Windows rendszeradminisztráció és Microsoft szerveralkalmazások támogatása

6. óra

Kocsis Gergely,
Supák Zoltán

2016.04.06.

Active Directory DS objektumok

Active Directory

Az AD DS fizikai és logikai komponenseket is tartalmaz

Logikai	**Fizikai**
Séma	Domain vezérlő (DC)
Partíció	Data Store
Domain	Global Catalog Server
Tree	RODC
Forest	
Site	
Container	
OU	

Active Directory

Az AD DS fizikai és logikai komponenseket is tartalmaz

Domain vezérlő: Tartalmazza az AD DS adatbázis egy másolatát. A legtöbb művelet bármely DC-n végrehajtható és az összes többire replikálódik (lásd FSMO szerepkörök).

Data store: Minden DC-n található egy Data Store. Ez tartalmazza a tényleges adatbázist (ntds.dit + log fájlok – C\Windows\NTDS).

Global Catalog Server: Olyan DC, mely a global catalog-ot tartalmazza. A global catalog a forest objektumainak egy részleges csak olvasható másolata, mely felgyorsítja a keresést különböző DC-ken tárolt adatok között.

RODC: Az AD DS csak olvasható másolata. Tipikusan kevéssé biztonságos környezetben használatos.

Active Directory

Az AD DS objektumok kezelése a következő eszközök segítségével történhet:

- AD Administration „snap-in”-ek
  - AD Users and Computers
  - AD Sites and Services
  - AD Domains and Trusts
  - AD Schema
- AD Administrative Center
- AD PoweShell modul
- Directory Service

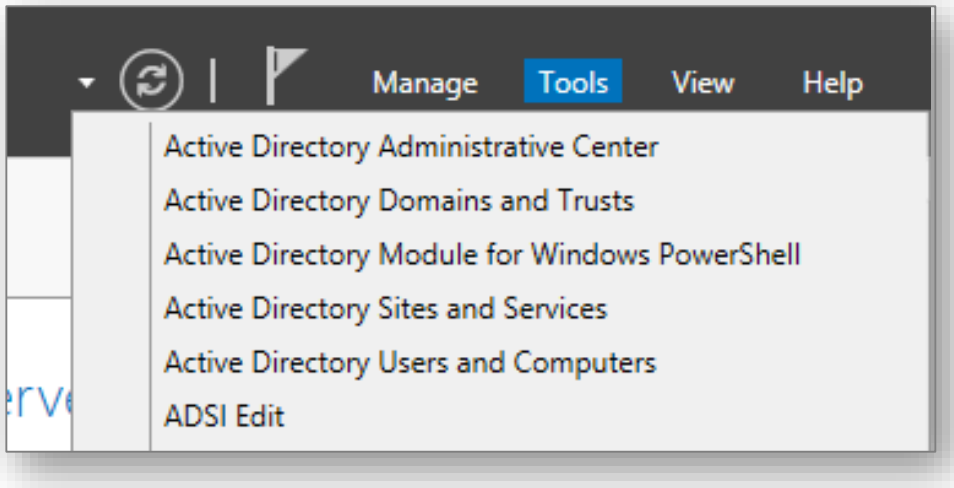
AD Administration „snap-in”-ek

AD Users and Computers: A leggyakrabban használt snap-in mindennapi feladatok elvégzésére (pl. felhasználók, csoportok, számítógépek ésOU-k kezelése)

AD Sites and Services: Replikáció és hálózatkezelés

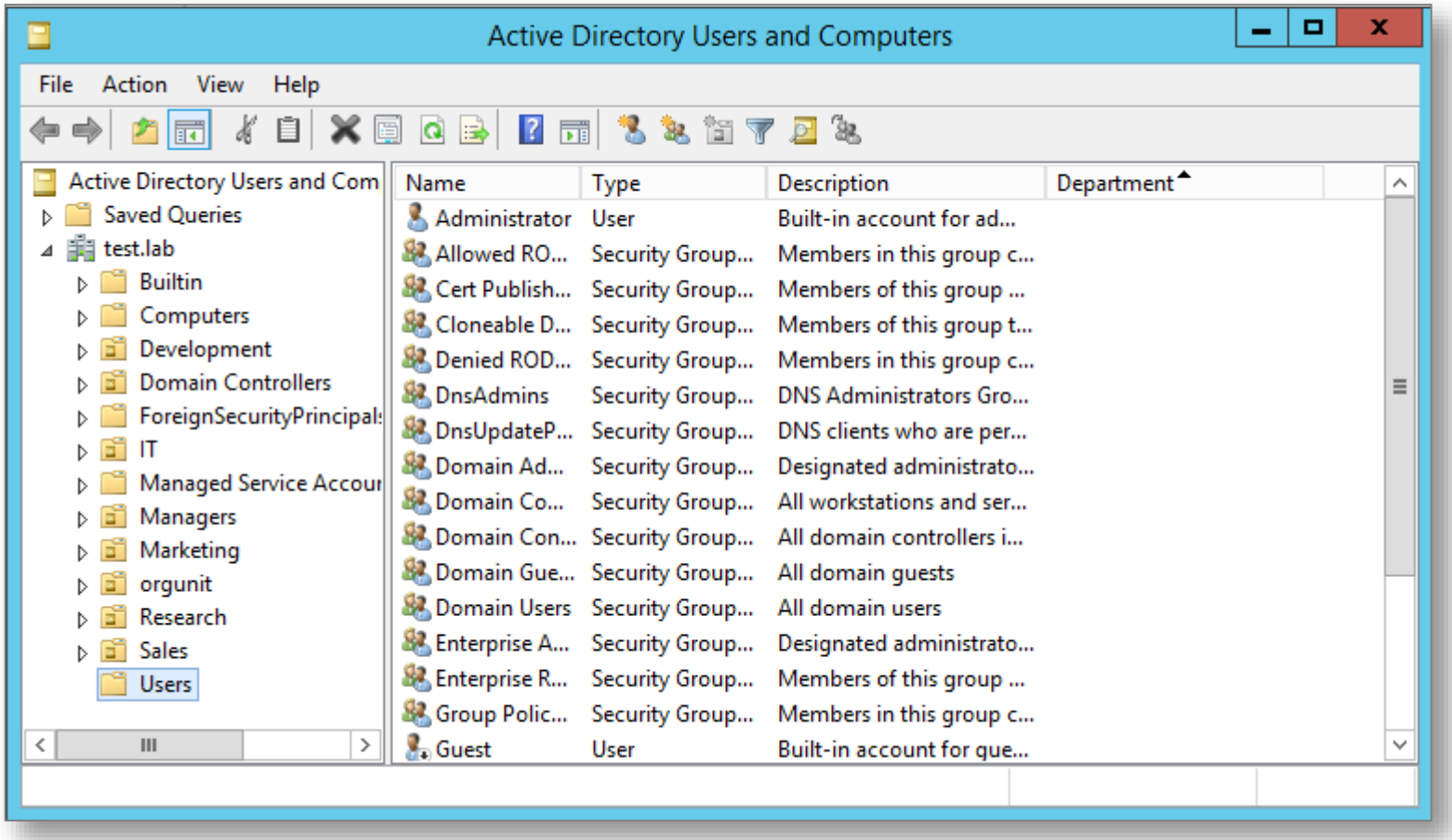
AD Domains and Trusts: Bizalmi kapcsolatok (trust) és forest kezelése

AD Schema: A séma ellenőrzése és módosítása. Ez a legritkábban használt snap-in a négy közül. Alapesetben nem is regisztrált (azaz használat előtt a `regsvr32 schmmgmt.dll` parancs kiadásával regisztrálni kell.



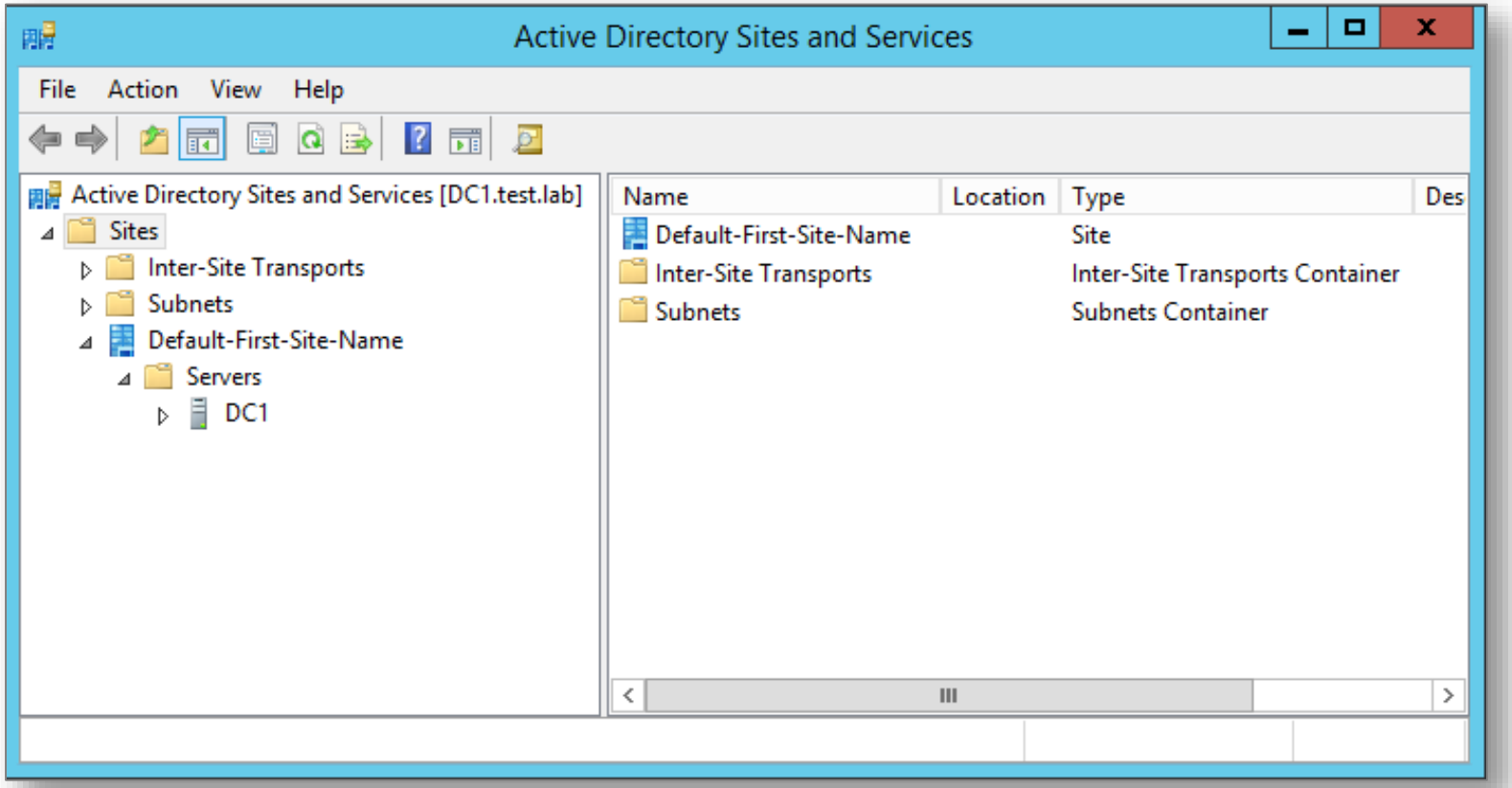
AD Administration „snap-in”-ek

AD Users and Computers



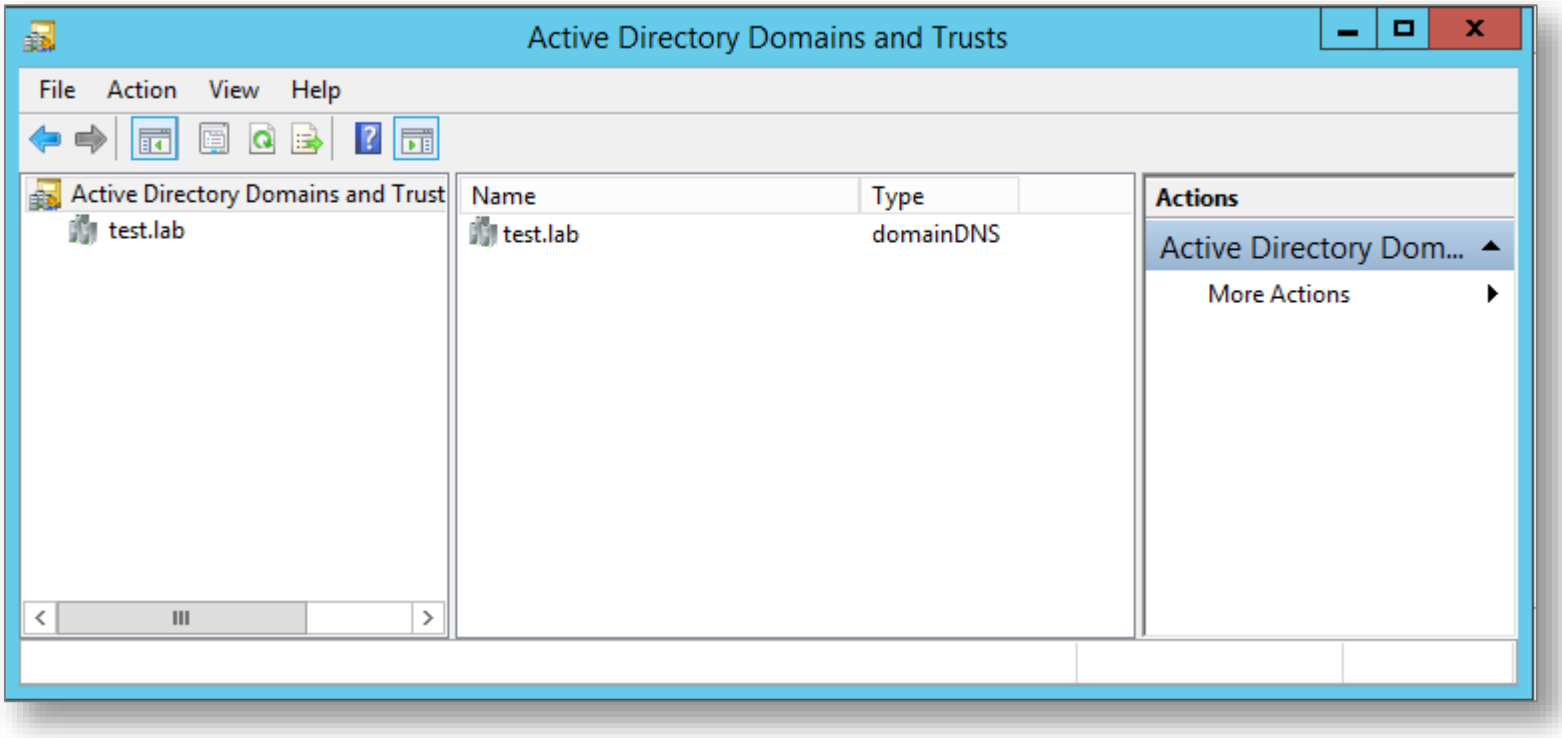
AD Administration „snap-in”-ek

AD Sites and Services



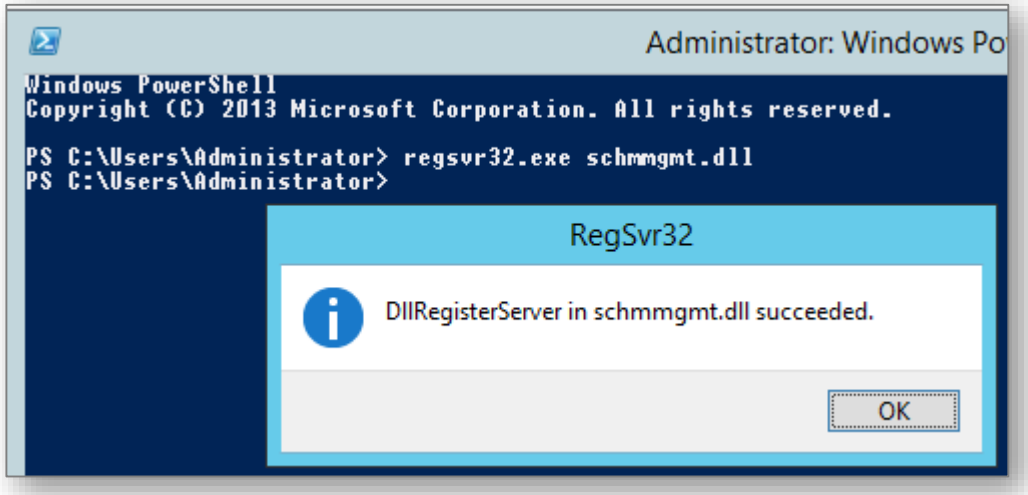
AD Administration „snap-in”-ek

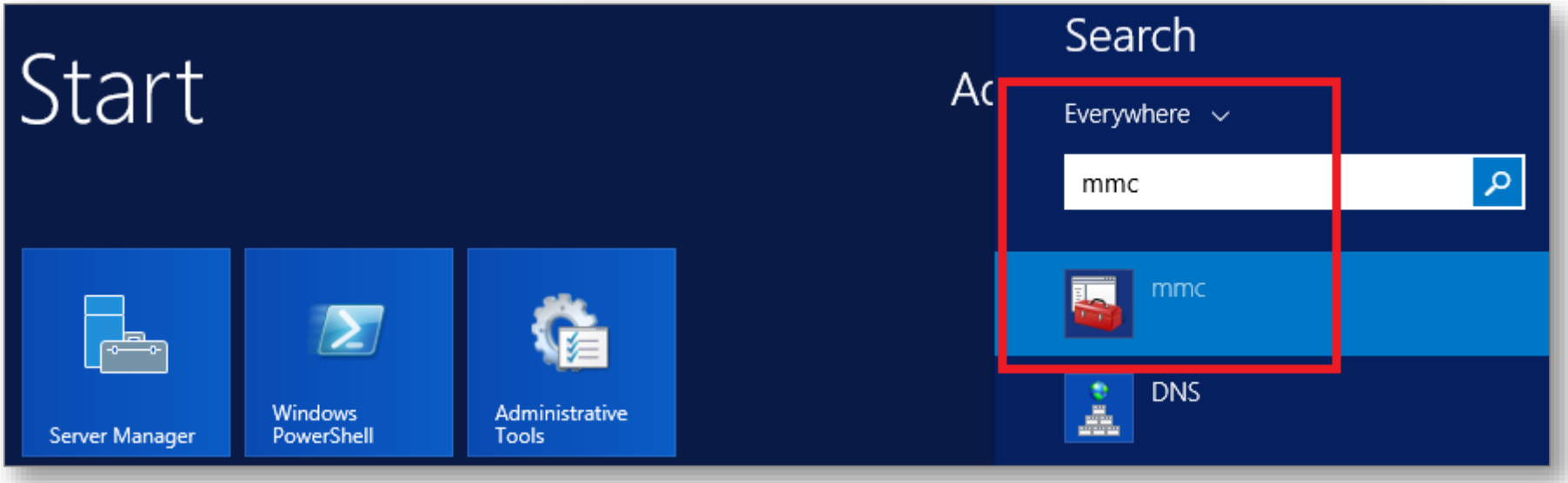
AD Domains and Trusts



AD Administration „snap-in”-ek

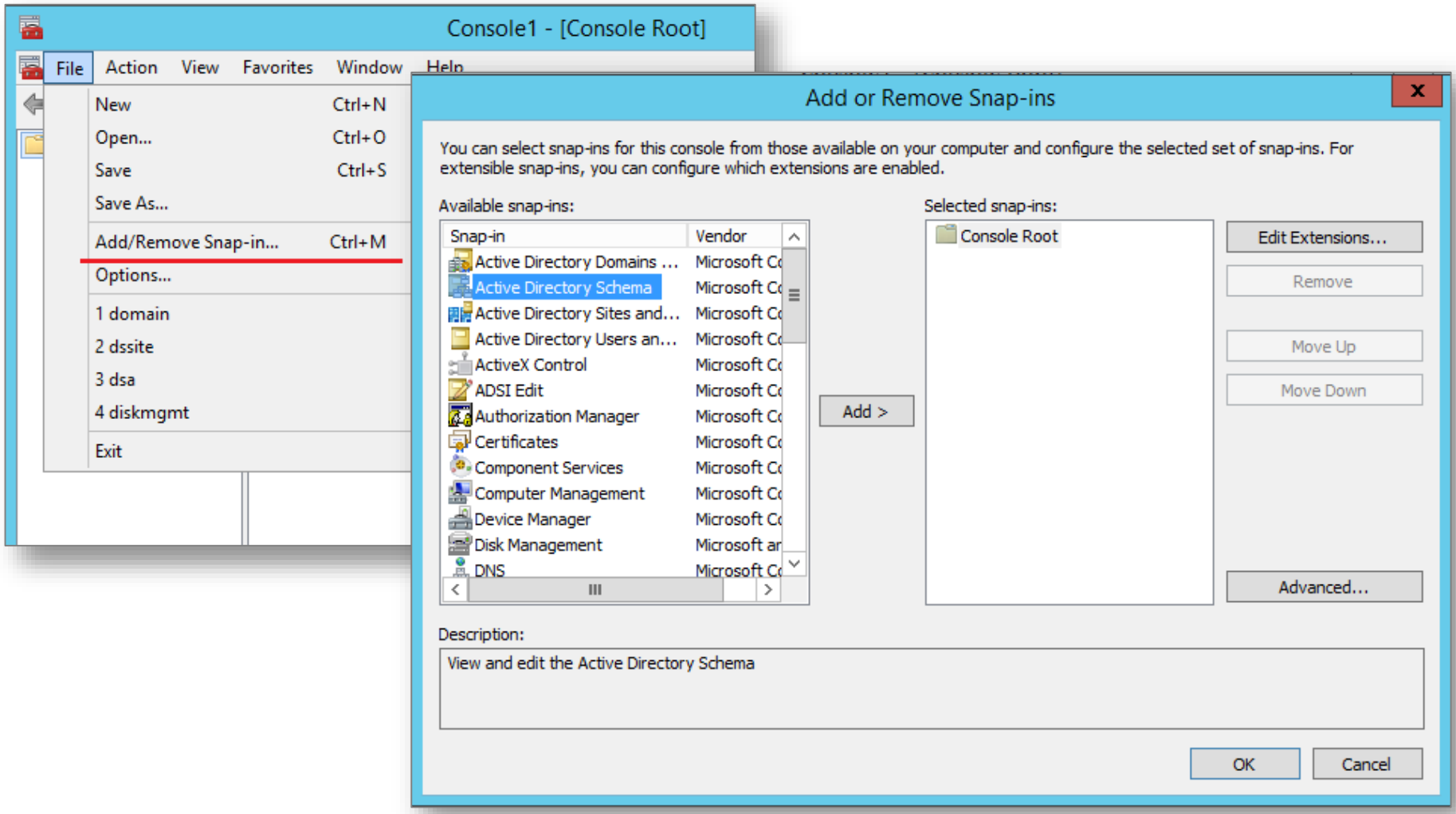
AD Schema





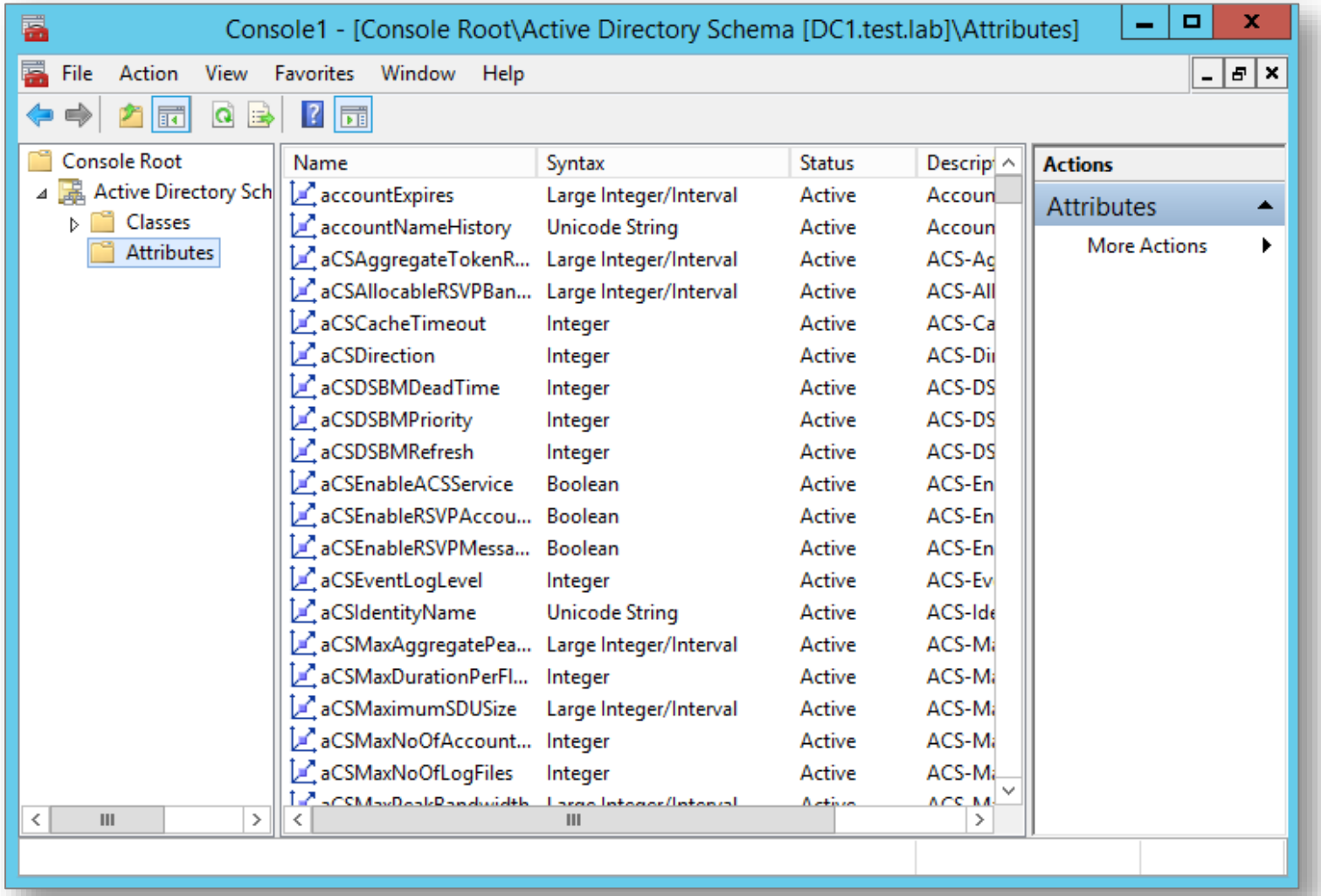
AD Administration „snap-in”-ek

AD Schema



AD Administration „snap-in”-ek

AD Schema



AD Administrative center

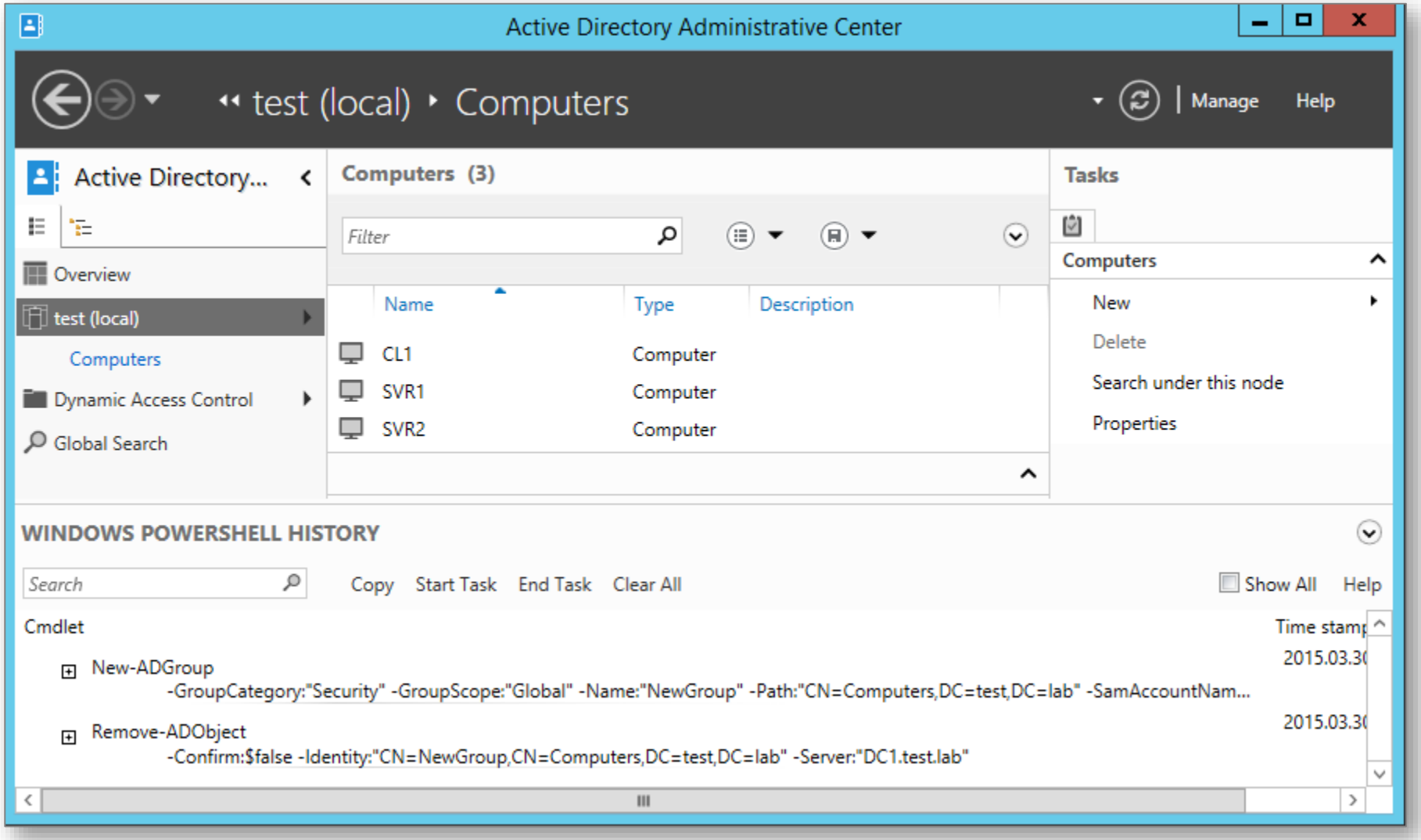
Grafikus PowerShell interfész AD DS objektumok menedzseléséhez.

Minden itt végrehajtott művelet igazából egy PoweShell parancs, amit akár ki is lehet másolni és PoweShell ablakba illeszteni.

Segítségével a következő feladatok végezhetők el:

- User, csoport és computer fiókok létrehozása és menedzsmentje
- OU létrehozás és menedzsment
- Csatlakozás domain-hez és a domain kezelése
- Keresés és szűrés AD adatokban
- Dynamic Access Control beállítása

AD Administrative center



PowerShell + Directory Service

PowerShell AD modul: Automatikusan importálódik, ha a modulhoz tartozó cmdlet-et használunk.

Directory Service parancssori eszközök:

- **dsadd**: Objektumok létrehozása
- **dsget:** Objektumok és azok tulajdonságainak megjelenítése
- **dsmod:** Objektumok tulajdonságainak módosítása
- **dsmove:** Objektumok mozgatása
- **dsquery:** Objektumok lekérdezése szűréssel
- **dsrm:** Objektumok törlése

Felhasználói fiókok

A felhasználói fiók (*user account*) tartalmazza a felhasználó nevét, jelszavát, csoporttagságait.

- Segítségével engedélyezhető, hogy egy felhasználó egy adott gépre bejelentkezzen a fiókhoz rendelt adatokkal.
- Szabályozható a hozzáférés egyes folyamatokhoz és szolgáltatásokhoz.
- Szabályozható az AD-beli objektumok elérése.

A felhasználói fiók domain szinten autentikálja a felhasználókat, azaz egy domain-en belüli felhasználói fiók a domain minden gépén érvényes alapértelmezetten.

Felhasználói fiókok

Felhasználói fiók létrehozása:

AD Users and Computers / AD Administrative Center / PowerShell / dsadd

A létrehozáskor meg kell adni:

Full name: OU szinten egyedi teljes név.
UPN (User Principal Name): Forest szinten egyedi név (nev@UPN_suffix)

Felhasználói fiókok

További beállítások:

Log on hours: *Mikor jelentkezhet be a felhasználó*

Log on to: *Mely gépekre jelentkezhet be a felhasználó*

Account expires: *Lejáró érvényességű fiók (szerviz fiókokhoz)*

User must change password at next log on

Smart card is required for interactive log on

Password never expires

User cannot change password

Store password using reversible encryption

Account is trusted for delegation: *Szerviz fiók inperszonalizálhat felhasználói fiókot, hogy azon keresztül érjen el szolgáltatásokat.*

Felhasználói fiókok

Organization: A felhasználó szervezettel kapcsolatos adatai

Member of: Mely csoportoknak legyen tagja a felhasználó

Password Settings: Felhasználóra szabott jelszó megszorítások megadása

Profile: Személyes adatok tárolásának helye

Extensions: Kiegészítő felhasználói információk

Template használata: Egy üzemen kívüli minta fiók létrehozása, majd annak másolása. (Pl AD Users and Computers -> jobb klikk a másolandó felhasználón, majd „Copy…”).

Csoportok

Distribution:

E-mail alkalmazások esetén használható. Nem használ SID-et.

Security:

Rendelkezik SID-del, így security-enabled. Jogosultságok adhatók a csoportnak. E-mail engedélyezettként is lehet használni.

A két csoport oda-vissza alakítható. Az alapértelmezett típus a security.

Csoport hatáskörök

Hatáskör	Mely csoportokból tartalmazhat fiókokat	Ezekhez adhat hozzáférést	Ezekké konvertálható
Local	Domain felhasználók és computer-ek, a forest bármely domainjének globális és univerzális csoportjai Domain-local csoportok az adott domainben A csomópont lokális felhasználói	Adott gép erőforrásai	---
Domain local	Domain felhasználók és computer-ek, a forest bármely domainjének globális és univerzális csoportjai Domain-local csoportok az adott domainben	A domainhez tartozó erőforrások	Universal (amíg nem tartalmaz másik domain local csoportot)
Global	Domain felhasználók és computer-ek, az adott domain globális csoportjai	Az erdő bármely domainjének erőforrásai	Universal (amíg nem tagja másik globális csoportnak)
Universal	Domain felhasználók és computer-ek, a forest bármely domainjének globális és univerzális csoportjai	Az erdő bármely domainjének erőforrásai	Domain local Global (amíg nem tartalmaz más univerzálisat)

IGDLA

A csoportok egymásba ágyazhatók (group nesting). Az egymásba ágyazás követendő mintája szerint az alábbi hierarchiát érdemes követni:

I: Identities
Olyan felhasználók és computerek, melyek benne vannak egy

G: Global group-ban
Ami szerepkörök alapján csoportosítja tagjait. A szerepköröket jelző tagok tagjai

DL: Domain Local csoportoknak
melyek az erőforrásokhoz adnak

A: (access) elérést

Multidomain környezetben a korábbi rövidítés egy „U” betűvel egészül ki (Universal group). Ez esetben a különböző domainek global csoportjait összegyűjtjük univerzális csoportokba, majd ezeket ágyazzuk be a Domain Local csoportba

Alapértelmezett csoportok

Adminisztrátor szerepkört adó csoportok

Forest root Users conntainer:

Enterprise admins – domain konfiguráció a forest-en belül bárhol

Schema admins – séma adminisztráció

Domainenkénti Users container

Domain admin – domain szintű adminisztráció

Cert Publishers – tanúsítványok kiadása

Domainenkénti Built-in container

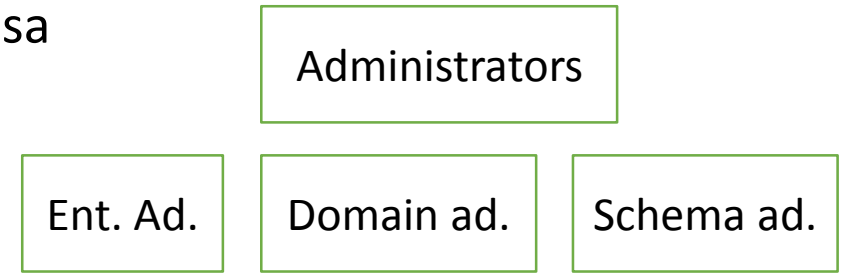
Administrators – fő admin

Server operators – DC felügyelet

Account operators – felhasználó management

Backup operators – backup

Print operators – nyomtatás, dc leállítás, indítás



Védett és saját csoportok

A védett (protected) csoportok tagjai jogosultságaikat nem az ou szintű jogosultság beállításból öröklik, hanem a védett csoportból.

Védett csoportok nem tehetők nem védetté (unprotected).

Általában nem javasolt az üres védett csoportokhoz (pl. Az előző dián *dőlttel* szedett csoportok) felhasználókat adni. Helyette hozzunk létre saját csoportot és állítsuk annak jogosultságait a **minimálisan elégséges**re.

Speciális identitások

Ezek olyan csoportok, melynek tagjait az operációs rendszer menedzseli.

Ezek a csoportok nem láthatók a megfelelő mmc snap-in-ekben, nem adhatunk és vehetünk el tagokat a csoportba/csoportból.

DE felhasználhatók jogosultság beállítások megadásakor.

Fontosabb speciális csoportok:

Anonymous Logon: Kapcsolat egyes erőforrásokhoz név és jelszó nélkül

Authenticated Users: Autentikált felhasználók kivéve „Vendég”

Everyone: Autentikált felhasználók + Vendég

Interactive: A helyi erőforrásokat elérő felhasználók (a hálózatiakat nem)

Network: A hálózati erőforrásokat elérő felhasználók (a helyieket nem)

Creator Owner: Az objektum létrehozója

Computer fiókok

A computer objektumok a felhasználókhoz hasonlóak

- Van nevük és jelszavuk, amit a Windows szerver tart karban periodikusan
- Autentikáltak a domainben
- Csoportokhoz tartozhatnak, jogosultságaik lehetnek

A computer objektumok menedzsmentje az alábbiakból tevődik össze

Beállítások módosítása

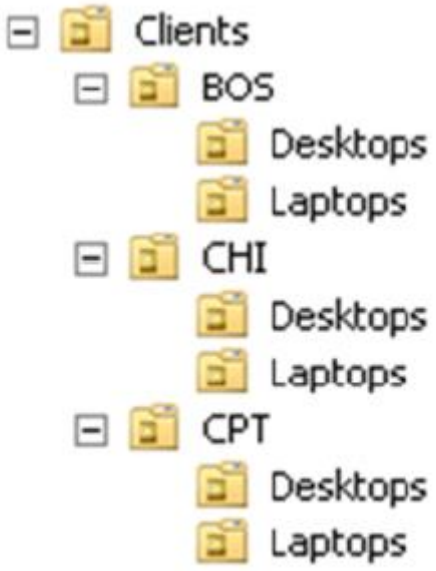
- Az objektumok mozgatása OU-k között
- Magának a computer-nek a menedzselése
- A computer objektum átnevezése, engedélyezése, letiltása, törlése, visszaállítása

A computer objektumok helye

A domain létrehozásakor automatikusan létrejön a Computers és egy Domain Controllers konténer

Ezek használata azonban pont a konténerek és ou-k közötti különbségek miatt nem ajánlott.

- Nem rendelhető hozzá GPO
- Nem osztható további részekre



Helyette érdemes saját hierarchikus rendszert felépíteni OU-kból.

Minimálisan egy servers és egy clients ou

A szervereket szokás szerepkör alapján, míg a klienseket pl elhelyezkedés alapján tovább csoportosítani.

A computer objektumok létrehozása

Alapesetben computer objektumot Enterprise Administrator, Domain Administrator, Administrator és Account operator hozhat létre, de javasolt inkább a „Create computer objects” jogosultság felhasználóhoz/csoporthoz rendelésével kijelölni.

Egy új gép domainbe léptetésekor javasolt először létrehozni az objektumot és csak ezután elvégezni a fizikai beléptetést, noha ez fordítva is lehetséges.

Gyakorlati feladat