

Windows rendszeradminisztráció és Microsoft szerveralkalmazások támogatása

7. óra

Kocsis Gergely,
Supák Zoltán

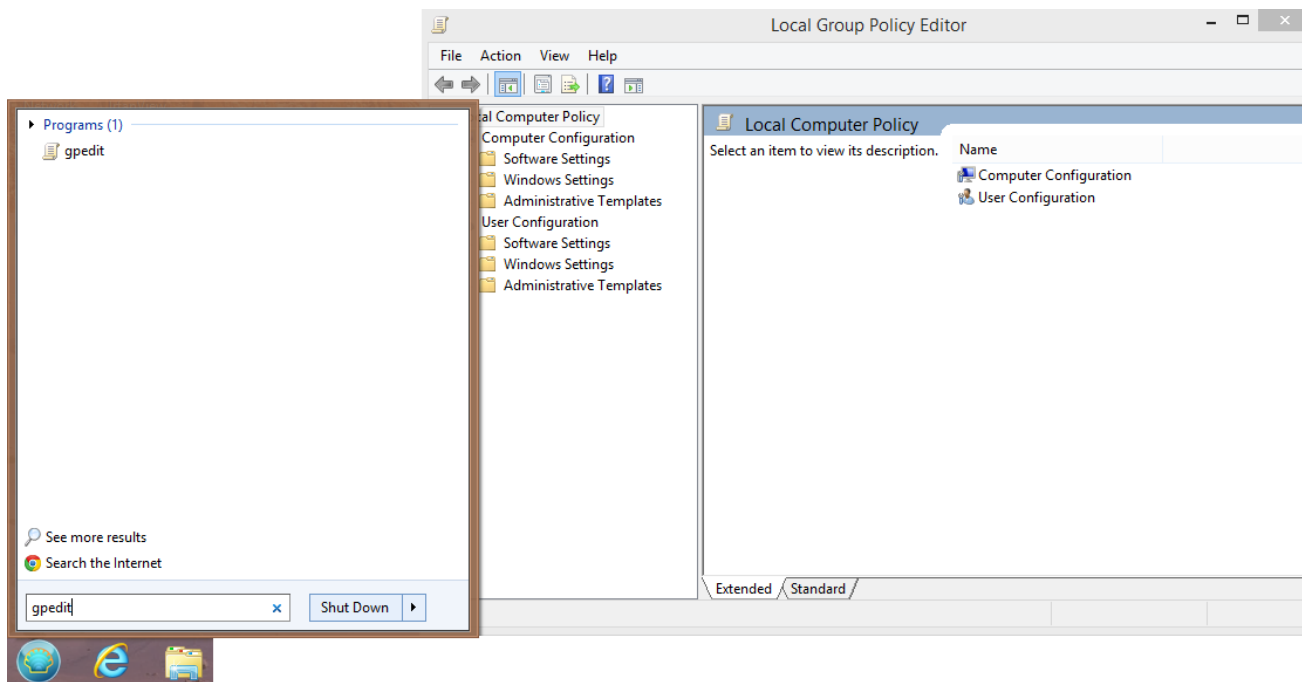
2016.04.13.

Group Policy alapok

Group Policy

A **group policy** (csoportházi rend) a Windows rendszerű számítógépek egy funkciója, melynek segítségével megoldható felhasználók és számítógépek viselkedésének és jogosultságainak szabályozása.

Nem csak Szerver környezetben használható:



Group Policy Settings

Group policy setting: A csoportházirend legalapvetőbb része. Egy konkrét, adott objektumra (számítógép/felhasználó) alkalmazott beállítás.

Ezekből a szabályokból több ezer létezik, de nem mindegyik alkalmazható egy adott rendszerben (Lehet elavult, vagy még nem alkalmazható).

Egy beállítás három különböző állapotban lehet:

- Nem beállított
- Engedélyezett (enabled)
- Tiltott (disabled)

Group Policy Settings

A GP beállítások általában két nagy csoport egyikébe sorolhatók

- felhasználóra vonatkoztatott
- számítógépre vonatkoztatott

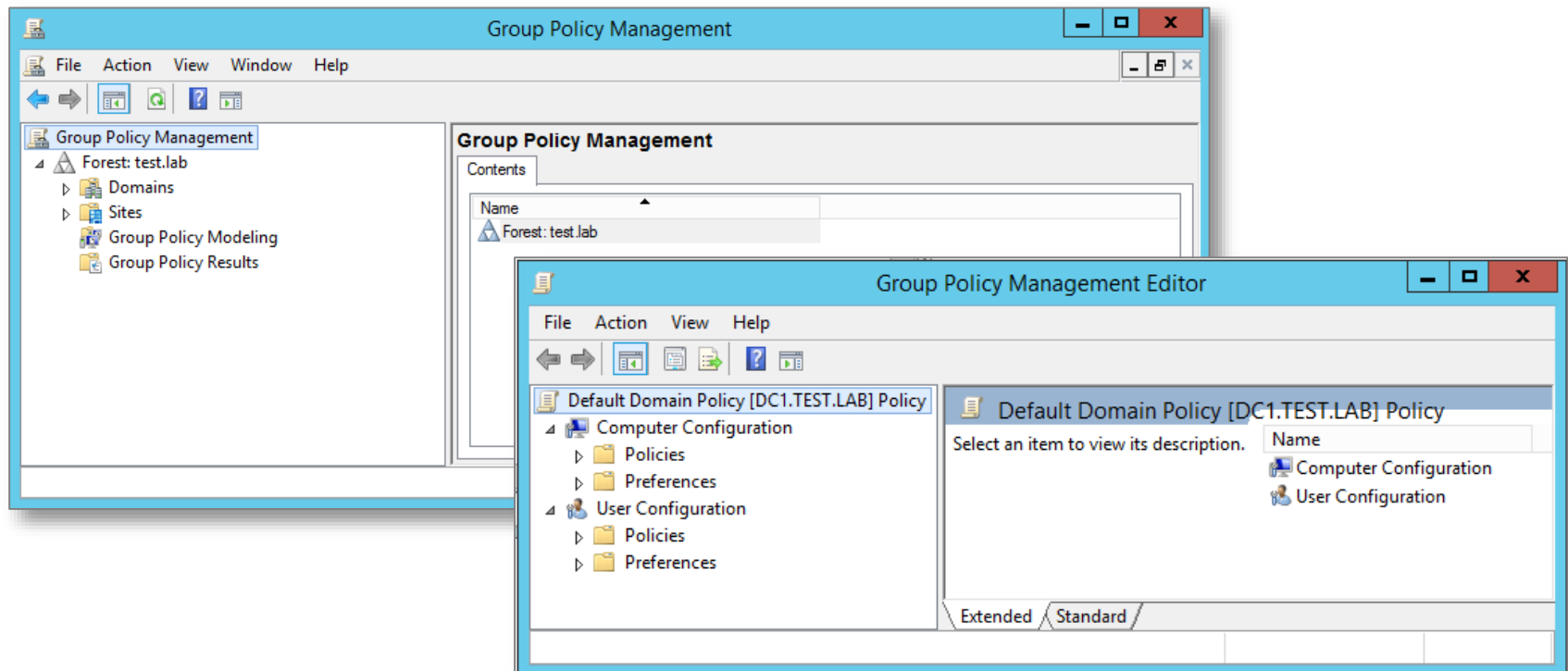
Mindkét csoporton belül három különböző területhez tartozhat egy beállítás:

- **Szoftver beállítás:** Mely szoftverek telepíthetők egy gépen, vagy egy felhasználó által.
- **Windows OS beállítás:** Script és biztonsági beállítások
- **Administrative template-ek:** Több száz a felhasználói munkakörnyezet befolyásolására alkalmas szabály a Microsoft-tól vagy más gyártótól. További templatek is letölthetők (Pl. MS Office templates).

Group Policy Object

A GPO olyan objektum, mely egy, vagy több (számítógépre és/vagy felhasználóra vonatkozó) GP beállítás tárolására szolgál.

A GPO-k kezelésére a GP Management Console szolgál (GPMC). A GPMC-n belül a GP Management Editor szolgál a GPO-k szerkesztésére.



Group Policy Preferences

A GP Management Edit-ben mind a Computer configuration, mind a User configuration csomópont alatt van egy Preferences lehetőség a Policies mellett.

A GP Preference-ek (tulajdonságok) további beállítási lehetőségeket tesznek lehetővé a GP Policy-k mellett.

Sok szempontból különböznek a GP policy-ktől.

- Nem kényszerítettek
- Bejelentkezéskor alkalmazódik, esetleg időintervallumonként újra
- A GPO eltávolításakor nem törlődnek
- ...

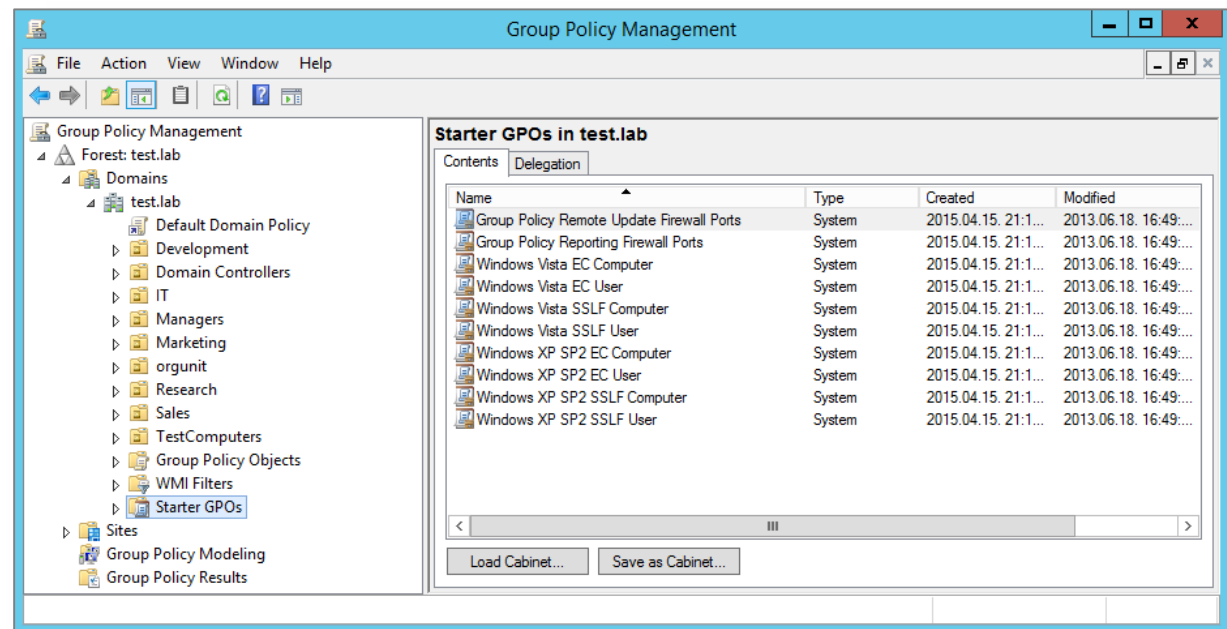
Pl. Parancsikonok, Start menü, Internet beállítások

Starter GPO

A Starter GPO gyakorlatilag egy GPO template melynek segítségével egyszerűen hozhatók létre azonos alapokon nyugvó, de egyes részletekben különböző GPO-k.

Egy Starter GPO tartalmazhat beállításokat a User és Computer configuration-ból, de a Software és Windows Settings-ből nem, mivel ezek a beállítások domain és szolgáltatásfüggők.

Minta Starter GPO-k:



The screenshot shows the Group Policy Management console for the test.lab domain. The left pane displays the tree structure under 'Forest: test.lab', with 'Starter GPOs' selected. The right pane, titled 'Starter GPOs in test.lab', shows a list of GPOs with columns for Name, Type, Created, and Modified. The list includes various GPOs for Windows Vista and Windows XP SP2, such as 'Remote Update Firewall Ports', 'Reporting Firewall Ports', 'EC Computer', 'EC User', 'SSLF Computer', and 'SSLF User'. The 'Created' and 'Modified' dates for all listed GPOs are 2015.04.15 21:1... and 2013.06.18 16:49... respectively.

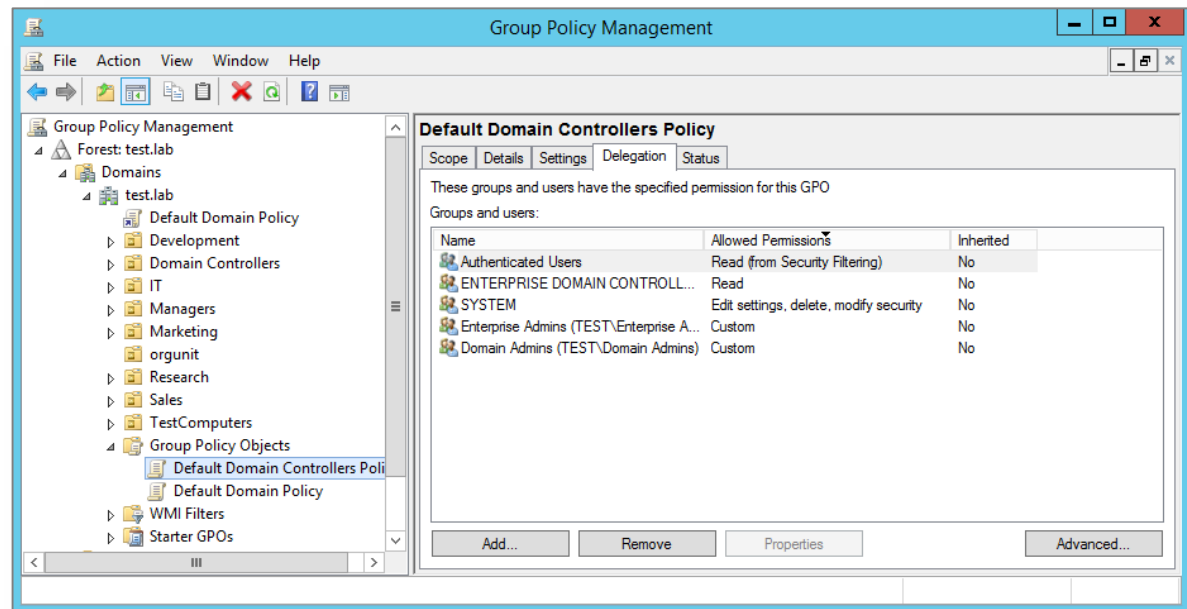
Name	Type	Created	Modified
Group Policy Remote Update Firewall Ports	System	2015.04.15 21:1...	2013.06.18 16:49...
Group Policy Reporting Firewall Ports	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows Vista EC Computer	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows Vista EC User	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows Vista SSLF Computer	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows Vista SSLF User	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows XP SP2 EC Computer	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows XP SP2 EC User	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows XP SP2 SSLF Computer	System	2015.04.15 21:1...	2013.06.18 16:49...
Windows XP SP2 SSLF User	System	2015.04.15 21:1...	2013.06.18 16:49...

GPO managemerek

Alapértelmezés szerint az alábbi csoportok tagjai szerkeszthetik a GPO-kat:

- Domain Admins
- Enterprise Admins
- Creator Owner
- Local System

A GPMC segítségével a GPO-k kezelésének nagy részével kapcsolatos jogosultságok más felhasználókra is ráruházhatók.



GPO linkelése

A GPO létrehozása után azt egy konténerhez kell linkelni.

GPO-t a GPMC segítségével lehet linkelni a következő konténer típusokhoz:

- Site
- Domain
- OU

Linkelés után a konténer (és minden tartalmazott konténer) minden objektumára aktiválódnak a GPO-ban leírt szabályok.

A létrejött link inaktíválható és törölhető.

GPO nem alkalmazható direktben felhasználókra, csoportokra, számítógépekre és rendszer szintű konténerekre sem. (Utóbbiak a domain szinten linkelt GPO-kat öröklük.)

GPO-k életbe lépése

- A számítógéppel kapcsolatos beállítások induláskor
- A felhasználókkal kapcsolatos beállítások bejelentkezéskor aktiválódnak
- A szabályok (policy) adott időközönként frissülnek
- A biztonsági beállítások 16 óránként frissülnek
- A GP szabályok manuálisan frissíthetők (Invoke-Gpupdate)
- WS2012 után távoli frissítés is lehetséges

GPO-k feldolgozási sorrendje

A később feldolgozott GPO-k felülírják a korábbi GPO-k által alkalmazott ütköző beállításokat.

1. Lokális GPO-k (a Windows gépeken lévő helyi beállítások)
2. Site szintű GPO-k
3. Domain szintű GPO-k
4. OU szintű GPO-k
5. Gyermek OU-k szintjén alkalmazott GPO-k

Azonos szinten alkalmazott GPO-k preferencia sorrend szerint kerülnek feldolgozásra. Ezt a sorrendet az Admin állítja meg.

Alapértelmezett GPO-k

Default Domain Policy

A domain-hez linkelt GPO alapértelmezés szerint tartalmazza a jelszóval és beléptetéssel kapcsolatos szabályokat. Elméletileg lehetséges, de nem javasolt további bővítése

Default Domain Controllers Policy

A Domain Controllers OU-hoz rendelt GPO. Felhasználói jogosultságokat és audit beállításokat kezel. Szintén nem javasolt további bővítése.

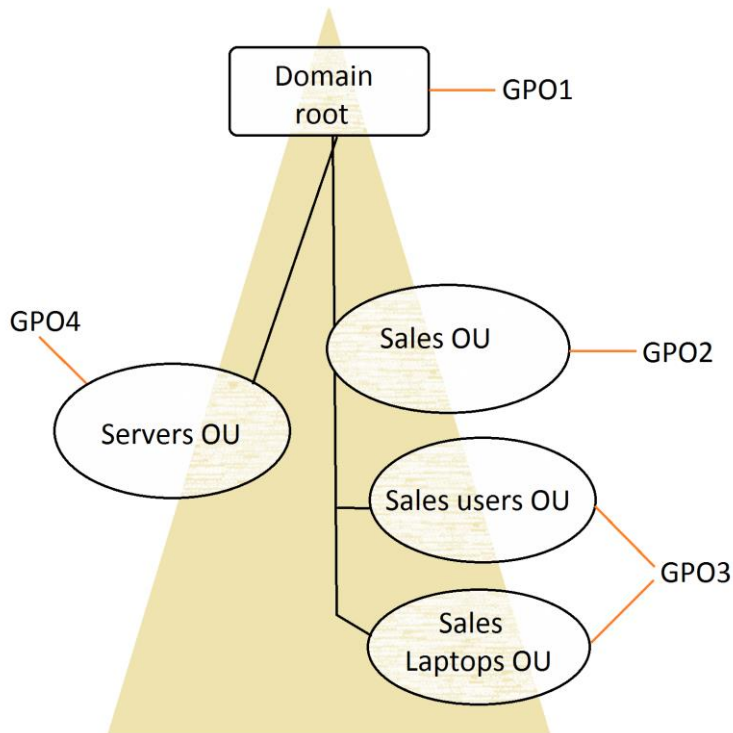
GPO Security szűrés

Minden GPO-hoz létezik egy ACL (access control list), melyen belül beállítható, hogy egyes csoportok milyen jogkörrel rendelkeznek a GPO-t illetően.

GPO letiltása: Az ACL megfelelő alkalmazásával az azzal kapcsolatos jogkörök úgy szűkíthetők, hogy pl egy adott OU-n belül ugyan alkalmazott a GPO, de ez alól kivételeket teszünk.

Ez a lehetőség a GPO szerkesztésekor a Delegation -> Advanced lehetőség alatt érhető el.

GPO-k sorrendje



GPO1: Domain szinten alkalmazott. 30 perc inaktivitás után kikapcsol a HDD és a monitor.

GPO2: Sales OU szinten alkalmazott. PI: nyomtató beállítás, gép lezárásának beállítása, Control Panel letiltás.

GPO3: További energiagazdálkodási beállítások a Sales Laptopok részére.

GPO4: A szerverek számára külön energiagazdálkodási szabályok (ne kapcsoljanak ki soha)

- A Servers OU szerverei milyen energiagazdálkodási szabályokat követnek?
- A Sales Laptops gépei milyen energiagazdálkodási szabályokat követnek?
- Milyen energiagazdálkodási szabályokat követ a domain többi gépe?
- Ha lokális szinten engedélyezem a Control Panel elérését a Sales OU egy gépén, elérhető lesz-e?
- Hogyan adhatnál Control Panel elérést egyes felhasználóknak?
- Alkalmazható a GPO2 más OU-kra is?

Ajánlott olvasmányok

Csoportházi rend áttekintése

<https://technet.microsoft.com/hu-hu/library/hh831791.aspx>

A csoportházi rendek kezeléséről IT-szakembereknek

<http://windows.microsoft.com/hu-hu/windows7/group-policy-management-for-it-pros>

Security filtering using GPMC

[https://technet.microsoft.com/en-us/library/cc781988\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/cc781988(v=WS.10).aspx)

Gyakorlati feladat

