

## 5.3.1. GPO backup/disabled pohdinta

Tuesday, October 28, 2025 16:54

### Pohdinta ja teoria:

Jos tekisi toisen VM3 (toisen serverin) pyörimään - niin tätä voisi esim. Suorittaa ja siirtää esim. VM1 <----> VM3 tietoja ja molemmissa pitää olla yhteensopivuuden datoja.

GPO-varmuuskopiot ovat yhteensopivia Windows Server 2019, 2022 ja 2025 välillä, kunhan domain-ypäristö on toimiva. Tärkeimmät tiedostot varmuuskopiassa ovat backup.xml, greport.xml ja GPT.ini, joista voit tarkistaa GPO:n asetukset, tunnisteet ja versiot.

### 📁 GPO-varmuuskopion rakenne ja tärkeimmät tiedostot

Kun suoritat Backup-GPO, se luo jokaiselle GPO:lle oman alikansion, esimerkiksi:

```
E:\GPO backups\{GPO-GUID}\  
|  
└── backup.xml      # Sisältää metatiedot: nimi, GUID, varmuuskopion aika  
└── greport.xml    # Raportti GPO:n sisällöstä: asetukset, linkitykset, suodatus  
└── GPT.ini        # SYSVOL-kansion asetustiedosto (versio, timestamp)  
└── Machine/       # Tietokonekohtaiset asetukset (jos käytössä)  
└── User/          # Käyttäjäkohtaiset asetukset (jos käytössä)
```

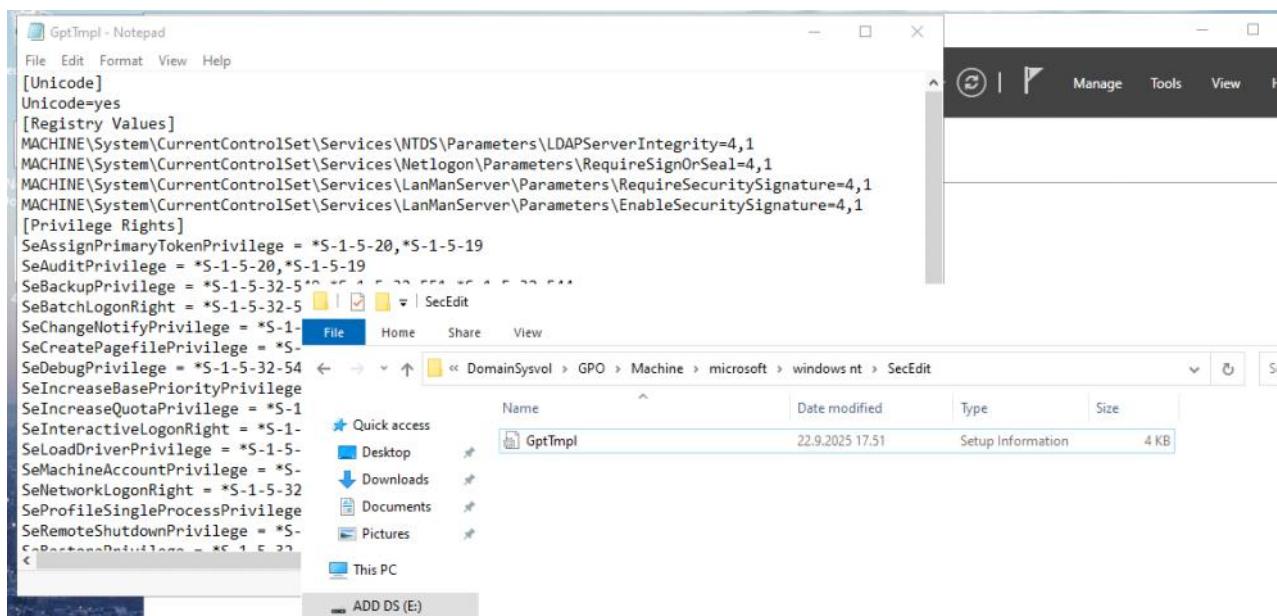
### 🔍 Mitä tarkistaa tiedostoista?

Tiedostoissa on asioita mitä pitää tarkistaa, jotta ne datat menevät yhteensopivuudeksi.

Otin jonkin noista, mutta katsellaan mitä se sanoo.. Ja täyttää liirum laarum

### 🔒 GptImpl.inf

- Tämä tiedosto määrittelee **Security Settings**-osion GPO:ssa:
  - Account policies (esim. salasanen pituus, lukitus)
  - Local policies (esim. auditointi, käyttäjäoikeudet)
  - Event log settings
  - Restricted groups
  - System services
  - Registry ja file system permissions



Palataan asiansa tähän:

File Home Share View

ADD DS (E:) > GPO backups > {651B8CD8-6D6E-4C94-8A19-FD9084283129} >

	Name	Date modified	Type	Size
Quick access	DomainSysvol	28.10.2025 3.49	File folder	
Desktop	Backup	28.10.2025 3.49	XML Document	7 KB
Downloads	greport	28.10.2025 3.49	XML Document	48 KB
Documents				

Tässä "backup.xml" tiedoston alla on jotakin keskeisiä asioita, ja miten se vaikuttaa GPO:n siirtoon tai palautukseen toisessa ympäristössä.

The screenshot shows the Windows Server Manager interface. In the left navigation pane, under 'All Servers', a GPO named '{651B8CD8-6D6E-4C94-8A19-FD9084283129}' is selected. In the main content area, the 'ADD DS (E:) > GPO backups' path is highlighted. A file named 'Backup' is selected and highlighted with a red box. The right pane displays the XML content of the 'Backup.xml' file, showing various XML elements like <SamAccountName>, <Type>, <NetBIOSDomainName>, <UPN>, <Group bkp:Source="FromDACL">, and <Sid>. Several entries contain the string 'YRITYSXC'. The status bar at the bottom indicates 'ms 1 item selected 47,2 KB'.

```

]]>
</SamAccountName>
- <Type>
  - <![CDATA[
    UniversalGroup
  ]]>
</Type>
- <NetBIOSDomainName>
  - <![CDATA[
    YRITYSXC
  ]]>
</NetBIOSDomainName>
- <DnsDomainName>
  - <![CDATA[
    YritysXC.local
  ]]>
</DnsDomainName>
- <UPN>
  - <![CDATA[
    Enterprise Admins@YritysXC.local
  ]]>
</UPN>
</Group>
- <Group bkp:Source="FromDACL">
  - <Sid>
    - <![CDATA[
      S-1-5-21-2366235558-2463432122-148030397-512
    ]]>
  </Sid>
  - <SamAccountName>
    - <![CDATA[
      Domain Admins
    ]]>
  </SamAccountName>
  - <Type>
    - <![CDATA[
      GlobalGroup
    ]]>
  </Type>
  - <NetBIOSDomainName>
    - <![CDATA[
      YRITYSXC
    ]]>
</NetBIOSDomainName>

```

## 🔍 Keskeiset osiot greport.xml-tiedostossa

### 1. SecurityGroups

Tämä osio listaa kaikki ryhmät, joihin GPO viittaa — joko suodatuskäytännöissä tai käyttöoikeuksissa.

- Monet ryhmät kuten Administrators, Authenticated Users, Domain Admins, Enterprise Admins jne. näkyvät, mutta **useimmita puuttuu SID**.
- Vain kaksi ryhmää (Enterprise Admins ja Domain Admins) sisältävät **SID-tunnisteen ja domainin tiedot**:
  - S-1-5-21-2366235558-2463432122-148030397-519 → Enterprise Admins
  - S-1-5-21-2366235558-2463432122-148030397-512 → Domain Admins

### 🔍 Tarkista nämä:

- Onko kohdeympäristössä **sama domain** (YritysXC.local)?
- Jos ei, nämä SID-viitaukset voivat olla **epäyhenteisopivia** ja GPO:n suodatus ei toimi.
- Jos palautat GPO:n eri domainiin, harkitse **ryhmien uudelleenmäärittelyä**.

### 2. GroupPolicyCoreSettings

Tämä osio kertoo GPO:n perustiedot:

Elementti	Arvo
ID	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Domain	YritysXC.local
• DisplayName	Default Domain Controllers Policy
MachineVersionNumber	65537
UserVersionNumber	0

#### ⌚ Tarkista nämä:

- **Domain:** Jos palautat eri domainiin, tämä voi aiheuttaa ristiriitoja.
- **DisplayName:** Jos kohdeympäristössä on jo GPO samalla nimellä, harkitse uudelleennimeämistä.
- **VersionNumber:** Ei yleensä ongelma, mutta kertoo että GPO:ta on muokattu.

## 3. GroupPolicyExtension

Tämä osio kertoo, mitä laajennuksia GPO käyttää — eli mitä asetuksia se sisältää.

#### 🔒 Security Extension:

bkp:DescName="Security"  
bkp:ID="{827D319E-6EAC-11D2-A4EA-00C04F79F83A}"

- Viittaa tiedostoon GptTmpl.inf, joka sisältää **Security Settings** (esim. käyttäjäoikeudet, auditointi).
- Polku: DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf

#### 📋 Registry Extension

bkp:DescName="Registry"  
bkp:ID="{35378EAC-683F-11D2-A89A-00C04FBBCFA2}"

- Viittaa rekisteriasetuksiin (esim. Registry.pol tiedostot).
- Polku: %GPO\_FSPATH%\Adm\\*.\*

#### ⌚ Tarkista nämä:

- Onko tiedostot kuten GptTmpl.inf ja Registry.pol mukana varmuuskopiossa?
- Jos palautat GPO:n, nämä tiedostot **määrittävät sen toiminnan** — varmista että ne ovat ehjiä ja relevantteja.

## 🌐 Yhteenveton tarkistus: mitä sinun kannattaa tarkistaa ennen palautusta

Tarkistettava	Miksi tärkeää
Domain (YritysXC.local)	Pitää olla sama tai yhteensopiva
SID-viittaukset	Vain kaksi ryhmää sisältää SID — tarkista yhteensopivuus
DisplayName	Vältä nimiristiriitoja kohdeympäristössä
Extension-polut	Varmista että GptTmpl.inf ja Registry.pol ovat mukana
SecurityDescriptor	Sisältää käyttöoikeudet — ei yleensä muokattava, mutta voi vaikuttaa

#####
#####

## GPO-sääntöjen hallinta: Käytöstä poistaminen testauksen tueksi

Windows Server -ympäristössä, jossa käytetään Active Directorya, ryhmäkäytäntöobjektien (GPO) avulla voidaan hallita työasemien ja käyttäjien asetuksia keskitetysti. Kun GPO-sääntöjä on määritetty useita — jopa vain muutamasta useampaan — voi syntyä ristiriitoja tai odottamatottomia vaikutuksia, erityisesti testaus- tai poikkeustilanteissa.

Tämä korostuu erityisesti hiekkalaatikkoympäristöissä, joissa esimerkiksi VM1 toimii Windows Server -toimialueohjaimena ja VM2 on Windows 10/11 -työasema. Useiden GPO-sääntöjen ollessa aktiivisina, VM2:n käyttäjä saattaa kohdata rajoituksia, kuten:

- PowerShellin avaaminen vaatii jatkuvasti toimialueenvalvojan tunnuksia
- Ohjauspaneeli (Control Panel) on estetty
- Verkon asetusten muuttaminen tai DNS-osoitteiden vaihtaminen on estetty

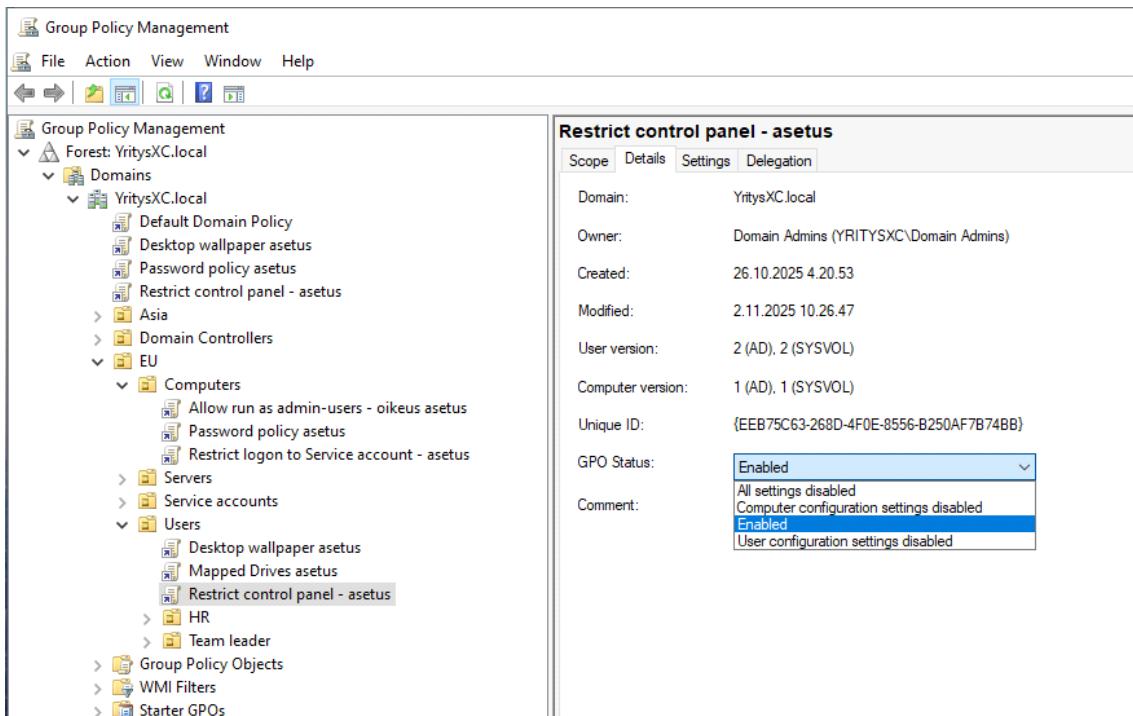
Yksi tehokas ja turvallinen tapa hallita tällaisia tilanteita on ottaa yksittäinen GPO tilapäisesti pois käytöstä muuttamalla sen **status** asetukseen "**Disabled**". Tämä ei poista GPO:ta tai sen linkityksiä, vaan estää sen vaikutuksen väliaikaisesti. Menetelmä on erityisen hyödyllinen, kun halutaan testata, aiheuttaako tietty GPO ongelmia, tai kun halutaan mahdollistaa poikkeuksellinen toiminta ilman pysyviä muutoksia.

Esim1)

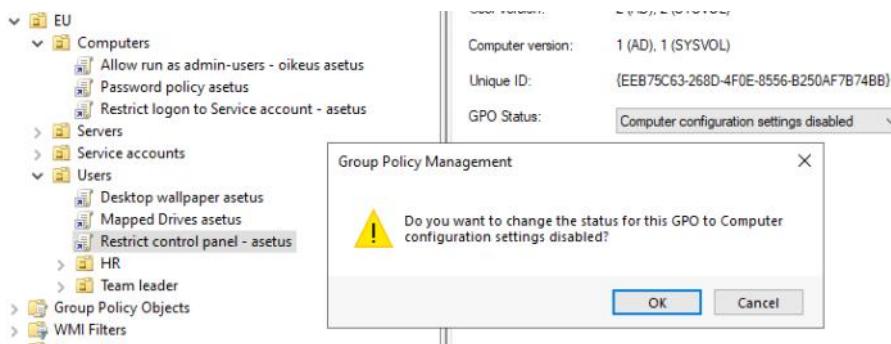
- Kokeillaan esim. Asettaa tämä vaikappa pios päältä, että menee pois väliaikaisesti käytöstä.

Oikea klikkaus GPO:sta → GPO Status → valitse jokin seuraavista:

<b>- Enabled (oletus)</b>	Sekä <i>User Configuration</i> että <i>Computer Configuration</i> ovat aktiivisia
<b>- User Configuration Settings Disabled</b>	Käyttäjäkohtaiset asetukset poistetaan käytöstä, konetasoiset jäävät voimaan
<b>- Computer Configuration Settings Disabled</b>	Konetasoiset asetukset poistetaan käytöstä, käyttäjäasetukset jäävät voimaan
<b>- All Settings Disabled</b>	Koko GPO poistetaan käytöstä, mutta säilyy olemassa ja linkitetynä



#### Kokeillaan "computer configuration settings disabled"



GPO:n tilan "**Disabled**", on hyvä päivittää käytännöt koneilla, jotta muutos astuu voimaan heti. Tämä ei tapahdu automaattisesti kaikilla koneilla välittömästi

#####
#####

## Miniyhteenvetö ja pohdinta (varmuuskopio osuus)

Tämä on tiivis kuvaus siitä, miten GPO-siirto voidaan toteuttaa käytännössä verrattuna hiekkalaatikko- eli testiympäristöön. Lisäksi pohditaan, milloin käyttöliittymä (UI) voi olla helpompi vaihtoehto kuin PowerShell.

Harjoituksen kannalta on tärkeää dokumentoida GPO-asetukset heti, kun ne on luotu, testattu ja todettu toimiviksi. Tällainen dokumentointi voi sisältää kuvakaappauksia, PowerShell-raportteja tai lyhyitä kommentteja. Varmuuskopio kannattaa tallentaa useaan paikkaan — esimerkiksi pilvipalveluun ja USB-tikulle — jotta siitä muodostuu toimiva "versio 1", johon voi tarvittaessa palata.

Sekä UI että PowerShell tarjoavat toimivia tapoja varmuuskopioida GPO:t:

- UI:n kautta voi varmuuskopioida koko objektiin tai yksittäisiä sääntöjä.
- PowerShellillä voi automatisoida prosessin ja hallita useita GPO:ita kerralla.

Jos varmuuskopio tallennetaan esimerkiksi C-levylle, verkkolevylle tai pilveen, on hyvä pitää mukana myös lyhyt kuvaus siitä, mitä GPO sisältää ja mihin se on tarkoitettu. Vaikka XML-muotoiset varmuuskopiot voivat olla vaikealukuisia, ne sisältävät selkeän rakenteen, josta voi tarkistaa asetukset, ryhmät ja linkitykset.

## POHDINTA OSUUS

Miten tästä voisi tosi elämässä kuin hiekkaympäristössä (Vmworkstaion) alla voisi suorittaa näitää GPO-sääntöjä ja asetuksia, josta vo itapahtua mm. VM1 <--> VM3 väliltä? Tämä päätee myös on eri tai sama domain yritys, että se yrityksen OU kansio yksikköiden nimeämisen käytäntö ja voi olla luotu paljon kansioita ettei haluta sotkea muita asetuksia. Kokonaisuudessaan tästä pitää suunnittella ja testata useita kertoja, jotta se GPO sääntö toimii ja pelittää.

- Yksi mahdollisuus on ensimmäisestä VM1 jos on konfiguroinnut samanaikaisesti niin ottaa videonauhoituksensa/kuvakaappauksensa niin dokumentoi johonkin talteen esim. Sharepoint tai muualta dokumentoivasta ohjeesta - niin toimivana ohje pohjana. Näin sitten jatkaa muokkaamista ja lisää tarvittavia osia ja sääntöjä, että jälkeen testaa ja toimiiko - jos toimii niin ottaa talteen siitä pohjana ja jne.
- Toisena ensimäisen VM1 siirtää VM3 windows serveriin, josta käynnistää ja suorittaa tuodun ensimmäisen varmuuskopioinnin (VM1:stä) --> VM3:lle ja jatkaa siitä - mutta ongelmansa tässä pitää tarkistaa onko sama domain ja muut koodin identtiset/yhteensopivuuden ID:t. Tämä päätee sama idea na ensimmäisen varmuuskopiointi jos on tallentanut pilvipalveluun tai tikun alle - toimivana extrana.
  - XML tiedoston alla voi olla paljon SID tai muita ID viittauksia, että OU linkitystä. Tämän osalta pitää varmistaa kahden VM1 <--> VM3 windows serveri saa yhteensopivuudensa ja pitää tarkistaa niiden täsmennykset.
- Kolmantena siirretty GPO sääntö VM1 <----> VM3:lle voi tulla toistoja , että kannattaako sitä siirrettyä GPO asettaa disabled tai ei linkitetty?