdonságok

- Replikációs partnereket alakít ki a rendszer (köztük gyors replkiálás).
- A normál változásokra automatikusan 15 másodperc múlva küld értesítést a forrás („change notification”) (push-pull).
- Telephelyen belüli működés az a **Change Notification** alapján működik: ahol változás van az a tartomány vezérlő értesíti a többit, hogy változás van, azok visszajeleznek, ha szeretnék megkapni a változásokat majd ez elküldi a változásokat.
- Vannak sürgős változások (pl felhasználói letiltás) ezeket azonnal replikálja.
- Jelszóváltozatás "félig" sürgős, a PDC emulátorhoz azonnal eljut.
- Nem tömöríti a rendszer az adatokat replikáció során.
- Az információt kíséri egy verziószám, egy időbélyeg és a szerver globális azonosítója, ezekkel oldja fel a replkiációs konfliktusokat ("verzió szám versengés") pl:
    - **Attribute Conflict**: ugyanazt az attribútumot megváltoztatunk két különböző tartományi vezérlőn.
    - **Deleted container cofilct**: egy tárolóban elhelyezünk egy objektumot, miközben a tárolót már máshol törölték (ilyenkor a talált tárgyak közé rakja a felmásolt objektumot).
    - **Relative Distinguished Name Conflict**: két helyen ugyanolyan néven létrehoznak két objektumot (*adsiedit.mmc*).
- (kiegészítő optimalizálási jellemző 1.): a replikáció több útvonalon történik.
- (kiegészítő optimalizálási jellemző 2.): Az objektum Update Seqence Number attribútuma (az összes) változásra folyamatosan növekszik (ez egy globális számláló) és ezt is ellenőrzik a vezérlők (push-pull).
- **K**(nowledge)**C**(onsistency)**C**(hecker) feladata a replikációs topológia fenntartása:
    - legalább két replikácós partnert állít be minden Active Directory-s partícióra
    - egy irányú kapcsolat, max három lépés távolságra legyenek a vezérlők (így lehet számításokat végezni, hogy mi mennyi ideig tart).
    - automatikusan és dinamikusan kezeli a replikációs térképet (bármi változás van, az saját maga újra rajzolja a topológiát és ezt bejegyzi a konfiurációs partícióba, ez replikálódik, több KCC esetén azé, aki később rajzolta)
- A kapcsolati objektumok egy vagy több alkalmazás partíciót replikálhatnak.
- *Active Directory Sites And Services és az Active Directory Users And computers-en belül a Domain Controllerek tulajdonságai közt ott az NTDS settings*
- Kézzel létrehozott replikáció (nem szokás):
    - ha nem elég a 2-3 lépés,
    - ha a KCC beállítása nem megfelelő,
    - KCC hibája miatt nem tud létrejönni.
- Lehet erőszakosan is replikálni.

10. Active Directory replikáció telephelyek között

Multimasteres replikáció: minden tartományi vezérlő írható és olvasható és a változások automatikusan átvezetődnek a tartományvezérlők között.

Replikációs Tulajdonságok

- **Push** és **pull** típusú replikáció (a másod példány kéri le a változásokat, de van, hogy a forrás kezdeményez).
- **Store and forward** (több tartományon kell végig terjedni, akkor az több lépésben, nem egy helyről)
- Replikáció során lehetnek átmeneti állapotok (**convergence érték**: mennyi időbe telik, amíg valamilyen változás teljesen átmegy)
- Új információ, vagy attribútum megváltozás értelemszerűen replikációt kezdeményez és a törlés is replikációt von maga után. Törlés működése: először törlésre jelöli (sírkő), ez lesz az új információ, amit replikál, ezután a valódi törlés a helyi adatbázis karbantartás során történik (alapból a sírkő 60 napig él))

Feltételezések:

- nincs nagy sávszélesség,
- a kapcsolat nem is megbízható és korlátozottak az erőforrások.

Tulajdonságok

- időzített (minimum 15 perc két replikáció között) és nem automatikus
- tömöríti a forgalmat (1/10-ére az Microsoft szerint)
- A telephelyet IP alhálózattal kell definiálni, a telephelyeket site-linkkel kell összekapcsolni
- *Active Directory Sites And Services-ben lehet beállítan.*
- **SiteLink** definíciója: ez rögzíti, hogy milyen szabályokkal tud két telephely replikálni, a rendszergazdák ezeket a szabályokat adják meg. (Beállítások: milyen időzítéssel és milyen protokollt használjon, de hogy merre menjen, azt az IP beállításoknál kell megadni (mert nem mindegy, ha pl. van egy bérelt vonal, akkor ténylegesen azon megy-e az információ) ez a költség beállítása). Lehetőséges protokollok:
  - IP (RPC) alapértelmezetten, nem tűzfal barát, de szinkron
  - SMTP tűzfalbarát, de aszinkron
  - költségeket lehet beállítani => a legkisebb költségű sitelinket fogja majd használni a replikációkor
- **Inter Site Topogy Generator**: feladata a térkép kezelése, a **KCC** barátja, egy telephelyen belül egy darab van.
- Kellenek hídfő (**bridge-head**) szerverek, ezek a ki- illetve a bejáratok a telephelyről és ez alapértelmezetten nincs beállítva, és ilyennek mindig kell lennie!
- RODC-vel csak egy irányú a replikáció lehetséges természetesen.
- **Site Link Bridge**: több replikációs lépcsőt egyszerűsíti a rendszer, feltéve hogy van azonos replikációs időszak és a prorokoll is ugyanaz.
- **Univerzális csoporttagság cache**: A bejelentkezéskor a GC-ből lekérdezett információ gyorsítótárba helyezhető, ezzel meggyorsítható a bejelentkezés. Amikor először jelentkezik be a kliens, akkor a helyi vezérlő lekéri az információkat és beteszi a cache-be, majd ezt 8 óránként frissíti.

Telephelyek osztályozása

- Kicsi telephely: nincs szerver, csak nagy sávszélesség (nincs szerverüzemeltetés, védelem, stb.).
- Közepes: DC van, de GC nincsen, ekkor jó a cachelés (erdő szintű replikáció nincs).
- Nagy telephely: DC és GC is van (védelem is van és van erdőszintű replikáció).

11. Globális katalógus

Speciális tartományvezérlő. A globális katalógus olyan tartományvezérlő, amely tartalmazza az erdő összes Active Directory objektumának a másolatát. A globális katalógus a gazdatartomány objektumairól teljes másolatot, míg az erdőben lévő többi tartomány objektumairól csak részleges másolatot tartalmaz. A rendszer automatikusan az erdő első tartományvezérlőjén hozza létre a globális katalógust.

Használata

- **Objektumok keresése**

A globális katalógus segítségével a felhasználók az erdő összes tartományában kereshetik a címtáradatokat függetlenül attól, hol vannak azok tárolva. Egy erdőn belüli keresés maximális sebességgel és minimális hálózati forgalommal történik.

- **Egyszerű felhasználónév hitelesítése**

A globális katalógus végzi az egyszerű felhasználónevek (UPN) hozzárendelését, amikor a hitelesítő tartományvezérlő nem ismeri a fiókot. Vegyünk például egy felhasználót, akinek a fiókja a pelda1.microsoft.com tartományban található. Ha ez a felhasználó úgy dönt, hogy a felhasznalo1@pelda1.microsoft.com egyszerű felhasználónévvel jelentkezik be egy olyan számítógépre, ami a pelda2.microsoft.com tartományban van, akkor a pelda2.microsoft.com tartomány vezérlője nem fogja megtalálni a felhasználó fiókját. A tartományvezérlő ilyenkor a bejelentkezési folyamat végrehajtása érdekében felveszi a kapcsolatot a globális katalógussal. További tudnivalók Az Active Directory névtérben használt nevek című témakörben találhatók.

- **Univerzális csoporttagságadatok szolgáltatása több tartományból álló környezetben**

Univerzális (Universal group): a Windows 2000 tartományok újdonsága volt a szintén csak natív tartományi üzemmódban elérhető univerzális hatókörű csoport, melynek tagjai a tartományfa vagy az erdő bármely tartományában lévő csoportok és fiókok lehetnek és ezeknek az erdő szintén bármely tartományában adható is jogosultság.

Az egyes tartományokban tárolt globális csoporttagságtól eltérően az univerzális csoporttagság csak egy globális katalógusban tárolódik. Ha például egy univerzális csoporthoz tartozó felhasználó olyan tartományra jelentkezik be, amely natív Windows 2000 működési szintre vagy annál magasabb szintre van beállítva, akkor a globális katalógus szolgáltatja a felhasználói fiók számára az univerzális csoporttagság adatait a bejelentkezéskor. Ha a globális katalógus nem elérhető, amikor a felhasználó natív Windows 2000 vagy annál magasabb működési szintre beállított tartományra jelentkezik be, akkor a számítógép a gyorsítótárban elhelyezett hitelesítő adatokat használja a felhasználó bejelentkezésekor, amennyiben a felhasználó valamikor már bejelentkezett a tartományra. Ha a felhasználó még soha nem jelentkezett be a tartományra, akkor csak a helyi számítógépre tud bejelentkezni. Ha a felhasználó tartományi rendszergazdaként jelentkezik be (beépített rendszergazdai fiók), ezt akkor is mindig megteheti, ha a globális katalógus nem érhető el.

- **Erdőn belüli objektumhivatkozások az érvényesítése**

A tartományvezérlők arra használják a globális katalógust, hogy érvényesítsék az erdő más tartományaiban lévő objektumokra mutató hivatkozásokat. Ha a tartományvezérlő olyan attribútummal rendelkező címtárobjektumot tárol, amely más tartomány objektumára mutató hivatkozást tartalmaz, akkor a hivatkozást a globális katalógus segítségével érvényesíti a rendszer.

A globális katalógus be-, kikapcsolható funkció minden tartományvezérlőben. **Active Directory Sites and Servicesnél** az adott szervernél az **NTDS** beállításoknál lehet megadni**.** A globális katalógushoz nagyteljesítményű számítógép és jelentős háttértároló kapacitás szükséges. Csak olyan helyre tegyük, ahol meg tudjuk oldani a fizikai védelmet is.

Ajánlás: mindegyik DC legyen globális katalógus is, mert így mindegyik tárol minden fontos információt, replikációs probléma nem lesz. De több tartomány esetén nem ajánlott, mert a globális katalógus az Infrastrucure Masterrel nem mindig képes együtt működni.

12. Kitűntetett szerver szerepek

A Windows Server 2008 tartományvezérlői funkcióinak legnagyobb részét elosztottan valósították meg, ezek a funkciók az összes tartományvezérlőn elérhetők és használhatók. Ezek az un. műveleti kiszolgálók, vagy
Operation Masterek (Flexible Single Master Operation):
Erdő szintű szerepek:

- **Séma Master**: Központosítva végzi el a séma összes frissítését és módosítását. Amennyiben az erdő sémáját frissíteni kívánjuk, hozzáférési joggal kell rendelkeznünk a séma-főkiszolgálóhoz (Schema Admin). Egyszer csak egy van belőle.
- **Domain Naming Master**: csak és kizárólag ezen lehet bejegyezni a konfigurációs adatok közé új tartományt, illetve törölni. Szintén egy van belőle. Használatához Enterprise Admin jogok kellenek!

Tartomány szintű szerepek:

1. **Relative Identifier (RID) Master**: relatív azonosítókat kezel,mégpedig biztosítsa azt, hogy egyedi azonosítóval (SID, Security ID) rendelkezzen minden objektum az AD-ban; relatív azonosítókat 200-as csomagokban osztja. Ha elfogy, akkor kér új csomagot, ha ez nem elérhető akkor nem lehet új objektumot létrehozni, ha azon a tartományvezérlőn elfogyott az azonosító. Egy tartományon belül csak egy van.
2. **Infrastructure Master**: Ebből szintén egy lehet a tartományon belül, de csak akkor van rá szükség, ha a hálózat több tartományból áll. Feladata a saját tartományának objektumai és a többi tartományban található objektumok közötti hivatkozások frissítése.Ehhez kell Globális Katalógusra van szüksége. Infrastructure Master és Globális Katalógus ugyanazon a gépen nem futhat, mert akkor az infastructure master szolgáltatás nem fog megfelelően működni.
3. **PDC emulator** (**Primary Domain Controller Emulator)**:
   - Nem kerberos-os bejelentkeztetés. Például kevert üzemmódban (vannak NT-s gépek is) ez az NT-s gépek tartományvezérlője, elvégzi a bejelentkeztetést az NT-s obejktumokra, stb. innen jön a neve is.
   - időszinkronizálás (Kerberos alap autentikáció miatt), erdő gyökér tartományában lévő PDC emulátor kér egy külső időalapot, onnan szinkronizálva az időt, azt a PDC emulátorok egymás között az erdő tartományaiban szinkronizálják, majd minden egyes PDC emulátor a saját tartományán belül, az összes többi számítógépnek szolgáltatja ezt a központi időalapot, hogy szinkronban legyenek a számítógépek.
   - Jelszóváltoztatás – **félig sürgős replikáció** a rendszerben (azonnal értesíti a rendszer a PDC-t az új jelszóval. Ez azért kell, mert ha kilép a rendszerből és vissza akar menni (pl. másik tartományvezérlőn) akkor ennek a tartományvezérlőnek egy járulékos ellenőrzést kell végeznie a PDC emulátor segítségével. Ha tényleg megváltozott a jelszó => beengedi. PDC terhelés jelszófeltöréskor, jelszó elgépelés)
   - házirend szerkesztésekkel kapcsolatos konfliktusok elkerülése miatt, a PDC emulátor alapértelmezésben az a tartományvezérlő, amin a házirend szerkesztése történik, alapértelmezés szerint PDC-hez fordulnak a tartomány vezérlők. Ez alapkonfiguráció, de ez felülbírálható.
     KIESÉSE problémát okoz.

Az összes kitüntetett szerver alapértelmezésben saját területén belül az első tartomány vezérlőre kerül, tehát ez erdőnek az első tartományvezérlője (Sőt az GC is). Minden további tartomány első tartomány vezérlője PDC emulátor, infrastructure master, RID master is lesz.
Ha a schema master vagy a domain naming master kiesik, akkor, nem tudunk bizonyos műveleteket elvégezni, de üzemszerűen nem is akarunk nagyon gyakran schémát módosítani, ill. tartományokat felvenni és eltávolítani, tehát azokat helyre lehet állítani egy kis késéssel is. Infrastructure masternél is átmeneti kiesés őrült nagy problémát nem okoz. RID master esetén pedig nem okoz problémát, amíg ugye az azonosító csomagok kitartanak a többi tartomány vezérlőn és el tudjuk intézni az objektum létrehozásokat, ha elfogynak a RID masteren segíteni kell. A PDC emulátor folyamatos, észrevehető sőt hogy ha olyan a rendszer, akkor jelentős terhelést okozhat egy tartományvezérlőnek és **ezek a szolgáltatások állandóan szükségesek**, tehát ezeket folyamatosan biztosítani kell, praktikusan PDC emulátor meghibásodik, akkor azonnal be kell avatkozni:

- Szerver szerepek átvihetők, transzfer műveletek segítségével. Erre grafikusan az AD schémában, **AD Domains and Trusts eszközben** ill. **AD Users and Computers eszközben** vagy parancssorosan **ntdsutil.exe** segítségével.
- ki lehet nevezni olyan gépeket akik átveszik a szerepet szükség esetén. **cease** műveletnek hívják, csak parancssorosan lehet ntdsutil-al.

13. Active Directory adatbázis működése, üzemeltetés

Az Active Directory alapjául egy JET (Joint Engine Technology) adatbázismotort felhasználó ESE (Extensible Storage Engine) adatbázis számos új tulajdonsággal és képességgel kiegészített változata szolgál. Félig strukturált adatok kezelésére lett optimizálva az ESE. Félig strukturált adat: ugyan a schémában definiálva vannak, de nincsenek szigorúan táblák, azokon belül rekordokban definiálva, hanem változó lehet, hogy egy-egy rekordhoz jelen esetben egy-egy objektumhoz milyen paraméterek tartoznak.

WINDOWS/NTDS

- **Ntds.dit** – a legfontosabb fájl az ntds.dit, ami magát az Active Directory- adatbázist tárolja. A dit kiterjesztés a „directory information tree" kifejezésre utal.
- **Edb.log** – a fájlban a tranzakciónapló található, amelynek tartalma azonnal követi a címtár minden változását. A változások aztán később, a megfelelő pillanatban átkerülnek végleges helyükre, az ntds.dit-be. A fájl maximális mérete 10 MB.
- **Edbxxxxx.log** – ezek a fájlok akkor jönnek létre, ha az Edb.log túllépi az említett 10 MB-os mérethatárt. Ebben az esetben az aktív tranzakciónapló ebbe a fájlba költözik. A 10 MB méretkorlát természetesen ezekre az állományokra is érvényes.
- **Edb.chk** – a fájl a címtárba még be nem került adatok „helyzetének" jelzője.
- **EdbRes1.jrs és EdbRes2.Jrs** – tartalék naplók
- **Temp.edb** – a fájl, amint a nevéből is látszik, ideiglenes adatokat tárol a tranzakciókról. Átmenetileg ide kerülnek az ntds.dit tömörítése közben eltárolandó adatok is.

Az adatbázis kezelése az NTSDUTIL.EXE (vagy az ESENUTIL.EXE), segítségével helyreállíthatjuk, ellenőrizhetjük és töredezettség mentesíthetjük az adatbázist, biztonsági másolatot készíthetünk. 12 óránként megtörténik az AD **karbantartása automatikusan**: töredezettség csökkentése – de a mérete nem változik.

WINDOWS/SYSVOL

- A mappa tartalmazza azokat az elemeket (fájlokat), amelyek az Active Directory-szolgáltatásokhoz kapcsolódnak ugyan, de mégsem tárolhatók a címtáradatbázisban
- Tartalmazza a házirendeket (globális egyedi azonosítókkal 31 és a 6a a két alapvető házirend),.
- Tartalmazza a replikálandó fájlokat.

Ajánlás: a **bináris adatbázist nagy teljesítményű és hibatűrő adattárolón** kell tárolni. Valami raid5-ön (tükrözés és sebességgyorsítás, 4 merevlemez). **Naplóállományokat** nem feltétlenül nagy teljesítményű, de hibatűrő rendszerben érdemes tárolni mondjuk **raid1** (tükrözés, 2 merevlemez).

14. Active Directory biztonsági mentése

A biztonsági mentés, mint szerver képesség telepíthető. Régen Ntbackup segítségével történt a Server 2008 új technológiát vezetett be, most már a **WBAdmin.exe** programmal történik (de használható a powershell és a grafikus Windows Server BackUp is). Nem támogatja a szalagos meghajtókat, mentés DVD-re, külső winchester-re vagy hálózati meghajtóra készülhet. Csak helyi mentés készíthető, vhd fájlba.
Windows 2008 előtt az állapot információkat kellett menteni. A Windows Server 2008 rendszerben nem csak a rendszerállapot-adatokról kell biztonsági másolatot készítenie, hanem inkább a kritikus kötetekről. A kritikus kötetek azok a kötetek, amelyek az Active Directory tartományi szolgáltatások helyreállításához szükségesek. A kritikus kötetek között szerepelnie kell a következő adatokat tartalmazó köteteknek:

- A rendszerkötet: Ez a kötet tartalmazza a rendszerindításhoz szükséges fájlokat, amelyek a Bootmgr fájlt és a BCD-tárolót tartalmazzák.
- A rendszerindító kötet Ez az a kötet, amelyen a Windows operációs rendszer és a beállításjegyzék található.
- A SYSVOL könyvtárat tartalmazó mappa
- Az Active Directory-adatbázist tároló kötet (Ntds.dit)

Mentési lehetőségek WBAdmin-nal:

- **Normális** (új nevén Full): Minden fájlt ment, függetlenül az archív attribútum beállításaitól. Törli a fájl attribútumokat.
- i**nkrementális** (növekményes): A legutóbbi normál vagy növekményes mentés után megváltozott fájlokról. Törli a fájl attribútumokat.
- **differenciális** (különbségi): A legutóbbi normál mentés után megváltozott fájlokról. Ezt a Ws2008, mint lehetőség megszűntette. (De, ha már van egy full mentés, akkor már csak a változtatásokat menti el).
- **Custom:** csak a megadott kötetekről fájlokról készít mentést.

Teljes biztonsági mentést heti rendszerességgel ajánlott készíteni és naponta pedig növekményes vagy különbségi mentés ajánlott. A mentés online módon történik, nincs szükség újraindításra. Visszaállításra is a WBAdmin, használható illetve a Directory Services Restore Mode múdú indítás.
Helyreállítás típusai:

- **Tartományvezérlők teljes kiszolgálóra vonatkozó helyreállítása:** A teljes kiszolgáló helyreállítása a kiszolgáló összes kötetét helyreállítja. A helyreállítás ezen típusával állíthatók helyre a merevlemezek hibái vagy a fájlok sérülései az azonos hardverrel és operációs rendszerrel rendelkező számítógépeken. A teljes kiszolgáló helyreállítása újraformázza és újrapartícionálja a kiszolgálóhoz kapcsolódó összes merevlemezt. Ezt a műveletsort akkor használja, ha a helyreállítást új hardverre kívánja végezni, vagy ha a helyreállítás eddigi összes próbálkozása a meglévő hardverre sikertelen volt.
- **Elsődleges visszaállítás:** Ez a visszaállítási módszer használatos akkor, ha a visszaállítani kívánt kiszolgáló a replikált adatkészlet egyetlen futó kiszolgálója (replikált adatkészlet például a SYSVOL könyvtár és a fájlreplikációs szolgáltatás replikakészletei) Általában csak akkor van szükség elsődleges visszaállításra, ha a tartomány összes tartományvezérlője használhatatlan, és a tartományt a biztonsági másolatból kell helyreállítani.
- **Mérvadó helyreállítás:** A mérvadó másolat visszaállítása egy olyan módszer, amellyel az Active Directory tartományi szolgáltatásokból törölt objektumok és tárolók állíthatók helyre. A visszaállított adatok többi szerverre való replikálásához mérvadó visszaállítást kell használni.
- **Normál visszaállítás:** Ekkor az objektumok eredeti frissítési sorozatszámukat kapják meg. Az Active Directory replikálórendszer e szám alapján érzékeli és továbbítja az Active Directory változásait a szervezeten belüli kiszolgálók között. Ennek következtében a nem mérvadó visszaállítással visszaállított adatok régi adatként jelennek meg az Active Directory replikálórendszerben, és ezeket az adatokat a rendszer soha nem replikálja más kiszolgálókra. Ehelyett az Active Directory replikálórendszer a visszaállított adatokat frissíti a többi kiszolgálón tárolt esetleges újabb adatokkal.

15. Windows Server 2008 Read Only DC ismertetése

Csak olvasható tartományvezérlő.

Tulajdonságai

- sosem kezdeményez replikációt,
- mindig friss információkat tárol,
- lehetnek helyi felhasználók és helyi rendszergazdák,
- kliens szempontjából nincs különbség, hogy RODC vagy rendes DC kezeli,
- nem hordozhat kitűntetett szerver szerepkört,
- nem lehet replikációs bridgehead szerver (telephelyről kifelé és befelé menő replikációt végző szerver),
- csak WS2008 lehet RODC, korábbi operációs rendszerek nem támogatottak,
- elvileg lehet Server core is.

Jellemzői

- egy irányú replikáció (csak fogad, de nem küld replikációs adatokat),
- jelszó kivonatokat tárolhat (angolul Credential Caching), pl. helyi felhasználók gyorsabb bejelentkeztetésére,
- van helyi rendszergazda (csoport) (Administrative role separation) a RODC kezelésére,
- DNS szerverként is működhet, de a DNS adatokra is vonatkozik a csak olvashatóság,
- azt is be lehet állítani, hogy milyen attribútumok replikálódjanak a RODC-re, ez a sémában állítható be.

Használatának feltételei

- funkcionalitási szintnek minimum Windows Server 2003 (2000-es gép tartományvezérlőként nem működhet!)-nak kell lennie,
- WS2008-as tartomány vezérlőnek lennie kell a tartományon belül valahol,
- elő kell készíteni az Active Directory-t a RODC befogadására (ADprep programmal tehető meg régebbi tartományok előkészítése).

Telepítés

- Úgy, mint egy sima DC-t telepíteni, csak ki kell pipálni a megfelelő tulajdonságot,
- advanced esetén megkérdi, hogy milyen jelszavak legyen replikálva, de ezt utólag is be lehet állítani,
- core változaton replicatornewdomain=readonlyreplicavalue.

Egy speciális lehetőség telepítésnél: telepítés átadása olyasvalakinek, akinek nincs megfelelő joga (DC-ben be kell állítani)

Biztonsági funkciók RODC-ben

Jelszavak kivonatának replikálása (alapból kettőt tárol: saját gépének és a KRBTGT felhasználó (kerberos fiók felhasználó))