

5. GPO - teoria, info ja backup

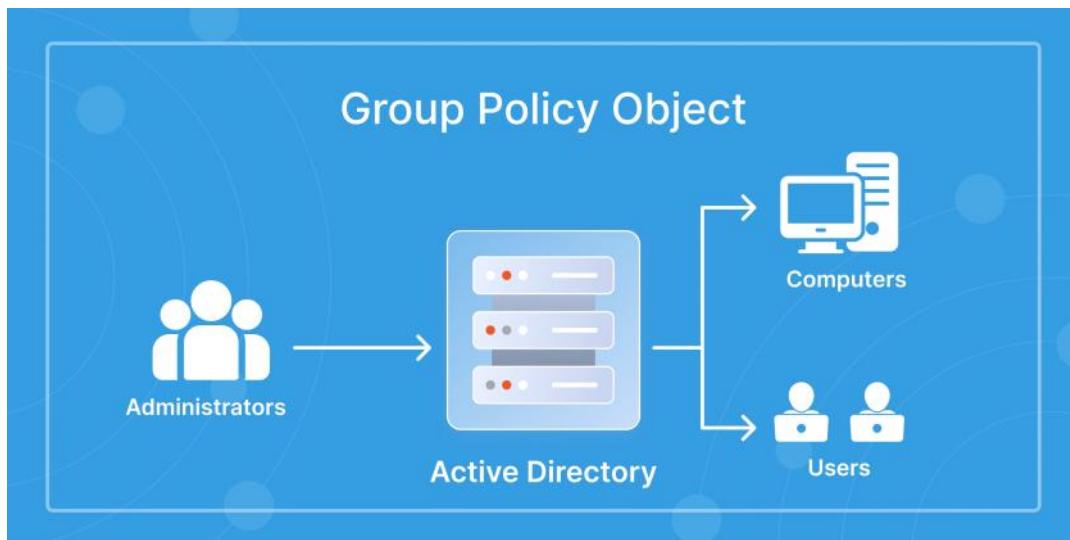
Saturday, October 11, 2025 09:32

GPO (Group Policy Object)

- GPO = ryhmäkäytäntöobjekti, jolla voidaan hallita käyttäjien ja koneiden asetuksia keskitetysti AD:ssä.

GPO EI rajoitu vain työasemiin. Se voi vaikuttaa:

- Käyttäjiin (esim. "Kaikki opiskelijat" tai "HR-tiimi")
- Laitteisiin (esim. "Kaikki työasemat", "Kaikki palvelimet")
- Ja **molempien erikseen tai yhtä aikaa**, riippuen miten GPO on kohdistettu.



📘 YLEINEN TILANNE HAASTATTELUSSA:

"Miten jakaisit ohjelmia tai asetuksia käyttäjille Active Directory -ympäristössä?"

"Oletko käytänyt ryhmäkäytäntöjä? Osaatko estää USB-tikut tai pakottaa työpöydän taustan?"

"Miten estäisit että käyttäjä ei pääse komentokehoteeseen tai tehtävienhallintaan?"

Mikä on tärkein ero **User Configuration** ja **Computer Configuration** välillä?

Mihin kohtaan AD-rakennetta sää linkittäisit GPO:n, joka rajoittaa opiskelijoiden ohjelmia?

Tämä pätee myös työssään jos pääsee työntekijäksi ja saa admin oikeudet, että tulevien ticketistä ja ongelmista voi tulla tällaisia AD juttuja. Ongelmista voi olla esim. Työasemat, käyttäjä itsensä, työaseman sovellukset, GPO oikeudet ja muu policy asetuksien kannalta, tai jopa AD palvelimen itsensä.

#####

◇ 1. Mikä on GPO? (Group Policy Object)

GPO on ryhmäkäytäntöobjekti – AD:n työkalu, jolla voidaan **asettaa sääntöjä ja asetuksia keskitetysti** koneille ja käyttäjille.

Esimerkiksi:

- Estää tehtävienhallinta
- Pakota taustakuva
- Määritää palomuuri- tai salasana-asetukset
- Salli vain tietyt ohjelmat
- Aja skripti kirjautuessa

▣ Tärkeää: **GPO ei tee mitään yksinään**. Se pitää:

1. Luoda
2. Linkittää oikeaan kohteeseen AD:ssä
3. Määrittää, mitä se tekee

◇ 2. Mihin GPO:t liittyvät Active Directoryssa?

AD:ssä resurssit jaetaan usein näin:

- Domains → esim. organisaatio.local
- Organizational Units (OU:t) → loogisia ryhmiä/yksikkö, esim. Opiskelijat, Henkilöstö, Palvelimet

GPO linkitetään näihin tasoihin. Se vaikuttaa kaikkiin kohteeseen alla oleviin käyttäjiin tai koneisiin.

Esimerkki:

Jos linkität GPO:n OU:hun nimeltä "Opiskelijat", se vaikuttaa:

- Kaikkiin opiskelija-käyttäjiin, jotka ovat siinä OU:ssa
- Tai niiden koneisiin – riippuen, onko GPO:n asetukset käyttäjä- vai konetason

3. GPO:ssa on kahta tyyppiä asetuksia:

Taso	Esimerkkejä	Vaikutus kohdistuu...
Computer Configuration	esim. palomuuri, käynnistyskriptit	laitteeseen (kun käynnistyy)
User Configuration	esim. työpöytä, ohjelmarajoitukset	käyttäjään (kun kirjautuu)

Tärkeä sääntö:

Jos asetat käyttäjäasetuksia mutta linkität GPO:n koneeseen – se ei tee mitään. Ja toisin päin.

4. Mitä pitäisi osata käytännössä (harjoittelussa tai työssä)?

Taito	Kuvaus
GPO:n luominen	Tiedät, miten luodaan uusi Group Policy Management Consolessa
Linkitys OU:hun	Osaat linkittää GPO:n oikeaan kohteesseen
Asetusten valinta	Osaat valita oikeat asetukset (User vs Computer)
gpupdate /force	Osaat päivittää GPO:t koneella manuaalisesti
gpresult /r	Osaat tarkistaa, mitkä GPO:t vaikuttaa johonkin käyttäjään tai koneeseen
Kohdistus (scoping)	Osaat rajata GPO:n vaikuttavuutta esim. ryhmäsuodattimilla (Security Filtering) tai WMI-suodattimilla
Vianetsintä	Osaat tarkistaa miksi GPO ei toimi (esim. linkitys puuttuu, oikea taso, periytyminen jne.)

Windowsin ryhmäkäytännön (Group Policy) päivitys

- Windows päivittää ryhmäkäytännöt automaattisesti **90 minuutin välein**, satunnaisella viiveellä **±30 minuuttia**.
- Jos ei jaksa odottaa automaattista päivitystä, voi pakottaa käytäntöjen päivityksen komentoriviltä:
 - **PowerShell / komentokehote:** gpupdate /force
- Tämä toimii sekä **palvelimella** että **työasemalla**, ja pakottaa kaikki käytännöt päivittymään heti.

5. Tyypillisiä tehtäviä harjoituksissa / työssä

- Luo GPO, joka estää USB-laitteet
- Pakota tietyt salasanakäytännöt (pituus, vanheneminen jne.)
- Estää pääsy komentoriville
- Aja kirjautumiskripti (esim. verkkolevyn mapitus)
- Näytää eri työpöydän asetukset opiskelijoille ja henkilökunnalle

Mitä "konfigurointi" GPO:ssa oikeasti tarkoittaa?

Konfigurointi = asetusten määrittämistä → mitä tehdään ja miten.

Tähän jakautuu kahteen osaan ja kahteen tyyppiin:

- "**Computer Configuration**" = mitä tapahtuu koneelle, kun se käynnistyy
- "**User Configuration**" = mitä tapahtuu käyttäjälle, kun hän kirjautuu

GPO voi kohdistua ryhmään vai yksittäiseen työasemaan/käyttäjään

miten GPO on sidottu ja suodattettu. Tässä simpeli jako:

1 Normaalisti GPO kohdistetaan kokonaisiin ryhmiin tai OU:ihin

- Esim. "Opiskelijat"-OU → kaikki sen käyttäjät saavat samat käyttäjäasetukset
- Esim. "Työasemat"-OU → kaikki sen koneet saavat samat konfiguraatiot

💡 Tämä on oletustapa: **hallitaan monia koneita/käyttäjiä samalla asetuksella**.

2 Mutta GPO voidaan kohdistaa tarkemmin

- **Security Filteringillä** → voit sanoa "tämä GPO vaikuttaa vain tähän AD-käyttäjään tai -ryhmään"
- **WMI-suodattimilla** → esim. "tämä GPO koskee vain koneita, joissa on Windows 11"

Yrityksien käyttö - Active Directory GPO asetuksista:

Active Directoryn GPO-asetukset voivat vaihdella organisaation koon, liiketoimintatarpeiden ja työympäristön mukaan:

◇ Miten nämä soveltuват eri kokoisiin organisaatioihin / etätyöhön

- **Pienet organisaatiot:** Usein vain muutama OU, vähän GPOja. Riittää, että nämä perusturva- ja hallintoperusasetukset ovat käytössä. Ei ole suurta byrokratiaa.
- **Keskisuuret & suuret:** Tarvitaan selkeä OU-rakenne, nimeämiskäytäntö, dokumentointi. Näitä minimiasetuksia voi laajentaa esim. yrityskohtaisilla sovelluksilla, verkkoasetuksilla, eri tiimien tai maantieteellisten sijaintien tarpeilla.
- **Etätyö / hybridti:** Kun käyttäjä ei ole aina toimistossa, pitää varmistua että GPO-asetukset päivityvät myös, että kirjautumiset, VPN-asetukset, palomuurit ja päivitykset toimivat myös kun laite on etänä.

#####

Työaseman konffaust ja esimerkit

◇ 1. Esimerkkejä GPO-asetuksista (sovellukset, USB, lokitus jne.)

💻 Työasemalle sovellusten hallinta (Computer Configuration):

- **Salli vain tietty ohjelmat (whitelisting):**
User Configuration > Policies > Administrative Templates > System > Run only specified Windows applications
→ Estää kaikkien muiden kuin lueteltujen ohjelmien käytön
- **Estää tietty ohjelmat:**
User Configuration > Policies > Administrative Templates > System > Don't run specified Windows applications
→ Käyttäjä ei voi käynnistää esim. cmd.exe, powershell.exe, regedit.exe

💡 USB-porttien estäminen/salliminen:

- **Täysi esto USB-laitteille (tallennus):**
Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access
→ Estää luku/kirjoitus USB:ltä
- **Salli vain luku tai estää kirjoitus:**
→ Voit erikseen säättää luku- ja kirjoitusoikeudet (esim. voit lukea mutta et kopioi tiedostoja koneelta tikulle)
- **Huom:** USB-hiiri/näppis ei esty näin – säädot koskee lähinnä **tallennuslaitteita**

💻 Administrator- tai käyttööikeuksiin liittyvät asetukset:

- **Estää paikallisen järjestelmävalvojan käyttö:**
→ Voit tehdä GPO:lla, joka tyhjentää Administrators-ryhmän tai määrittää sallitut käyttäjät
- **Ei oikeutta asentaa ohjelmia:**
→ Rajoita User Configuration > Policies > Control Panel > Prohibit access to Control Panel and PC settings
→ Tai käytä Software Restriction Policies tai AppLocker

💻 Lokitus / auditointi:

- **Kirjaa kaikki kirjautumiset:**
Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration
→ Kirjaa mm. kirjautumiset, tiedostojen käytöt, järjestelmämuutokset
- **Tarkastele lokitapahtumia koneelta:**
→ Event Viewer > Windows Logs > Security

⌚ 2. Entä jos kyseessä on Mac?

GPO toimii vain Windows-ympäristössä. Jos käytössä on **Mac-koneet**, GPO ei niihin suoraan vaikuta.

Mutta:

🔧 Miten Macien hallinta hoidetaan?

- **MDM (Mobile Device Management) = Maceille tyypillinen hallintatapa**
 - Esim. Jamf, Microsoft Intune, Mosyle
 - Näillä voidaan:
 - Hallita ohjelmia ja päivityksiä
 - Estää sovelluksia
 - Hallita asetuksia (verkkoyhteydet, salasanat, jne.)
 - Lukita tai tyhjentää laitteen etänä

⌚ Microsoft Intune osaa nykyään hallita sekä Windowsia että MacOS:ää, mutta se ei käytä GPO:ta – vaan omaa profiilijärjestelmää.

#####

#####
#####

GPO ja OU - konffaust

OU = organization units

Mitä OU tarkoittaa?

OU = looginen "kansio" tai ryhmä Active Directoryssä. Niihin laitetaan:

- Käyttäjät (esim. työntekijät)
- Tietokoneet (esim. työasemat)

ESIM)

 Esimerkki tilanteesta:

Myynti (OU)
|— Myynti-Helsinki (alinen OU)
|— Myynti-Tampere
└— Myynti-Turku

Mitä tapahtuu, jos asetat GPO:n "Myynti"-OU:hun?

◊ GPO vaikuttaa kaikkiin sen OU:n alla oleviin kohteisiin:

- Myynti-Helsinki
- Myynti-Tampere
- Myynti-Turku

→ Periytyy alikansioihin, ellei estä periytymistä.

 Tätä kutsutaan GPO:n periytymiseksi (inheritance).

ESIM2)

Entä jos haluat rajoittaa vaikutusta vain esim. Helsingin myyntitiimiin?

Tässä on pari tapaa:

1. Linkitä GPO vain "Myynti-Helsinki"-OU:hun

→ Vain sen sisällä oleviin koneisiin/käyttäjiin vaikuttaa

2. Security Filtering

- GPO voidaan linkittää laajempaan OU:hun (esim. koko Myynti)
- Mutta **Security Filteringillä** määritetään:
"Tämä GPO vaikuttaa vain ryhmään Myynti-Helsinki"

 Tämä toimii, kun haluat **täsmärajauksen ryhmän mukaan**, ei OU:n

VINKKINÄ:

- Pienemmissä ympäristöissä riittää usein OU-pohjainen hallinta
- Isomissa tai monimutkaisemmissa tilanteissa yhdistetään:
 - OU-rakenne
 - GPO:n **Security Filtering**
 - Mahdollisesti **WMI-suodattimet** (esim. "vain Windows 11 -koneisiin")

#####
#####

#####
#####

GPO - harjoituksien ideoita - START HERE;

Siis vinkkeinä mitä esim. Voisi kokeilla ja harjoitella tulevaisuudessaan/myöhemmin

1. Käynnistä työpöytä rajoitetusti (Desktop Lockdown)

- Estä oikean hiirinapin käyttö työpöydällä
- Piilota "This PC" ja "Network" -kuvakkeet
- Estä pääsy komentokehotteeeseen ja Regeditiin

 **Hyöty:** Turvallisuus, kontrolli esim. koulussa tai julkisessa käytössä

2. USB-muistitikkujen estäminen (Device Installation Restrictions)

- Estää kirjoitus tai luku USB-laitteilta
- Estää kaikki siirrettäväät tallennuslaitteet

 **Hyöty:** Yritystietoturva ja tietovuotojen esto

3. Aseta pakotettu taustakuva (Desktop Background)

- Aseta yrityksen logo tai väri työpöydän taustaksi
- Estää käyttäjää vaihtamasta sitä

 **Hyöty:** Brändäys ja yhtenäinen ilme

4. Skripti kirjautumiseen tai uloskirjautumiseen

- Kirjoita PowerShell- tai .bat-skripti, joka suoritetaan käyttäjän kirjautuessa
 - Esim. luo kotikansio, kirjaa logitiedosto, tarkista levytila

 **Hyöty:** Automaattiset toiminnot ilman IT-tukea

5. Ohjelman asennus GPO:lla (Software Deployment)

- Jaa esimerkiksi 7-Zip tai Notepad++ käyttäjille tai koneille MSI-paketilla
- Voit käyttää joko **User Configuration** tai **Computer Configuration**-asetusta

 **Hyöty:** Keskitetty ohjelmahallinta

6. Aseta salasana- ja lukituspolitiikka

- Salasanan vähimmäispituus, vanhenemisaika, monimutkaisuusvaatimus
- Aseta ruudun lukitus x minuutin jälkeen

 **Hyöty:** Vaatimus lähes kaikissa tuotantoymäristöissä

7. Rajoita pääsy Ohjauspaneeliin ja asetuksiin

- Poista "Settings" tai "Control Panel" kokonaan näkyvistä
- Estää käyttäjän muokkaamasta verkkaoasetuksia tai näyttöasetuksia

 **Hyöty:** Hallinta, etenkin julkisilla tai jaetuilla koneilla

BONUS: Harjoittele GPO:n kohdistamista oikein

Käytä **Security Filtering** ja **WMI Filtering**:

- Kohdista GPO vain tietyille käyttäjille (esim. vain "Myynti" OU)
- Kohdista GPO vain tiellylle Windows-versiolle (esim. vain Win11)

 Harjoitusympäristöehdotus:

```

YritysXC.local
├── OU=IT
│   └── Käyttäjät: janne.it, pekka.it
├── OU=Myynti
│   └── Käyttäjät: laura.myynti, tommi.myynti
└── OU=Harjoittelu
    └── 5 muuta käyttäjää
  
```

Testata GPO:n kohdistamista **vain Myynti-OU:lle**, ja varmistaa että **IT:n käyttäjät eivät saa samaa GPO:ta**.

#####

GPO-konfiguroinnin perusmuistutus – START HERE

Tämä on tärkeä kuvaus GPO-asetusten konfiguroinnista, joka koskee sekä käyttäjiä, työasemia että järjestelmän toimivuutta kokonaisuutena.

◊ GPO-asetukset vaikuttavat:

- **Käyttäjiin (User Configuration)**
- **Laitteisiin (Computer Configuration)**
- Sekä koko **organisaation AD-rakenteeseen**

Muista aina:

Asetuksista voi tulla **ristiriitoja**, jos:

- Samoja asetuksia konfiguroidaan useassa GPO:ssa eri tavoilla
- Asetukset periytyvät ylhäältä ja alempi GPO tekee toisin
- Eri tiimit tekevät omia GPO-muutoksia koordinoimatta

GPO:t eivät vaikuta vain käyttäjän oikeksiin – ne voivat muuttaa koko **työaseman toimintaa**, esim.:

- USB-porttien käytettävyyttä

- Sovellusten asennusoikeuksia
- Turvallisuuspolitiikkaa (salasanat, kirjautumiset, lokitus)

Testaaminen ja erottelu on välttämätöntä:

Jos aiot kokeilla tai testata GPO-asetuksia:

- Luo itsellesi **oma testikäyttäjä tai testi-työasema**
- Luo erillinen **OU testikäytöön**
- Vältä suoraa muutosta tuotantoon → testaa ensin pienessä mittakaavassa

Tee testit niin, että **ne eivät vaikuta muihin tiimeihin tai työasemiin**

→ Tämä estää vahingot ja helpottaa virheiden korjausta

Vinkki:

Jos joskus ei muista tarkalleen mitä GPO tekee →

Tarkista:

- Mihin se on linkitetty?
- Mitä asetuksia se sisältää (User vai Computer)?
- Onko se "Enforced"?
- Onko periytyminen estetty jossain?

 Jos aikoo tehdä GPO-muutoksia, josta vaikutavat vain yhteen käyttäjään - saattaa myös vaikuttaa koko tiimiin tai työasemiin, että testattavana on parasta dokumentoida ja erota asiansa selkeästi.

TOP 7 GPO-pelisääntöä (konfiguroinnin hyvät käytännöt)

1. Suunnittele ensin – konfiguroi vasta sitten

- Älä tee "testi-GPO:ta" tuotantoon summassa
- Piirrä tai hahmottele OU-rakenne ja mihin mitäkin GPO:ta tarvitaan

2. Nimeä GPO:t selkeästi

- Esim. GPO - Myynti - Estä USB
 - Ei nimiä kuten "Test1" tai "Uusi GPO"
- Selkeä nimi auttaa heti ymmärtämään mitä GPO tekee ja mihin se liittyy

3. Pidä yksi GPO yhdelle tarkoitukselle

- Älä tunge 50 eri asetusta yhteen GPO:hon
 - Esim. yksi GPO salasanapolitiikalle, toinen ohjelmarajoituksille
- Tämä tekee hallinnasta ja vianetsinnästä paljon helpompaa

4. Käytä OU-rakennetta hyödyksi – älä tee liikaa poikkeuksia

- Tee GPO:t OU-tasolla, jos mahdollista
- Älä rakenna joka koneelle tai yksittäiselle käyttäjälle omaa GPO:ta

5. Vältä ristiriitaisia asetuksia

- Jos sama asetus on kahdessa GPO:ssa eri tavalla → voi tulla konflikti
- Tällöin voimaan jää:
 - Se, jonka **linkitys on lähempänä** objektiä (esim. alimmassa OU:ssa)
 - Tai se, jolla on "**Enforced**" (**pakotettu**)-tila päällä

6. Dokumentoi, mitä GPO tekee ja miksi

- Kirjoita GPO:n "**Comment**"-kenttään selitys
- Hyvä muistaa, kun joku toinen (tai sinä itse puolen vuoden päästä) kysyy: "Miksi tämä on täällä?"

7. Testaa ensin pienellä ryhmällä

- Luo testi-OU tai testikäyttäjäryhmä
 - Linkitä GPO ensin sinne
- Näet miten se käyttäätyy ennen laajempaa käyttöönottoa

#####
#####

5 tärkeää asiaa koskien GPO oppiminen ja käyttää kunnolla työssään - START HERE;

1. "Loopback Processing" – erikoistilanne työasemille

Jos haluat, että **käyttäjä saa tietyt asetukset vain tiellä koneella**, etkä kaikkialla:

 Käytetään asetusta:

Computer Configuration > Policies > Administrative Templates > System > Group Policy > User Group Policy loopback processing mode

 Tätä tarvitaan esim. **yhteiskäyttööasemissa** (esim. koulun kirjaston koneet, vieraskäyttäjät)

◊ 2. Vianetsinnän perustyökalut:

Kun GPO ei toimi, nämä **komennot auttavat**:

- gpupdate /force = päivittää GPO:t heti
- gprestart /r = näyttää käyttäjään ja koneeseen kohdistuvat GPO:t
- rsop.msc = avaa graafisen näkymän toteutuneista asetuksista

➡ Näillä selvität:

- Mitä asetuksia on voimassa?
- Mitä GPO:ita on sovellettu ja missä järjestysessä?
- Mikä GPO voitti, jos asetukset menevät ristiin?

◊ 3. "Enforced" ja "Block Inheritance" – sääntöjen painottaminen

- **Enforced (Pakotettu)** = GPO asetetaan niin, että sitä **ei voi ohittaa alempaan**
- **Block Inheritance** = estää yläpuolelta tulevien GPO:iden periytyminen

❖ Käytä näitä harkiten, sillä ne voivat **tehdä rakenteesta monimutkaisen** tai vaikeasti ylläpidettävän.

◊ 4. Käyttöoikeudet GPO-hallintaan

Et voi aina muokata kaikkia GPO:ita – niihin liittyy **oikeudet**:

- **GPO:n luonti ja muokkaus** vaatii, että sulla on siihen tarvittavat AD-oikeudet
- GPO:lle voi antaa muokausoikeudet esim. tietylle tiimille, mutta muille vain lukuoikeudet

⌚ Esimeriksi harjoittelijana et ehkä pääse suoraan muokkaamaan tuotanto-GPO:ita.

◊ 5. Dokumentointi ja versointi – tärkeys kasvaa isommissa ympäristöissä

Jos organisaatiossa on paljon GPO:ita, **kaiken dokumentointi on pakollista**, esimeriksi:

- Mikä GPO tekee mitä?
- Mihin se on linkitetty?
- Kuka sen loi tai muutti ja milloin?

❖ Isommissa ympäristöissä käytetään joskus työkaluja kuten:

- **AGPM (Advanced Group Policy Management)**
- **Microsoft Intune** (jos siirrytään pilvihallintaan)

#####
#####

Tarkistus joko Powershellin ja käyttöliittymän (GUI) kanssa - koskien GPO - START HERE;

Molemmissa on yhtä hyvä ja huonot puolet, mutta riippuu tottumuksesta ja käyttötä, ja toiminnasta kummasta tarkistaa niitä GPO asetuksia.

GUI (käyttöliittymä) toimii hyvin, kun halutaan esim. selata ja muokata yksittäisiä GPO:ita manuaalisesti.

Powershell on parempi, kun halutaisiin tarkistaa nopeasti, mitä GPO:ita vaikuttaa tiettyyn käyttäjään tai koneeseen – **ja ilman että sotkeaisi mitään.**

❖ Hyödyllisiä PowerShell-komentoja GPO-tarkistuksiin

- ◊ Näytä kaikki GPO:t domainissa: \$Get-GPO -All
- ◊ Tarkista tietyn GPO:n asetukset: \$Get-GPOReport -Name "GPO-nimi" -ReportType Html -Path "C:\Temp\GPO.html"
 - → Avaa GPO.html selaimessa, näet kaikki asetukset tarkasti
- ◊ Näytä GPO:t jotka on linkitetty tiettyyn OU:hun: \$Get-GPLink -Domain "domain.local" -Target "ou=Myynti,dc=domain,dc=local"
- ◊ Näytä käyttäjään tai koneeseen kohdistuvat GPO:t (koneelta käsin): \$gprestart /r

Muutamia esimerkki tilanteita ja tämä voisi toimia lunttilappuna ja esimerkinä:

- Etsi OU tai ryhmä: ou=Myynti-Helsinki & tarkistaa siihen linkitetty GPO:t
 - \$Get-GPLink -Target "ou=Myynti-Helsinki,dc=firma,dc=local"
- Vie jokaisen GPO:n sisällöt tiedostoon:
 - \$Get-GPOReport -Name "Estä USB" -ReportType Html -Path "C:\GPO\EstäUSB.html"

#####
#####

Mahdolliset yleiset GPO - konfigurointien virheet - START HERE;

Yleisimpiä virheitä Active Directoryssa ja GPO-asetuksissa ovat huolimattomuus käyttöoikeuksissa, huono OU-rakenne ja puutteellinen testaus ennen tuotantoon viemistä. Nämä virheet voivat aiheuttaa tietoturvaongelmia, toimintahäiriöitä ja hallinnan vaikeuksia.

Active Directoryn yleiset virheet

- **Lian monta käyttää Domain Admins -ryhmässä**
 - Lisää tietoturvariskiä. Vain harvojen tulisi kuulua tähän ryhmään.
- **Privilegioitujen tilien käyttö arkipäiväisiin tehtäviin**
 - Esim. sähköpostin lukeminen Domain Admin -tilillä altistaa järjestelmän turhaan.
- **Ei nimeämiskäytäntöä AD-objekteille**
 - Sekava rakenne vaikeuttaa hallintaa ja automatiota.
- **Kuvauskenttiä jättäminen tyhjiksi**
 - Vaikeuttaa objektienv tunnistamista ja dokumentointia.
- **Flat OU-rakenne (Organizational Unit)**
 - Ei mahdollista tarkkaa GPO-kohdistusta tai delegointia.
- **Stale accounts – vanhojen tilien jättäminen järjestelmään**
 - Käytämättömät tilit voivat olla hyökkäysvektoreita.
- **DNS-virheellisydet**
 - AD riippuu DNS:stä – virheellinen konfiguraatio voi estää GPO:n toiminnan ja kirjautumiset.
- **Ei System State -varmuuskopioita**
 - Vaarantaa palautumisen kriittisissä tilanteissa.

GPO-asetuksiin liittyvät virheet

- **GPO:n kohdistus väärään OU:hun**
 - Väärät asetukset voivat levitä laajalle tai jäädä kokonaan soveltuumatta.
- **Security Filteringin virheellinen käyttö**
 - GPO ei ehkä kohdistu haluttuihin käyttäjiin tai koneisiin.
- **Useita ristiriitaisia salasana-politiikkoja**
 - Voi aiheuttaa epäselvyyksiä käyttäjille ja teknisiä ongelmia.
- **Default Domain Policy -asetusten ylikirjoittaminen**
 - Voi rikkota perusasetuksia, kuten kirjautumiskäytäntöjä.
- **Liiallinen GPO:n käyttö**
 - Monimutkaista hallintaa ja hidastaa koneiden käynnistymistä.
- **Ei testata hiekkalaatikossa ennen tuotantoa**
 - Virheelliset asetukset voivat lamauttaa koko ympäristön.

Parhaat käytännöt virheiden välttämiseksi

- Luo selkeä OU-rakenne ja nimeämiskäytäntö.
- Käytä ryhmäsenyyksiä ja **Security Filteringia** hallitusti.
- Testaa GPO:t **hiekkalaatikossa** ennen tuotantoon viemistä.
- Dokumentoi kaikki muutokset ja käytä **kuvauskenttiä**.
- Pidä **System State -varmuuskopiot** ajan tasalla.
- Käytä **Least Privilege -periaatetta**: vain tarvittavat oikeudet.

Testaus hiekkaympäristössä

Hiekkaympäristö (sandbox) on korvaamaton, koska se mahdollistaa:

- **GPO-asetusten kokeilun ilman riskiä**
- **Skriptien ja automaation testauksen**
- **Käyttäjäroolien ja oikeuksien simuloinnin**
- **Palautumisen harjoittelun (esim. System State -backup)**

Testaa aina ennen tuotantoon vientiä, vaikka käyttäjä olisi vain muutama. Pienikin virhe voi lamauttaa koko ympäristön.

Olennaiset konfiguroitavat asiat

- **OU-rakenne**: Jäsennä käyttäjät loogisesti (esim. tiimit, roolit, testikäyttäjät).
- **GPO-politiikat**:
 - Salasanakäytännöt
 - Kirjautumisrajoitukset
 - Desktop-asetukset
 - Software deployment (jos käytössä)
- **Ryhväsenyydet**: Luo AD-ryhmät roolien mukaan (esim. HR, IT, Johto).
- **Delegointi**: Anna tiiminvetäjille oikeudet hallita omia OU:itaan.
- **Auditointi ja lokitus**: Seuraa muutoksia ja kirjautumisia.

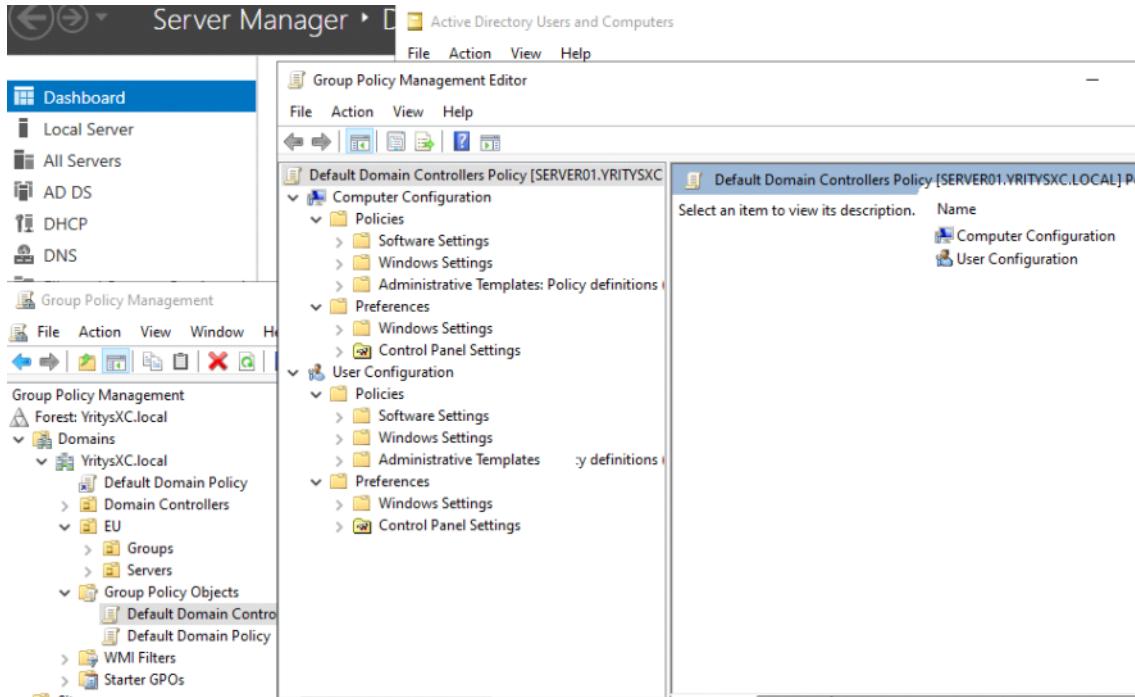
Parhaat käytännöt

- **Versioi GPO-muutokset**: Pidä kirja mitä muutettiin ja miksi.

- **Käytä testikäyttäjiä:** Luo dummy-käyttäjiä eri rooleihin.
- **Simuloi virhetilanteita:** Testaa mitä tapahtuu, jos GPO ei toimi.
- **Dokumentoi kaikki:** Helpottaa vianmääritystä ja tiimityötä.

```
#####
#####
```

GPO User & Computers configuration --> policies & preferences



Tämä koskien yksittäisen GPO säännön sisällä sisältyy "Computer & User configuration" asetusta, että molempien alla sisältyy lisäksi "Policies" ja "Preferences" alikansiot.

Molempien alla on mukaan lukien erilliset asetukset (policies & preferences), että mukaan lukien sisäisessä jakautuu lisää policy asetuksia ja on vaikea päätellä uudesta policy asetuksista, että kumppaan ne menee..

Group Policy Object (GPO) jakautuu kahteen osaan:

- Computer Configuration ja User Configuration.
- Molemmissa on kaksi haaraa: Policies (pakottavat asetukset) ja Preferences (suosituksit, joita käyttäjä voi muuttaa).

TÄMÄ ON HYVÄ PIENI PELISÄÄNTÖ:

Jos kyseessä on kohdistus koskeeko se koneeseen vai käyttäjään & Kun puhutaan Computer Configuration ja User Configuration -termeistä, ne viittaavat Active Directory objekteihin: tietokoneobjekteihin ja käyttäjäobjekteihin.

Computer Configuration

- Kohdistuu tietokoneeseen riippumatta siitä, kuka käyttäjä kirjautuu sisään.
- Esimerkkejä: palomuuriasetukset, ohjelmien asennukset, salasana- ja suojausasetukset, käynnistysskriptit.
- Käytetään, kun halutaan, että *kaikki käyttäjät samalla koneella* noudattavat samoja sääntöjä.

User Configuration

- Kohdistuu käyttäjään riippumatta siitä, millä koneella hän kirjautuu sisään.
- Esimerkkejä: työpöydän taustakuva, verkkolevyjen kytkennit, selainasetukset, kirjautumisskriptit.
- Käytetään, kun halutaan, että *käyttäjä saa samat asetukset kaikkialla*.

Jos halutaan, että kaikki samalla koneella noudattavat sääntöä → Computer.

Jos halutaan, että käyttäjä saa asetukset missä tahansa koneella → User.

Sitten molemmilla jakutuu haara alikansioita:

Jos kyseessä on sääntö onko se pakko (policies) vai suositus (preferences)

- **"Policies = laki, Preferences = ehdotus. Policies pakottaa ja palauttaa, Preferences antaa muuttaa."**
- **"Policies päivityvät säännöllisesti, Preferences ei välittämättä."**

Policies vs. Preferences

- Policies (käytännöt)
 - Pakottavia asetuksia.
 - Käyttäjä ei voi muuttaa niitä (tai jos muuttuu, järjestelmä palauttaa ne seuraavassa päivityksessä).
 - Esim. salasanojen pituusvaatimus, estettyjen ohjelmien lista.
- Preferences (mieltymykset)
 - Suosituksia tai oletusasetuksia.
 - Käyttäjä voi muuttaa niitä, eikä järjestelmä pakota takaisin.
 - Esim. verkkolevyn automaattinen kytkentä, oletustulostin, pikakuvakeet työpöydälle.

#####
#####

GPO asetuksien backup ja muu backup

Tämä pieni kuvaus koskien GPO policy säännöstä, jos on konfiguroinut alkuun ja tätä on hyvä suorittaa **varmuuskopiointia**. Koska jos windows serverissä tapahtuu jotakin poikkeamia mm. bluescreen, suurta vianmääritystä, päivitystä tai muuta poikkeavaa - on hyvä ottaa aikaisempia konfiguroituja GPO policy sääntöjä talteen.

Koska ettei tarvitse keksiä uutta pyörää (Älä turhaan tee uudelleen sellaista, mikä on jo olemassa ja toimivaa.) niin siirtää olemassa olevan säännön ja muokkaa esim. Siitä ja jos on tarvetta. Tämä päätee tuotannossa kuin hiekkaympäristössä (Vmworkstation testilabrassa), ja samahan siirrettyn varmuuskopioinista pitää ehdottomasti testata, että pelittääkö ja pienellä testi käyttäjällä ja laiteella.

- Virallinen GPO backup ohje ja demo sivusto on alla (5.3. GPO ja powershell - backup)

Mikä on varmuuskopointi (backup)?

Varmuuskopointi tarkoittaa alkuperäisen datan tallentamista erilliseen paikkaan, jotta se voidaan palauttaa, jos järjestelmässä tapahtuu jokin häiriö, virhe tai vaurio. Esimerkiksi jos Windows Server -työasemassa ilmenee ongelma, voidaan aiemmin otettu varmuuskopio palauttaa joko testilaboratorioympäristöön tai viralliseen tuotantoymäristöön. Näin saadaan järjestelmä takaisin toimivaksi ilman, että kai kki täytyy rakentaa uudelleen alusta.

Active Directoryn varmuuskopointi

Active Directoryn (AD) osalta tärkeintä on varmuuskopioida **järjestelmän tila (System State)**, joka sisältää kaikki AD:n toiminnan kannalta kriittiset tiedot:

- AD-tietokanta (NTDS.dit)
- SYSVOL-kansio (ryhmäkäytännöt ja skriptit)
- Rekisteri
- Sertifikaattipalvelut (jos käytössä)
- Käynnistystiedostot ja palvelinkokoontanot

Erityishuomiot virtuaaliympäristössä (esim. VMWorkstation)

Virtuaalikoneessa (VM) varmuuskopioinnissa ja palautuksessa on tärkeää huomioida:

- Snapshotteja ei tule käyttää AD:n palautukseen ilman erityiskäsittelyä – ne voivat aiheuttaa replikointivirheitä
- Palautuksessa tulee käyttää **järjestelmän tilan varmuuskopiota**
- Varmista, että AD:n replikointikumppanit tunnistavat palautetun tilan oikein (Invocation ID)