Az Active Directory, röviden AD a Microsoft egyes hálózati szolgáltatásainak gyűjtőneve, ezek:

- X.500 specifikációjú, LDAPv3 protokollal lekérdezhető címtárszolgáltatás,
- Kerberos5 protokoll alapú hitelesítés,
- DNS alapú névszolgáltatás (Windows 2000 előtti rendszerekhez WINS).

Mint látható, nyílt rendszereket használ.

Az LDAPv3

Az LDAP a Lightweight Directory Access Protocol rövidítése. Ez a protokoll directory szolgáltatások elérését szabályozza.

A directory szolgáltatás egy olyan speciális adatbázist takar, mely keresésre van optimalizálva, ennek megfelelően olyan esetekben célszerű ilyet használni, ahol kevés a módosítás, és nagy-számú, gyors lekérdezésekre van szükség.

Az információ egy faszerű szerkezetben tárolódik, és minden csúcsában bejegyzések (entry) szerepelnek. Egy bejegyzésnek van típusa, amely meghatározza, hogy milyen attribútumai lehetnek. Minden egyes ilyen bejegyzésre egyértelműen hivatkozhatunk a bejegyzés DN-jével (DistinguishedName), mely lényegében a fában a csúcshoz vezető utat írja le.

Például a MAGIK.HU tartomány HIDRAULIKA szervezeti egységében (Organizational Unit:OU) található HPLaserjet4 nevű nyomtatóobjektumnak a DN-je CN=HPLaserjet4,OU=HIDRAULIKA,DC=MAGIK,DC=HU, ahol CN a közönséges név (common name), DC a tartomány objektumosztály (domain class). A megkülönböztetett név természetesen négynél több részből is állhat. Az objektumnak lehet kanonikus neve (canonical name, röviden CN), ami lényegében a DN megfordítva, azonosítók nélkül és perjeleket használva: magik.hu/Hidraulika/HPLaserjet4. Valamennyi objektum rendelkezik globális egyedi azonosítóval (GUID) is, ami egy egyedi, az objektum élettartama során változatlan, 128 bites érték, amit az AD-n belüli keresés és replikáció során használnak. Egyes objektumoknak elsődleges felhasználóneve (User principal name, röviden UPN) is van, ez objektumnév@tartománynév formátumú.

A címtár

A címtár segít nyilvántartani és felügyelni azokat az objektumokat, amelyek egy meghatározott hálózatban vagy hálózatrészben előfordulhatnak. A címtár nyilvántartja a hálózat felhasználóit, számítógépeit, nyomtatóit és sok esetben a hálózatban levő számítógépek megosztott erőforrásait is.

Miért jó ez? Először is egyetlen helyen vannak felsorolva a hálózat felhasználói: nem kell ugyanazokat a felhasználókat felvenni az egyes számítógépek helyi felhasználó-adatbázisába. Másodszor, összefogott nyilvántartásban megjelennek a felhasználók és a számítógépek, ezáltal – ha a címtárszolgáltatás mellé a rendszergazda megfelelő eszközöket is kap – központi helyről, a címtár irányából felügyelhetők: ez többek között azt jelenti, hogy sok felügyeleti feladat elvégezhető anélkül, hogy a rendszergazdának ténylegesen oda kéne mennie a kérdéses felhasználóhoz vagy számítógéphez. Harmadszor, a címtárban megjelenhetnek a hálózatban megosztott erőforrások – megosztott könyvtárak, nyomtatók és esetleg kiszolgáló oldali alkalmazások szolgáltatási – is: ezáltal a felhasználóknak nem kell tudniuk, hogy az egyes erőforrások mely kiszolgálón érhetők el: elég, ha a címtárhoz hozzá tudnak férni, az pedig automatikusan átirányítja őket a kívánt erőforrást tartalmazó kiszolgálóhoz (sokszor anélkül, hogy a felhasználó tudomást szerezne az átirányításról).

Röviden összefoglalva: a címtárszolgáltatás lehetővé teszi a számítógépek központi felügyeletét és a nyilvántartások maximális központosítása révén csökkenti a hálózat üzemeltetésével járó költségeket; emellett lehetőséget ad az erőforrásokhoz való egységes hozzáférésre is. Mindezt persze csak akkor, ha a rendszergazda megfelelően kialakítja a címtárbeli adatstruktúrákat: feltölti a felhasználók és a számítógépek nyilvántartását, közzéteszi a szükséges erőforrásokat és beállít egyéb automatizmusokat is, mintpéldául a csoportházirend vagy a logon script.

Azt a hálózatot vagy hálózatrészt, amelyet egyetlen közös címtárral felügyelnek, tartománynak (domain) nevezzük. A tartományi címtár fizikai megjelenése a címtáradatbázis, amelyet a tartomány címtárkiszolgálói tárolnak, és ezek nyújtják a vele kapcsolatos szolgáltatásokat is. A címtárkiszolgálókat tartományvezérlőnek (domain controller) nevezzük. A címtáralapú hálózatban lévő számítógépeket – amelyek maguk is benne vannak a nyilvántartásban – a tartomány tagjainak (member) nevezzük. A tartomány címtárába felvett felhasználók pedig elvileg a tartomány valamennyi számítógépén jogosultak helyben bejelentkezni – vagy a számítógépek erőforrásaihoz hálózaton keresztül csatlakozni -, ha csak a hozzáférési jogok beállításával a rendszergazda el nem tiltja őket egyik vagy másik számítógéptől.

De mi történik, amikor a tartomány egy felhasználója leül egy tartománybeli számítógép elé és bejelentkezik rajta? A bejelentkezés során közli a felhasználó nevét és jelszavát, továbbá azt, hogy ő a tartományban nem pedig – nem pedig a számítógép helyi felhasználói-adatbázisában – van nyilvántartva.

Mivel pedig a felhasználó nem a helyi számítógép nyilvántartásában szerepel, az nem tudja önállóan elvégezni a hitelesítést. Ehelyett – a hálózaton keresztül – a legközelebbi címtárkiszolgálóhoz, tartományvezérlőhöz fordul, és attól kérdezi meg, hogy adott névvel és jelszóval szerepel-e felhasználó a címtárban. Ha igen, a tartományvezérlő visszaküldi a felhasználó biztonsági azonosítószámát (SID), illetve azon felhasználócsoportok azonosítóját, amelyeknek a felhasználó tagja. A hitelesítést tehát a tartományvezérlő végzi el: ezzel a hálózat teljes biztonsági rendszere egy

kézben tartható. Bár ha egy tartománybeli számítógépen például megosztunk egy könyvtárt, akkor az ahhoz tartozó hozzáférési jogokat ott, azon a számítógépen kell beállítani – igaz viszont, hogy ekkor adhatók hozzáférési jogok a tartomány felhasználóinak is, és az is igaz, hogy a megosztások kezelése és a hozzáférési jogok beállítása távolból, a tartomány tetszőleges más számítógépéről elvégezhető.

Ha a felhasználó sikeresen bejelentkezett, a címtárbeli jogaitól függően nemcsak a saját számítógépe – és egyes hálózati kiszolgálók – erőforrásaihoz, hanem a címtár adatbázisához is hozzáférhet, ott erőforrásokat kereshet, illetve megfelelő jogok birtokában a számítógépek és a felhasználók nyilvántartásába is beleláthat.

Egy tartomány címtárában a számítógépeket, a felhasználókat és az erőforrásokat szervezeti egységekbe (organizational unit, röviden:OU) lehet szervezni. Ezzel egyetlen tartományon belül tükrözni lehet a hálózatot üzemeltető intézmény szervezeti felépítését. Akár minden szervezeti egységnek saját rendszergazdája lehet, aki a felhasználókat és a csoportokat kezeli. Így a tartományi rendszergazda feladata megosztható.

Az Active Directory felépítése

Tartomány, fa, erdő, szervezeti egység

Az Active Directory által felügyelt hálózatok alapegysége a tartomány, hiszen ez az a hálózat vagy hálózatrész, amely egyetlen, közös címtáradatbázist használ. Azonban a címtárrendszer igény szerint a tartomány szintje alatt és fölött is tovább strukturálható. Így több tartomány nagyobb egységgé fogható össze anélkül, hogy címtáradatbázisaikat egyesíteni kellene. Az összekapcsolás alapja a tartományok közötti bizalmi kapcsolatok (trust), amelyek lehetővé teszik, hogy egy tartomány felhasználói igénybe vegyék egy másik tartomány erőforrásait és fordítva. A bizalmi kapcsolatok útján a tartományok először is fába (tree) szervezhetők: ez azt jelenti, hogy a tartományok között hierarchiát alakítunk ki, vagyis egyes tartományok más tartományok alá vannak rendelve. Egy tartomány hierarchiabeli helye pedig kiolvasható a tartomány nevéből: minden tartománynak strukturált neve van, amelyben azok a tartományok is fel vannak tüntetve, amelyeknek az adott tartomány alárendeltje.

Mint minden rendes fának, az Active Directory-tartományfának is van gyökere (root). Ez a gyökér nem más, mint a struktúra legfelsőszintű tartománya. A tartománystruktúra kialakításakor először ez kap nevet. A tartományok logikai elrendezéséhez hasonlóan azok elnevezési rendszere is hierarchikus. Kézenfekvő tehát, hogy az Active Directory a tartományok elnevezésére az internet DNS-rendszeréből ismert tartománynév-hierarchiát alkalmazza.

Például: legyen egy gyökértartomány neve **szak**. Ha ez a tartomány egy könyvkiadóé, akkor ott nyilván van szerkesztőség, illetve pénzügyi és kereskedelmi részleg. Tegyük fel, hogy mindhárom

részleg külön tartományt tart fenn, amelyek között azért van átjárás, mert a gyökértartomány segítségével fába szervezzük őket. Az új tartományok a **szak**gyökértartomány gyermekei és tartománynevük a következő:

- **szerkesztoseg.szak**
- **penzugy.szak**
- **kereskedelem.szak**

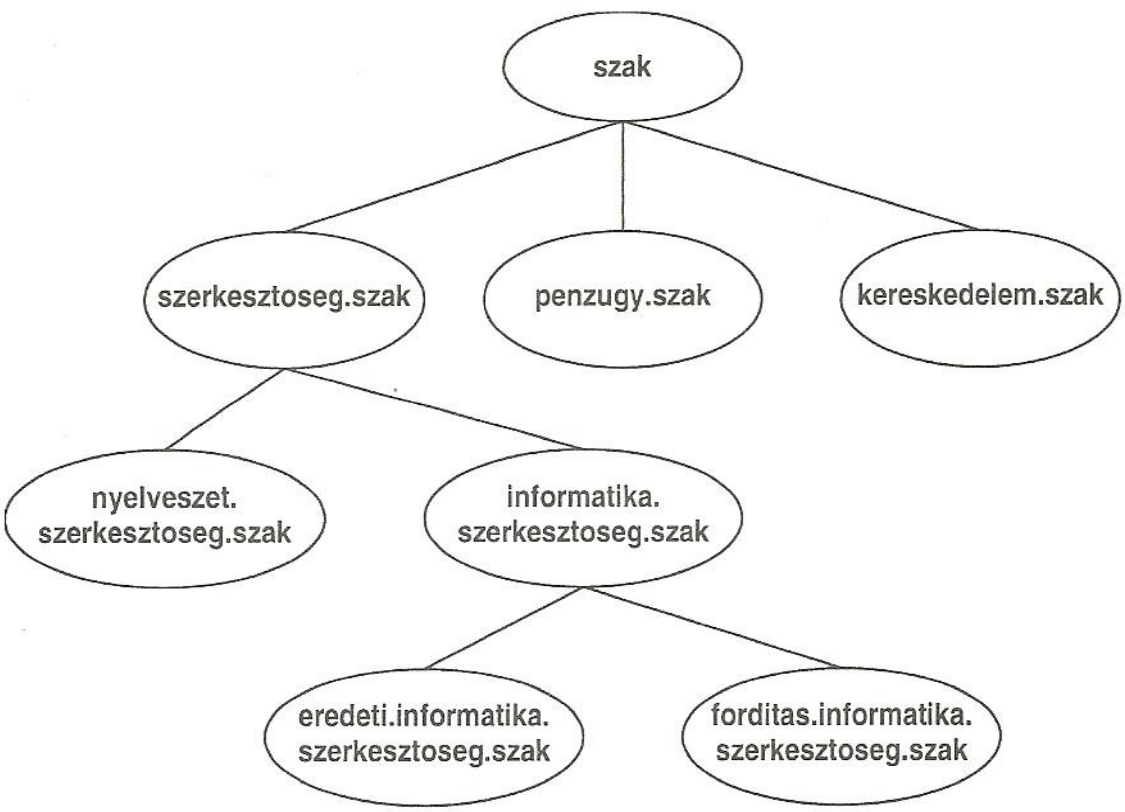
A szerkesztőség maga is két részlegre oszlik a könyvek témája szerint és mindkettőnek van saját tartománya. Ezek nevei:

- **informatika.szerkesztoseg.szak**
- **nyelveszet.szerkesztoseg.szak**

Az informatikai szerkesztőség kétféle könyvet ad ki: eredeti műveket és fordításokat. Ezért itt is két részleget hoztak létre, külön címtárral:

- **eredeti.informatika.szerkesztoseg.szak**
- **forditas.informatika.szerkesztoseg.szak**

Ezek után a tartományfa:



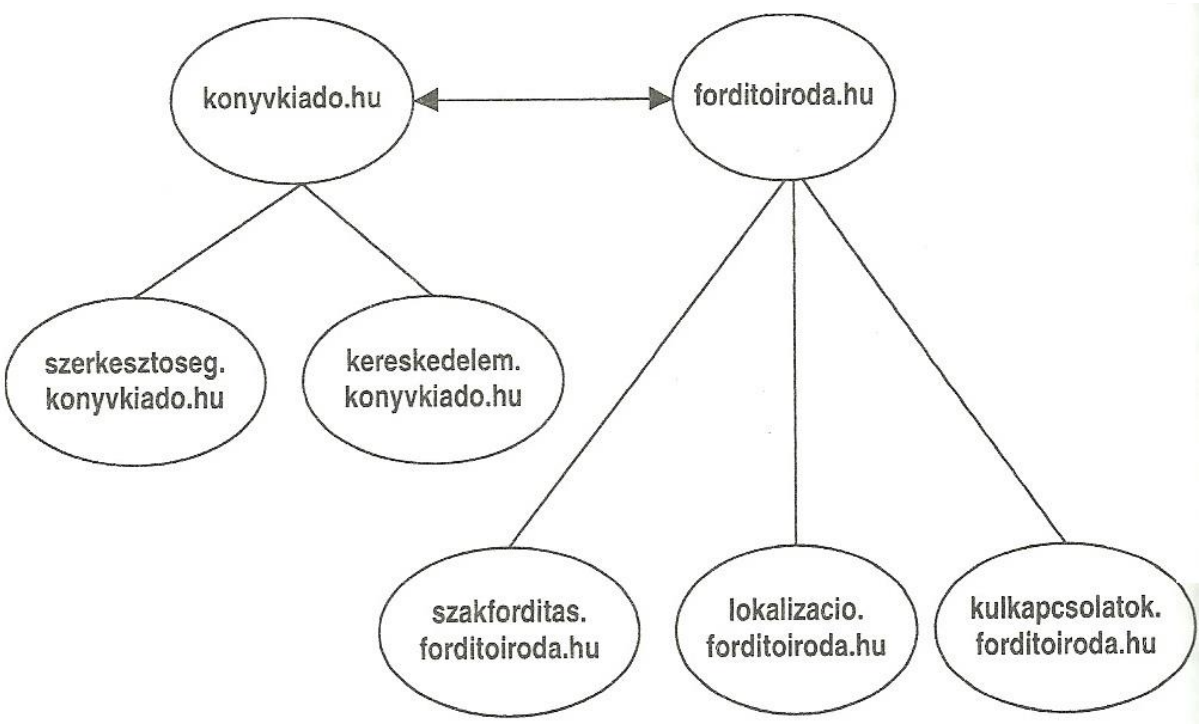
A rendszer egy kicsit túl van bonyolítva, mert a felhasználókat nem egy, hanem 8 különálló címtárban tartjuk nyilván. De látszik belőle, hogy az Active Directory ugyanolyan névhierarchiát

használ, mint az internet tartománynév-rendszere, így aztán az elnevezési rendszer megvalósítására is ugyanazt a névkiszolgáló szolgáltatást – a DNS-t – használja, mint az internet. Ebből következik, hogy az Active Directory címtár TCP/IP és DNS-kiszolgáló nélkül nem működhet. Az már más kérdés, hogy egy intézmény belső tartományhierarchiája – amely az elnevezési hierarchiában is megjelenik – illeszkedik-e az internet névhierarchiájába vagy sem. Az előbbi esetben – a példabeli tartomány neve ekkor lehetne például **szerkesztoseg.szak.hu**, a tartományok és a bennük lévő kiszolgálók elvileg látszanak az internet felől, az utóbbi esetben – a **szerkesztoseg.szak** – formájú nevek esetén - nem. (Ekkor érdemes a szerkesztoseg.szak.local formátumot használni.)

Az egy fába szervezett tartományok között szabad az átjárás. Bár a fára nem igaz, hogy egyetlen közös címtárt használna, a fa bármely tartományának felhasználói hozzáférhetnek a többi tartomány erőforrásaihoz. Például egy felhasználó, aki az **eredeti.informatika.szerkesztoseg.szak** tartomány címtárában van nyilvántartva, leülhet a **kereskedelem.szak** tartomány bármely számítógépe elé és bejelentkezhet. Közli felhasználónevét és jelszavát, valamint azt, hogy ő az **eredeti.informatika.szerkesztoseg.szak** tartomány tagja. A számítógép ezután kapcsolatba lép saját tartományvezérlőjével (a **kereskedelem.szak** tartományban), az pedig a hitelesítési kérést az **eredeti.informatika.szerkesztoseg.szak** tartomány tartományvezérlőjéhez továbbítja. Ha a felhasználót az **eredeti.informatika.szerkesztoseg.szak** tartományvezérlője igazolja, akkor hozzáférhet a **kereskedelem.szak** erőforrásaihoz, amennyiben a **kereskedelem.szak** tartomány rendszergazdája megfelelő hozzáférési jogokat adott neki.

Mivel minden tartománynak külön címtára van, mindegyiket külön rendszergazda felügyeli. De a tartományfa azért ennél jobban összefogja a tartományokat: bár a fában nincs közös címtár, viszont vannak közös nyilvántartások. Például van olyan rendszergazda, aki a fa minden tartományában rendszergazdai jogokkal bír, tehát tulajdonképpen felettese az egyes tartományok rendszergazdáinak. Ez a rendszergazda a gyökértartomány felhasználója.

Vannak olyan esetek, amikor úgy kell egy struktúrába szervezni Active Directory tartományokat, hogy nem lehet egy névhierarchiát létrehozni. Ez azt jelenti, hogy több gyökértartománynak kell lennie, mert nem minden tartomány legfelső szintű neve egyforma. Ebben az esetben tartományfákból erdő (forest) hozható létre. Egyesül például egy könyvkiadó és egy fordítóiroda:



Ebben a helyzetben mindkettő megtartja saját tartománynevét, mindkettő saját tartományfával rendelkezik. Ezek a fák összekapcsolhatók erdővé, amelynek bármely két tartománya között ugyanolyan az átjárás, mint egy fán belül. Csak éppen nem egy, hanem kettő vagy több elnevezési hierarchiát tart fenn. Ily módon a tartományok két szinten szervezhetők egységbe: a tartományokból fa, a fákból erdő alakítható ki.

Tehát elmondhatjuk, hogy az Active Directory-címtár legmagasabb szintje az erdő (forest), ami egy vagy több bizalmi kapcsolatokkal (trust) összekötött tartományt (domain) magába foglaló egy vagy több fa (tree) összessége.

Mint korábban szó volt róla, a példa kicsit túl van bonyolítva. Akkor is tükrözhetjük a szervezeti felépítést, ha csak egyetlen tartományt használunk. A tartomány címtáradatbázisában lévő objektumok – felhasználói és csoportfiókok, számítógépek, erőforrások – ugyanis szervezeti egységekbe (organizational unit: OU) csoportosíthatók. Minden tartományban tetszés szerint hozhatók létre szervezeti egységek, az egyes szervezeti egységeken belül pedig további szervezeti egységek. Így a tartományokban a szervezeti egységekből tetszőleges mélységű hierarchia alakítható ki.

A tartományban és a szervezeti egységekben alapvetően kétféle objektum lehet: fiók (account) és erőforrás (resource). A fiók a hálózat olyan szereplőjét képviseli aki, vagy amely hozzáfér erőforrásokhoz, így azokhoz hozzáférési jogokat kaphat. Fiókja felhasználónak, felhasználói csoportnak és számítógépnek van. Az erőforrás pedig olyan megosztott könyvtár vagy nyomtató, amelyet közzé tettek a címtárban.

Tartományvezérlők és telephelyek

A tartományokban a címtár központi nyilvántartás. Ez többek között azt jelenti, hogy kitüntetett számítógép tárolja, amelyet tartományvezérlőnek (domain controller) nevezünk. Egy tartományban több tartományvezérlő is lehet – sőt ajánlatos többnek lennie. Mindegyik tárolja ugyanannak a címtáradatbázisnak egy másolatát, és annak alapján címtárszolgáltatást nyújt. Ha a tartományban több tartományvezérlő van, a címtárszolgáltatás működőképes marad akkor is, ha egy tartományvezérlő meghibásodik.

Mivel a címtárszolgáltatás hálózati szolgáltatás, működése hálózati forgalommal jár: a felhasználók számítógépeinek kommunikálniuk kell a tartományvezérlőkkel, azoknak pedig egymással – leginkább avégett, hogy a címtáradatbázis valamennyi példánya egyforma legyen.

A felhasználók számítógépei és a tartományvezérlők közötti hálózati forgalom alapvetően kétféle:

- A felhasználók bejelentkeznek: ez hitelesítési forgalom a felhasználói számítógép és valamelyik – a hálózatban legközelebb lévő – tartományvezérlő között. Ez a forgalom „idényjellegű”: kötött munkaidővel működő intézményekben csúcsforgalom lehet a reggeli órákban.
- A felhasználók erőforrások adatait kérdezik le.

Amikor a címtáradatbázis megváltozik, például azért, mert a rendszergazda felvesz egy új felhasználót, a változás először csak az egyik tartományvezérlőn történik meg. De a változásnak el kell jutnia a többi tartományvezérlőhöz is. Az Active Directory tartományvezérlői automatikusan és összehangoltan gondoskodnak arról, hogy a címtáradatbázis egyforma legyen minden tartományvezérlőn. Ez az automatizmus a replikáció: minden tartományvezérlő rendszeresen ellenőrzi, hogy a nála lévő címtárpéldány megváltozott-e, és ha igen, jelzést küld a többi tartományvezérlőnek. Azok pedig átmásolják a változásokat a náluk lévő adatbázis-példányokba. Vagyis az Active Ditectory replikáció lekéréses (pull), nem pedig leküldéses (push) típusú. Ütközés esetén a későbbi változást tekinti érvényesnek.

A hálózati forgalom szempontjából fontos, hogy a tartománystruktúra – akár egy tartomány, akár fa, akár erdő – számítógépei (és tartományvezérlői) több, egymástól esetleg távol levőtelephelyre (site) is szét lehetnek szórva. A telephelyek rendszere pedig nem feltétlenül felel meg a tartományhierarchiának. Az Active Directory ezért nyilvántartja a telephelyeket. A telephely-nyilvántartás a teljes hálózati struktúra minden tartományában, minden tartományvezérlőjén rendelkezésre áll.

A telephelyek segítségével el lehet különíteni az alacsony (például WAN vagy VPN) és a magas sávszélességű kapcsolattal összekötött (LAN) helyszíneket. A helyek kialakítása független a tartományi és a szervezeti egység szerinti hierarchiától, és erdő-szinten egységes. A helyek szerepe a

replikáció hálózati forgalmának szabályozásában van, továbbá abban, hogy a felhasználók a hozzájuk lehető legközelebb eső tartományvezérlőre csatlakozzanak.

Az Active Directory adatbázisa

Az Active Directory adatbázisa, a Directory Information Tree (címtárinformációs fa, DIT) az alábbi három tárterületre vagy partícióra bomlik:

- Sémapartíció (schema partition): az egész erdő számára meghatározza az objektumosztályokat: az objektumok létrehozásának és módosításának a szabályait, az objektumok lehetséges tulajdonságait (attribútumait). Az erdő minden tartományvezérlőjére replikálódik, ezért ún. vállalati partíció (enterprise partition)
- Konfigurációs partíció (configuration partition): az egész erdő fizikai szerkezetét (például topológiáját) és beállításait határozza meg, beleértve a fákat, tartományokat, tartományi bizalmi kapcsolatokat és helyeket. Az erdő minden tartományvezérlőjére replikálódik, ezért ez is ún. vállalati partíció (enterprise partition)
- Tartományi partíció (domain partition): minden információt tárol az adott tartomány objektumairól (beleértve a szervezeti egységeket, csoportokat, felhasználókat stb.). Kizárólag az adott tartomány tartományvezérlőire replikálódik (illetve az erdő globális katalógusi – Global Catalog, GC – szerepkörű tartományvezérlőire is, részlegesen).

Műveleti főkiszolgálók

Az AD tartományvezérlői általában multi-master-replikációs modellben működnek, tehát a legtöbb műveletet bármelyik kiszolgálón el lehet végezni, mert replikáció útján automatikusan eljutnak a változások a többi, egyenrangú tartományvezérlőre. Van azonban néhány olyan feladatkör, ahol ez másként van: például a séma csak a Schema Master-en módosítható. Ezek az úgynevezett FSMO szerepkörök (ejtsd: kb. „fizzmó”), FSMO=„FlexibleSingle Master Operations” ~ „Mozgó egyedüli főkiszolgálóval végzett műveleti szerepek”, vagy szokásosan csak műveleti főkiszolgáló-szerepek kizárólag 1-1 kitüntetett tartományvezérlőn fordulhatnak elő, a következőképpen:

Szerep neve	Hatásköre	Leírása
Schema Master Séma-főkiszolgáló	Erdőnként 1	A séma minden frissítését és módosítását ellenőrzi. Ha nem elérhető, nem lehet sémát bővíteni/frissíteni.
Domain Naming Master Tartománynév-kiosztási főkiszolgáló	Erdőnként 1	Tartományok erdőhöz való hozzáadását/erdőből való eltávolítását ellenőrzi. Ha nem elérhető, a tartományfákkal kapcsolatos változtatások nem hajthatók végre.

PDC Emulator PDC-emulátor	Tartományonként 1	Visszamenőleges kompatibilitást nyújt az NT4 kliensek számára
RID Master RID-főkiszolgáló	Tartományonként 1	Valamely tartományvezérlő kérésére kiosztja egy új objektum részére a relatív azonosító (RelativeIDentifier) részt a biztonsági azonosítóból (SID). Ez a művelet az új objektum létrejöttekor zajlik. A relatív azonosító egy tartományon belül egyértelműen azonosítja az objektumot. Ha nem elérhető, nem lehet a tartományban új objektumokat létrehozni. Véd, nehogy 2 objektumnak egyforma SID-je legyen.
Infrastructure Master Infrastruktúra-főkiszolgáló	Tartományonként 1	A saját tartományába tartozó objektumok más tartományokba tartozó objektumokra való hivatkozásainak frissítéseit végzi (jellemzően a tartományközi csoporttagság-változásokat szinkronizálja). Ha nem elérhető, a többi tartománnyal való kapcsolattartás során frissítési problémák lépnek fel. Felelős a tartományi kereszthivatkozások megfelelő működéséért. Több tartományvezérlős környezetben az IM nem lehet Global Catalog (GC) szerver is egyben, mivel ebben az esetben a kiszolgáló nem tudja, hogy melyek az általa nem tárolt objektumokra mutató hivatkozások, hiszen a GC szerveren az erdő összes objektumáról van részleges replika. A domain-közi kereszthivatkozások frissítése ilyenkor hibaüzenettel leáll. Amennyiben viszont minden egyes DC egyben GC is, úgy már nincs jelentősége, hogy ki hordozza ezt a szerepkört.

Bizalmi kapcsolatok (trusts)

Mint már szó volt róla, a tartományok közötti kommunikáció bizalmi kapcsolatokon keresztül történik. Ez egy olyan hitelesítési csatorna, amely lehetővé teszi a tartományi felhasználók számára egy másik tartomány erőforrásainak elérését.

Fajtái:

- Egyirányú bizalmi kapcsolat (One way trust) – az egyik tartomány felhasználói hozzáférhetnek a másik tartomány erőforrásaihoz, de a másik tartomány felhasználóinak nem enged hozzáférést az elsőhöz
- Kétirányú bizalmi kapcsolat (Two way trust) – két tartomány felhasználói hozzáférnek egymás erőforrásaihoz

- Tranzitív bizalmi kapcsolat (Transitive trust) – olyan bizalmi kapcsolat, ami a résztvevő két tartományon túl is kiterjeszthető
- Nem tranzitív bizalmi kapcsolat (Intransitive trust) – olyan bizalmi kapcsolat, aminek a hatálya csak a résztvevő két tartományra terjed ki
- Explicit bizalmi kapcsolat (Explicit trust) – a rendszergazda által létrehozott bizalmi kapcsolat.
- Közvetlen bizalmi kapcsolat (Cross link/shortcut trust) – két külön tartományfában lévő tartományok, vagy egy tartományfán belüli, de szülő-gyermek viszonyban nem álló tartományok között létrehozott explicit bizalmi kapcsolat.

A csoportházirend

Ez a címtár legerősebb eszköze a központi felügyelethez: megoldható a felhasználók, a számítógépek és a felhasználói munkakörnyezetek viselkedésének és jogosultságainak szabályozása. A csoportházirend (Group Policy) Active Directory környezetben lehetővé teszi az operációs rendszerek, alkalmazások és a felhasználók beállításainak központosított konfigurálását és menedzselését.A csoportházirend alapvetően azokra a szervezeti egységekre (OU), telephelyekre (site) vagy tartományokra vonatkozik, amikhez hozzárendelik.

A Kerberos

Feladata a felhasználók hitelesítése a hálózati szolgáltatások eléréséhez, annak biztosítása, hogy a hitelesítési kommunikáció során az adatok titkosítva haladjanak át a hálózaton, valamint harmadik személy ne tudja elolvasni vagy módosítani őket.
Létrehozásakor a legfontosabb feltétel az volt, hogy a jelszó nem jelenhet meg a hálózaton!

Felhasználói adatok titkosítása:

A felhasználói fiókok és jelszavak a KDC-ben (Key Distribution Center - Kulcskiosztó központ) tárolódnak.Ez a tartományvezérlőkön az Active Directory-ban kapott helyet. A KDC-ben a felhasználói jelszavak titkosítva vannak MD4 hash algoritmussal. (Nem a jelszavak vannak tárolva, hanem csak a lenyomatuk.) Amikor a felhasználó bejelentkezéskor közli a felhasználónevét és jelszavát, a számítógép a beírt jelszónak elkészíti a lenyomatát. Ez egy 128 bites érték. Ezzel, mint kulccsal titkosítjuk az időbélyeget (timestamp, a számítógép belső órája) 3DES, AES128 vagy RC4 algoritmussal, valamint a sértetlenség biztosítására létrehoz egy HMAC kivonatot (MD5). Ezt a kódolt információt, a felhasználónevet és a kivonatot küldi el a számítógép a KDC-nek. Szintén ezzel a kulccsal titkosítjuk valamelyik kódolással az egész jegymegadási folyamatot. Mivel a KDC-ben szintén meg van a felhasználó neve és jelszavának MD4 lenyomata, a megkapott kódolt azonosítót (idő), dekódolni tudja. Ha ez megegyezik az Active Directory-ban tárolt felhasználónévvel és az idő is a csoportházirendben beállított tűréshatáron belül van, elkezdődik a jegymegadási folyamat.

A Kerberos jegyrendszer:

- A felhasználó megadja felhasználó nevét és jelszavát a KDC-nek (ez történhet egy bejelentkező dialógus ablakkal vagy smart kártyával is)
- A KDC lekéri a felhasználó SID-jeit a felhasználó tartományvezérlőjétől, valamint megnézi (ha van) a globális katalógus (GC) kiszolgálót is, van-e a felhasználónak magasabb szintű SID-je
- A KDC ezekből az összegyűjtött SID-ekből listát készít, ez a TGT (Ticket Granting Ticket - jegymegadási jegy) és ezt a TGT-t elküldi a felhasználónak (Egy TGT maximum 1024 SID-et tartalmazhat)
- Ezzel a TGT-vel kéri a felhasználó a TGS-t (Ticket Granting Service - jegymegadási szolgáltatás), biztosítsa számára a hozzáféréseket
- A TGS kiad az ügyfélnek egy szolgáltatásjegyet (Access Token).
- A hálózati szolgáltatások eléréséhez az ügyfél ezt a szolgáltatás jegyet fogja bemutatni. Ezt nevezik kölcsönös hitelesítésnek, mert a jegy hitelesíti az ügyfelet a szolgáltatásnak, a szolgáltatás pedig hitelesíti magát az ügyfélnek.

A jegymegadási jegy valamint a szolgáltatásjegy maximális élettartamát valamint megújításának maximális élettartamát a rendszergazda felügyeli a csoportházirendben.

A Domain Name System (DNS)

A Domain Name System, azaz a tartománynév-rendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A résztvevő objektumok számára kiosztott tartomány nevekhez különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető IP címekre „fordítja le”, „oldja fel”, melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton.

A DNS segítségével az Active Directory tartományhierarchiát akár teljes internetkörben is definiálhatjuk, vagy maradhat különálló, magánjellegű (local).

Amikor egy ilyen típusú tartományban számítógépes erőforrásokra hivatkozunk, a teljes minősített állomásnevet használjuk: pl.**kliensgep.szerkesztoseg.szak.hu**. Itt **kliensgep** jelöli az adott számítógép nevét, a **szerkesztoseg.szak** a szervezeti tartományokat, és a **hu** a legfelsőbb szintű tartományt. A legfelsőbb szintű tartományok képezik a DNS-hierarchia gyökerét (root). Az ilyen tartományok szervezhetők akár földrajzi alapon, kétbetűs országkódokat alkalmazva (pl. HU, mint Magyarország), szervezeti típusonként (pl.com, mint kereskedelmi szervezetek), vagy akár funkciójuk alapján (pl. shop az online üzletek esetében). A normál tartományokat, mint pl. **szak.hu**, szülőtartományoknak is

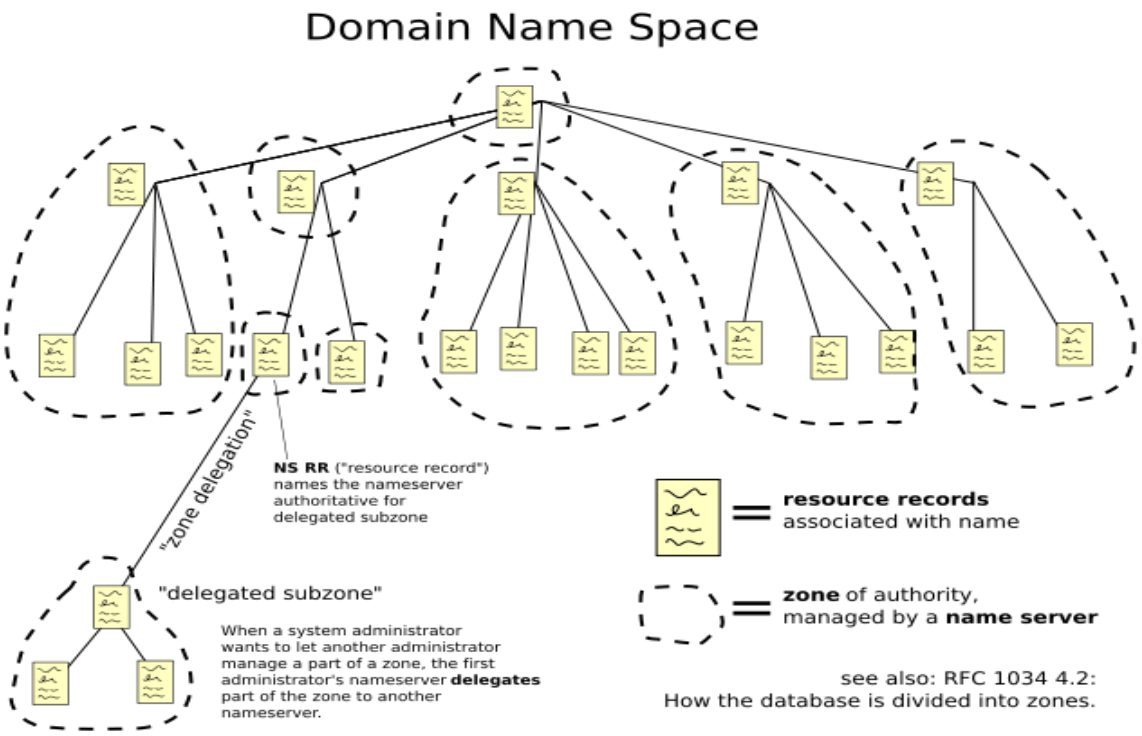
nevezik. A nevüket onnan kapták, hogy ők egy szervezeti struktúra szülei. A szülőtartományok további altartományokra vagy gyermek-tartományokra oszthatók, amelyek különböző hivatalokat, részlegeket vagy földrajzi helyeket jelölhetnek.

A DNS 3 fő részből áll:

- Tartománynévtér
- Névszerver
- Resolver

A tartománynévtér

A DNS fordított fastruktúrájú hierarchiáját egymásba ágyazott tartományok alkotják, melyek szintjeit ponttal választják el egymástól, fontosságuk pedig jobbról balra haladva egyre csökkenő. (pl. eredeti.informatika.szerkesztoseg.szak.hu)A fa minden csomópontjához nulla vagy több, a hozzá tartozó tartomány információit tároló erőforrásrekord (resource record) tartozik. A fa adminisztratív egységekre, zónákra (zone) van osztva, a gyökérzónától kezdődően. Egy-egy DNS-zóna a fa összefüggő, önálló egységként kezelt része, állhat egyetlen tartományból vagy tartozhat alá számos tartomány és altartomány, a rendszergazda által kiosztott adminisztrációs jogoktól függően. Egy zóna kezelője (földrajzi, topológiai vagy strukturális okokból) tovább delegálhatja a hozzá tartozó zóna egy része fölötti adminisztrációs jogát más feleknek. Ilyenkor a delegálással lényegében korlátozásmentes autonómiát ad át a felügyelt névtér fölött.



A névszerver

Névszervernek (name server) egyrészt azokat a programokat nevezzük, amelyek a domainnév-tartományhoz irányuló kérdésekre válaszolnak. Gyakorlatilag azokat a számítógépeket értjük, amelyeken ezek a programok futnak. Van egy megkülönböztetés: van autoritatív és nem autoritatív névszerver.

Az autoritatív névszerver egy adott zóna felelőse. Az adott zónával kapcsolatban tárolt adatai emiatt tehát biztonságosnak tekinthetők. Minden zónához legalább egy autoritatív névszerver tartozik, az elsődleges névszerver (primaryname server). Ez található meg a zónafájl SOA erőforrás rekord-jában (resource record). Adatbiztonság és terheléselosztás miatt az autoritatív névszerverek általában mindig szerverklaszterekből épülnek fel, ezeknél egy vagy több másodlagos névszerver (secondaryname server) ugyanazt a zónafájlt tartalmazza. Az elsődleges névszerver és a másodlagos névszerverek közötti adatszinkronizálás ún. Zonetransfer-rel valósul meg.

A nem autoritatív névszerver a zónákra vonatkozó adatait másod- vagy harmadkézből (a forrásból) kapja, így az ebben tárolt információt nem biztonságosnak tekintjük. Mivel a DNS-adatok elvileg nagyon ritkán változnak, a nem autoritatív névszerver a Resolver-től kért adatokat a lokális memóriába(RAM) menti, hogy ezt egy újabb kérdésnél gyorsabban tudja válaszként kiadni. Ennek a technikának a neve DNS-gyorstárazás (DNS caching). Minden bejegyzésnek van egy elavulási ideje (Time-to-Live, TTL), amely idő után törlődik a gyorstárból (cache-ből). A TTL időbejegyzés valamelyik autoritatív névszervertől érkezik, értékét az adatok változási valószínűségének függvényében határozzák meg (a gyakran változó DNS-adatok alacsony TTL értéket kapnak). Ez azt is jelenti, hogy egy adott névszerver ebben az elavulási időben rossz információt adhat, ha az adatok pont ekkor változtak meg.

A resolver

A resolver egy egyszerű felépítésű, a DNS rendszerbe tartozó számítógépre telepített szoftvermodul, amely le tudja kérdezni az adatokat a névszerverektől. A resolver valójában egy csatolófelület a program és a névszerver között. A resolver elintézi a program kérdését, s ha szükséges, kiegészíti azt FullyQualified Domain Name-mé (FQDN), majd elküldi a fix névszerverhez. A resolver iteratív vagy rekurzív üzemmódban működhet.

Rekurzív (önmagát meghívó) üzemmódban a resolver rekurzív kérdést küld a hozzá rendelt névszerverhez. Ha annak nincs meg a szükséges adat a saját adatbázisában, akkor további névszerverekkel veszi fel a kapcsolatot mindaddig, amíg pozitív vagy negatív választ nem kap egy autoritatív névszervertől. A rekurzív üzemmódban dolgozó resolver a munkát teljes egészében átadja a névszervereknek.

Iteratív (ismétlő) lekérdezési üzemmódban a resolver vagy megkapja a kívánt információt (resourcerecord), vagy egy linket kap a következő névszerverhez, és azt kérdezi le. Így a resolver lépésről lépésre haladva annyi kérdést tesz fel az adott névszervereknek, amennyi az információ beszerzéséhez szükséges.

A resolver az így kapott választ átadja a programnak, amely az információt kérte, például a böngészőnek. A közönséges felhasználói resolverek csak rekurzívan működnek, ezeket stub-resolvernek nevezzük. A névszervereknek általában saját resolverük van, ezek iteratívan dolgoznak.