

# WINDOWS SERVER ADVANCED

GPO

# GROUP POLICY - WAT IS HET?

# Wat?

---

- Centraal beheer van instellingen
- Configuratie-instructies
- Bewaard binnen o.a. Active Directory
- Voor computeraccount(s) of gebruikeraccount(s)

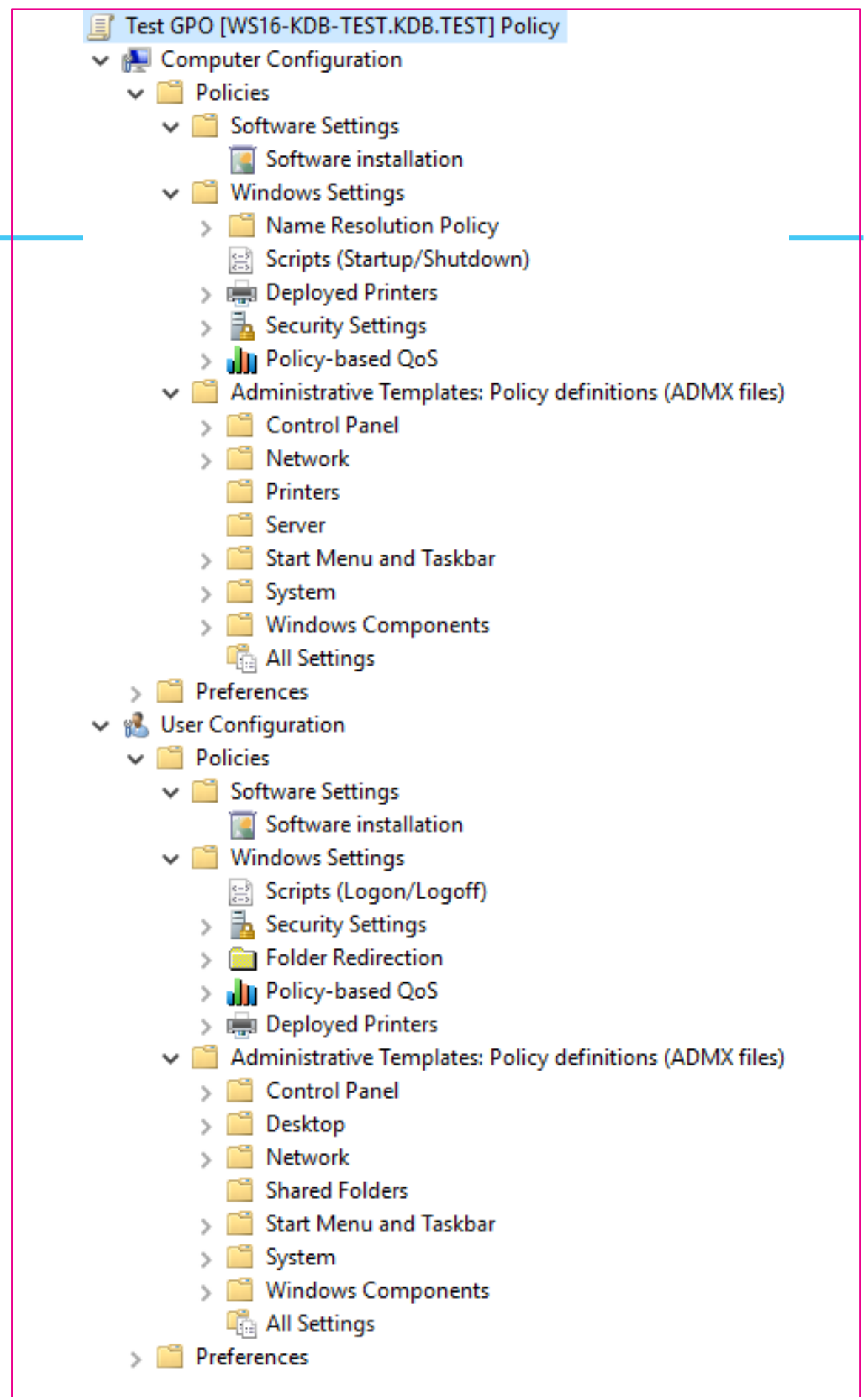
# Instellingen

---

- Security instellingen → paswoord, automatisch lockscreen, firewall
- Scripts bij opstarten, afsluiten, aanmelden en afmelden
- Publiceren van software
- Koppelen van netwerkschijven
- Publiceren van printers
- Zowat elke instelling die door een gebruiker kan aangebracht worden
  - Registry instellingen!

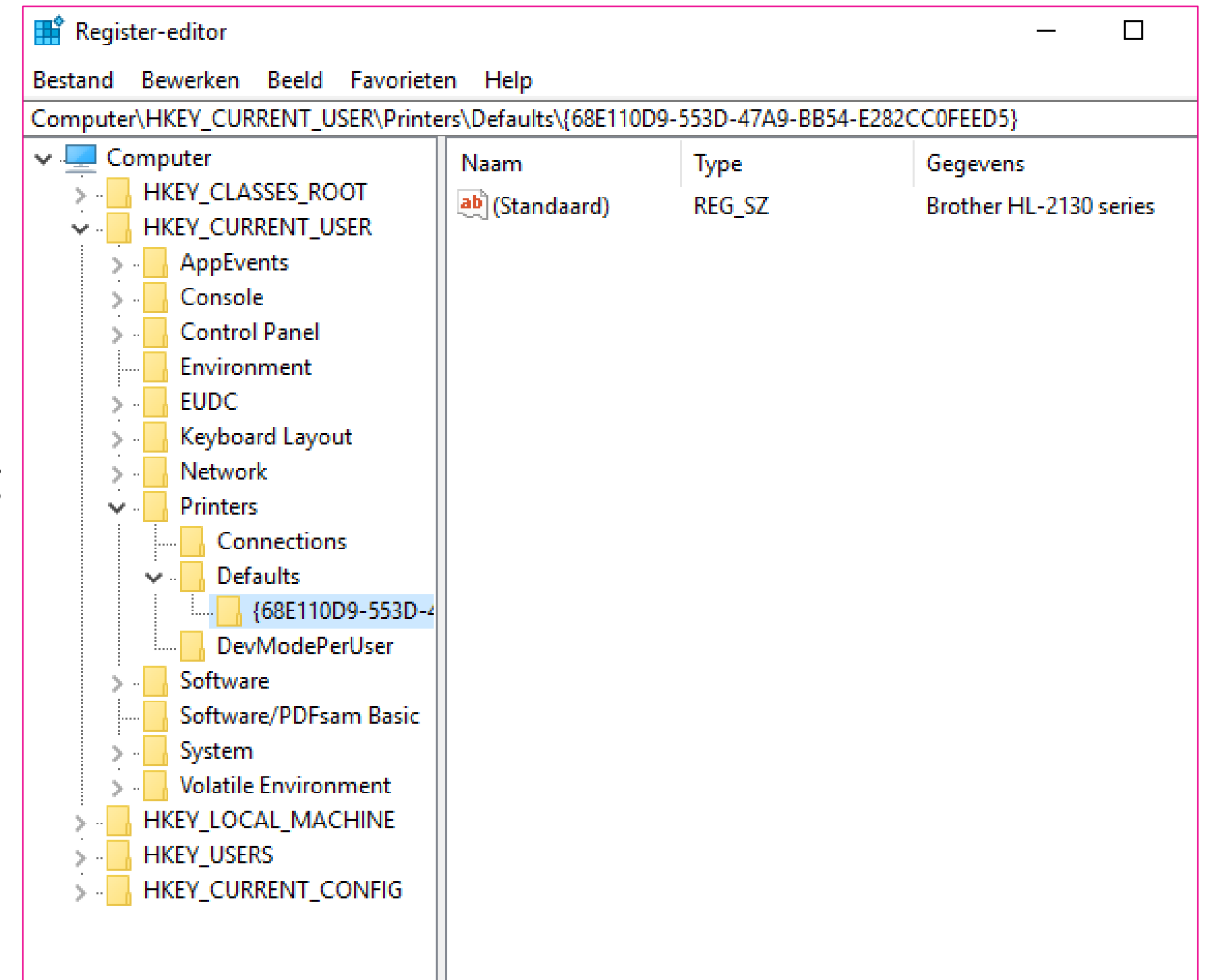
# Group Policy Settings

- Computer Configuration <> User Configuration
- Policies:
  - Software Settings: Applicaties en andere software
  - Windows Settings: Windows instellingen
    - Security
  - Administrative Templates (zie verder)
- Preferences:
  - GPP Group Policy Preferences
  - Instelling toepassen, maar gebruiker kan deze veranderen
    - Item Level Targeting -> instellingen toepassen volgens uitgebreide query tot op individuele gebruiker



# Registry

- DB dat instellingen van het Windows OS (SW en HW) en applicaties, die het registry gebruiken, bewaart.
- Instellingen via
  - Key
    - Unieke code omtrent het type instelling
  - Value
    - De bijhorende waarde
- Openen via 'regedit'
  - Backup!



# Registry

---

- Onderverdeling via 5 secties
  - HKEY\_CLASSES\_ROOT
    - Gegevens voor algemeen gebruik, alle gegevens voor geregistreerde bestandstypen, gegevens voor programma's die gegevens kunnen uitwisselen.
  - HKEY\_CURRENT\_USER
    - Hierin worden gegevens geformuleerd die de gebruiker heeft ingesteld zoals geïnstalleerde software, netwerkinstellingen, toetsenbord en muis.
  - HKEY\_LOCAL\_MACHINE
    - Alle instellingen voor hardware en software worden hier beschreven: standaardconfiguratie, gegevens van aangesloten hardware, gebruikersgegevens en alle softwareconfiguraties.
  - HKEY\_ALL\_USERS
    - De sleutel met alle gebruikersprofielen.
  - HKEY\_CURRENT\_CONFIG
    - Alle huidige instellingen.

# Administrative Templates

---

- Vroeger (tot 2008 r2): ADM bestanden
- ADMX bestanden (XML syntax) → instellingen
- ADML bestanden → vertalingen
- C:\Windows\PolicyDefinitions <> SYSVOL\PolicyDefinitions
- **Tattooing**: eenmaal een instelling gewijzigd, wijzigt hij niet automatisch terug naar de originele als de GPO verwijderd wordt
- Overzicht van enkele instellingen:
  - 1903: <https://www.microsoft.com/en-us/download/details.aspx?id=58495>
  - 1909: <https://www.microsoft.com/en-us/download/100591>
  - 20H2: <https://www.microsoft.com/en-us/download/details.aspx?id=102157>
  - W11 21H2: <https://www.microsoft.com/en-us/download/103507>



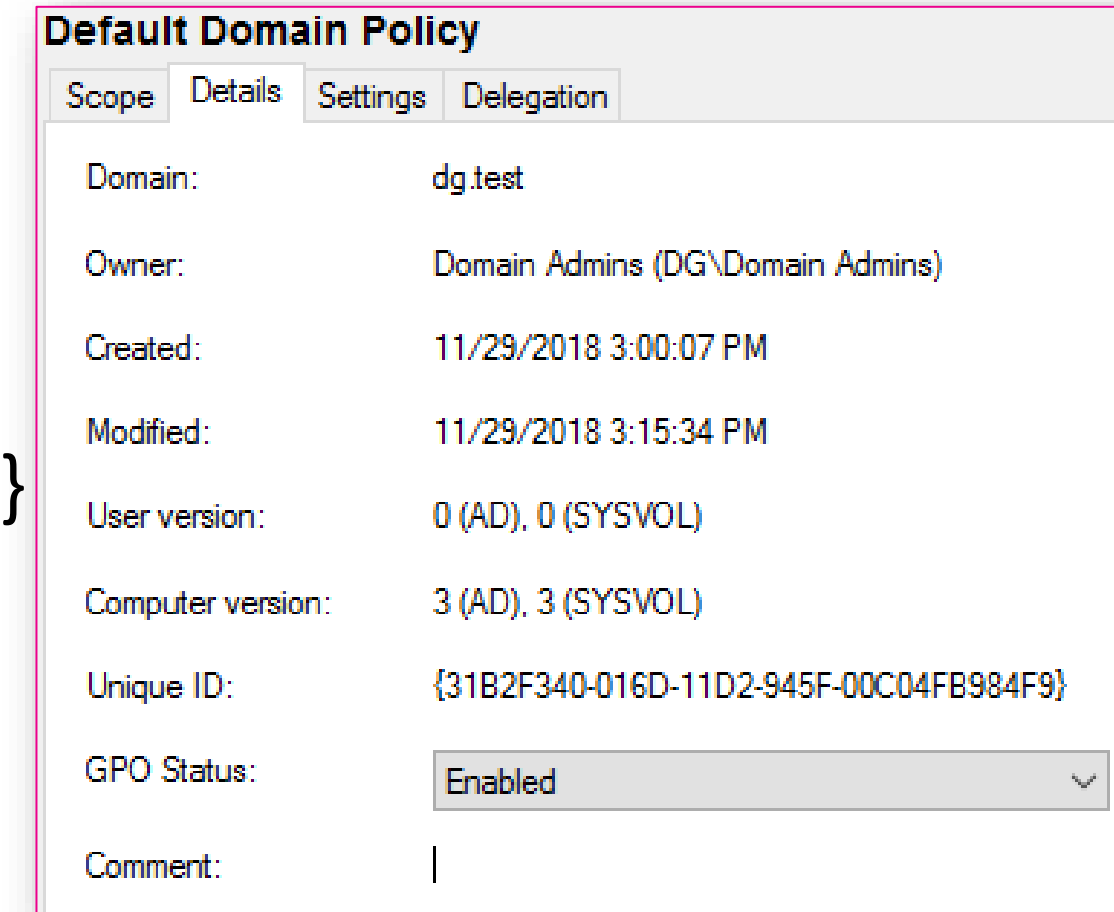
BEHEER

# Default Policies

- Default Domain Policy
  - Alle gebruikers- en computeraccounts
  - Paswoord, lockout en Kerberos
  - Domain GPO GUID {31B2F340-016D-11D2-945F-00C04FB984F9}
- Default Domain Controllers Policy
  - Alle domeincontrollers
  - Toewijzen van gebruikersrechten en Auditing
  - DC GPO GUID {6AC1786C-016F-11D2-945F-00C04FB984F9}

Herstel van deze default policies: dcpofix.exe

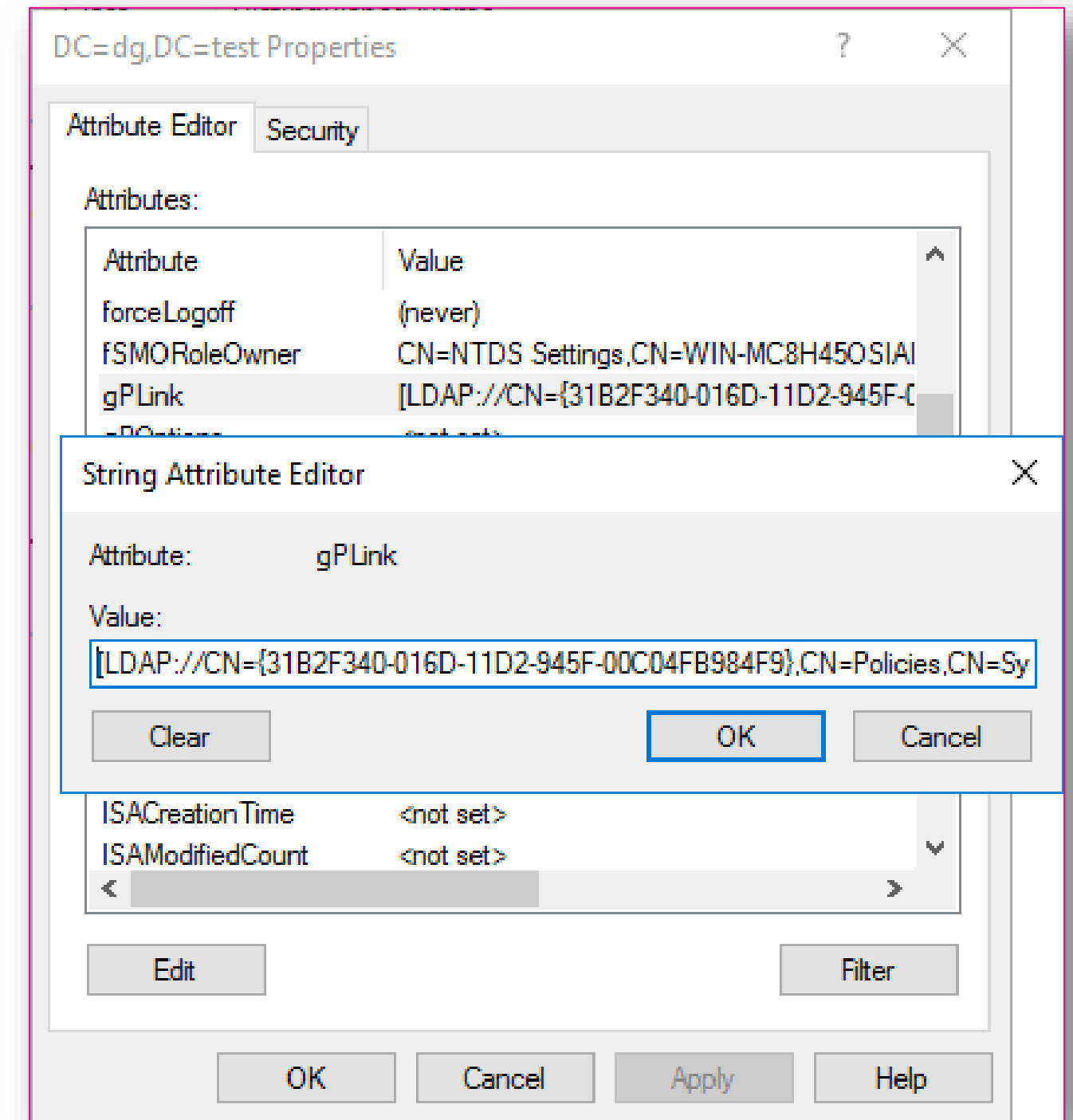
Best Practice: Niet gebruiken voor andere instellingen



Default Domain Policy			
Scope	Details	Settings	Delegation
Domain:	dg.test		
Owner:	Domain Admins (DG\Domain Admins)		
Created:	11/29/2018 3:00:07 PM		
Modified:	11/29/2018 3:15:34 PM		
User version:	0 (AD), 0 (SYSVOL)		
Computer version:	3 (AD), 3 (SYSVOL)		
Unique ID:	{31B2F340-016D-11D2-945F-00C04FB984F9}		
GPO Status:	Enabled		
Comment:			

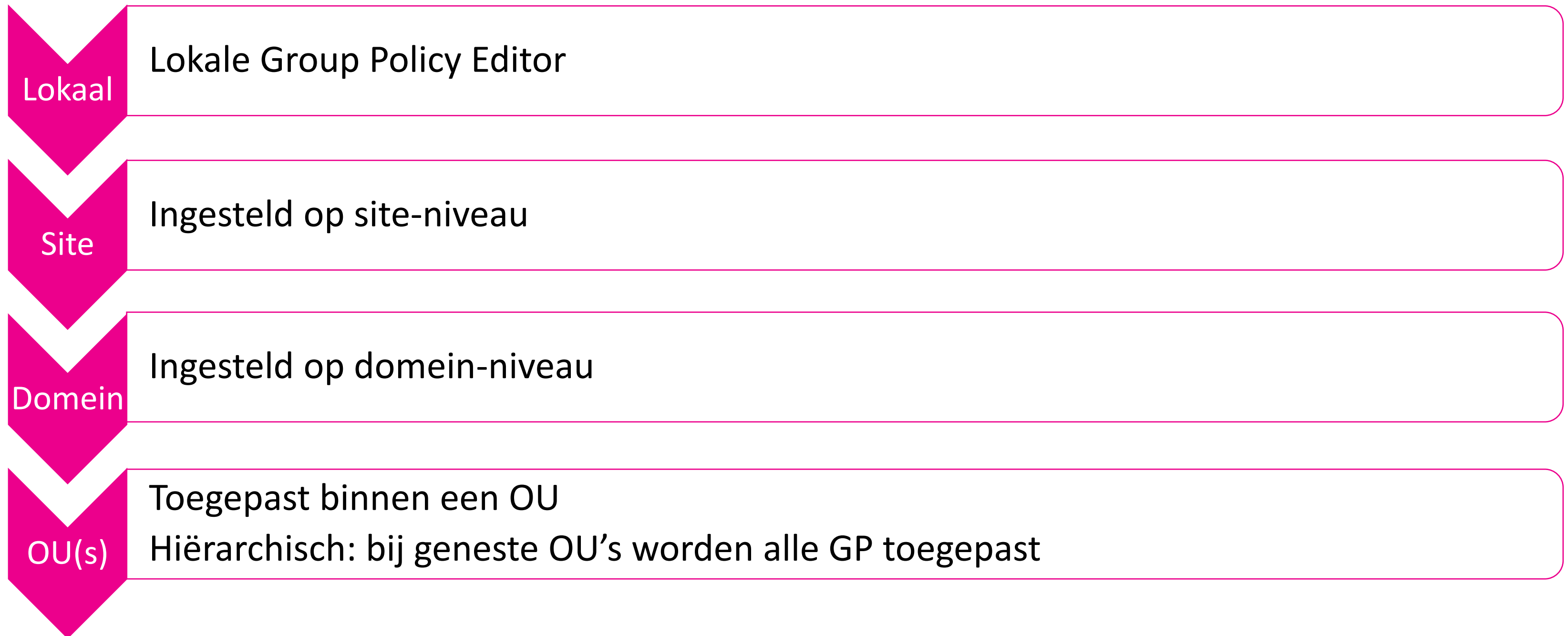
# Linken

- Eenmaal een GPO gecreëerd is, dienen we deze te linken aan een container object (site, domein, OU)
- Link wordt bewaard in het container object
  - In het gPLink attribuut



# Scope/volgorde

---



Als dezelfde instelling gewijzigd wordt, is de laatste instelling van toepassing!

# Security Group Filtering

- Default:
  - Authenticated Users
    - Read
    - Apply


Default Domain Policy

ScopeDetailsSettingsDelegation

Links

Display links in this location:dg.test


The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
 dg.test	No	Yes	dg.test

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name

 Authenticated Users

Add...

Remove

Properties

WMI Filtering

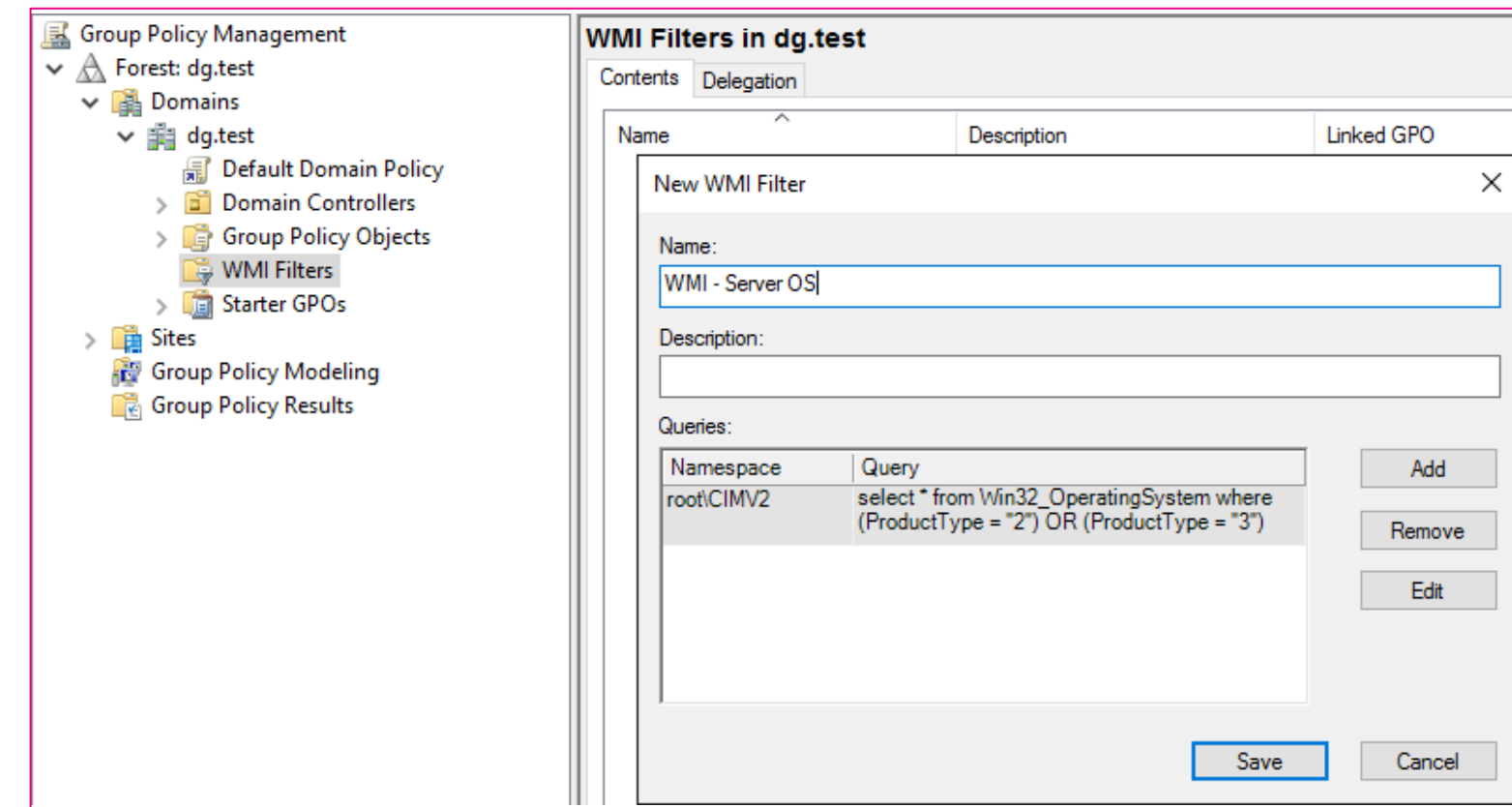
This GPO is linked to the following WMI filter:

<none>

Open

# WMI Filtering

- Toepassen op basis van computerkenmerken
  - Computer hardware en configuratie, gebruikersprofiel, environment settings, ...
- WMI is Microsoft z'n implementatie van CIM
  - Common Information Model
    - Een model om computer en netwerkobjecten te beschrijven
- WMI is deprecated -> CIM gebruiken waar mogelijk

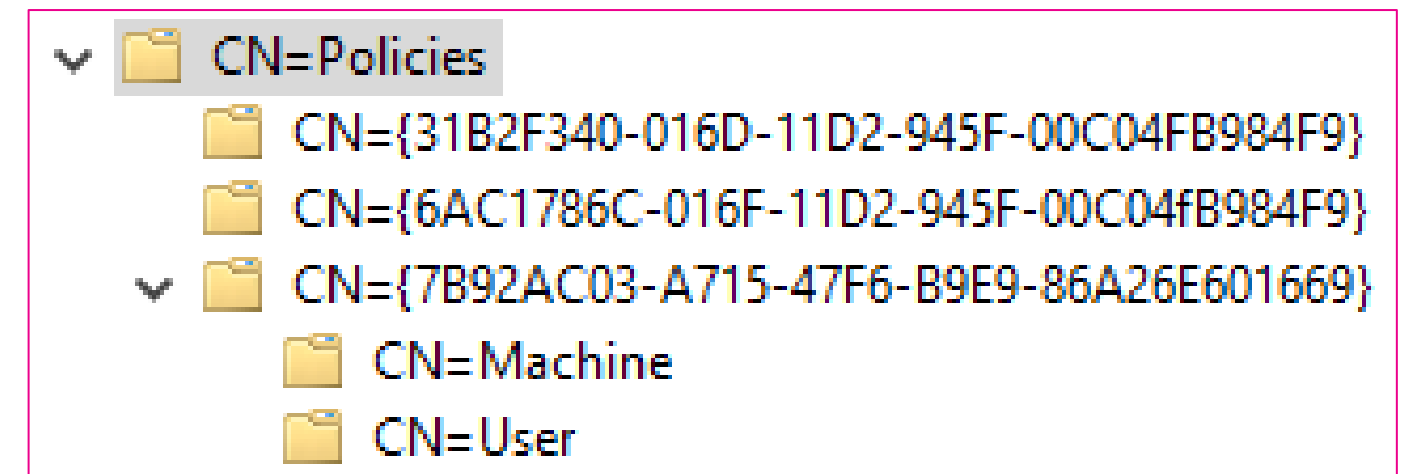


ProductType = 1 = Client OS  
ProductType = 2 = DC's  
ProductType = 3 = Server OS exclusief DC

# GPO ANATOMIE

# Hoe worden GPO's bewaard?

- GPO bestaat uit 2 onderdelen
  - GPC
    - Group Policy Container
    - GPO eigenschappen zoals versie info, status, ...
    - Wordt bewaard binnen AD
      - LDAP://CN={GUID},CN=Policies,CN=System,DC=domain,DC=TLD

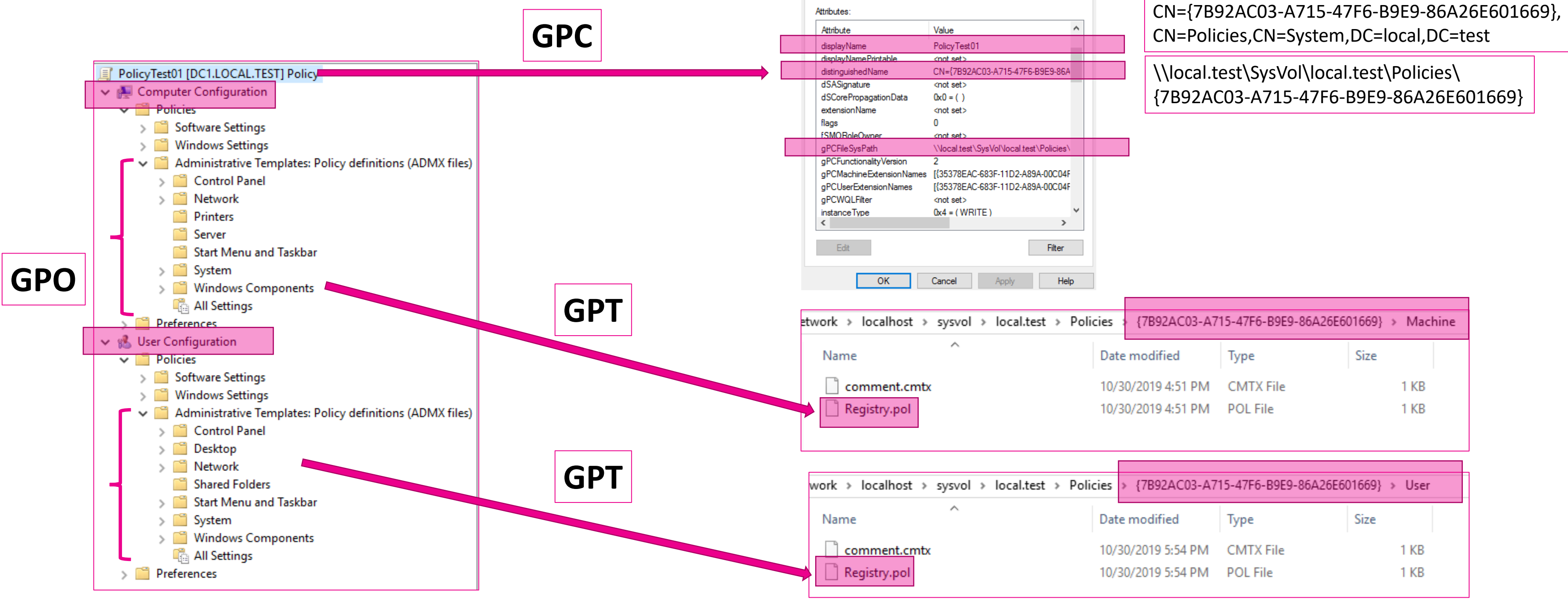


- GPT
  - Group Policy Template
  - Wordt bewaard binnen **SYSVOL**
    - \\domain\SYSVOL\domain.tld\Policies\{GUID}
  - Hierin zitten de eigenlijke instellingen van de GPO

network > localhost > sysvol > local.test > Policies > {31B2F340-016D-11D2-945F-00C04FB984F9} > {31B2F340-016D-11D2-945F-00C04FB984F9}				
Name	Date modified	Type	Size	
MACHINE	10/16/2019 4:56 PM	File folder		
USER	10/16/2019 4:41 PM	File folder		
GPT	10/16/2019 4:56 PM	Configuration sett...		1 KB



# Hoe worden GPO's bewaard? Voorbeeld



# Replicatie

---

- DC-DC
  - GPC → via AD replicatie
  - GPT → via DFS-R replicatie
- DC-CLIENT
  - Versie GPO op client bijgehouden
    - HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State
  - Bij opvragen vergeleken met versienr GPO
  - Zorgt ervoor dat de client niet telkens opnieuw de instelling moet ophalen en toepassen
  - Slow-link processing
    - Default: 500kbps
    - Bij een slow-link worden bepaalde zaken niet toegepast. Gedrag kan je aanpassen in:
      - Computer Configuration\Policies\Administrative Templates\System\Group Policy

# TOEPASSEN VAN GPO'S

# Wanneer wordt group policy toegepast? (1/3)



# Wanneer wordt group policy toegepast? (2/3)

---

- Standaard
  - Op werkstations en member servers
    - Policies worden gerefreshed om de 90 minuten
  - Op domain controllers
    - Policies worden gerefreshed om de 5 minuten
  - Om het netwerk niet te verzadigen met gelijktijdige refreshs
    - Er wordt een willekeurige offset interval toegevoegd aan deze refresh tijd
      - Tussen 0 en 30 minuten voor werkstations en member servers
      - 0 minuten voor domain controllers
- Manueel
  - Via het command: “gpupdate /force”

# Wanneer wordt group policy toegepast? (3/3)

- Per policy
  - Instellen van een refresh tijd in de policy zelf
    - Administrative templates -> System -> Group Policy -> Set Group Policy refresh interval for computers

Set Group Policy refresh interval for computers

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on: At least Windows 2000

Options:

This setting allows you to customize how often Group Policy is applied to computers. The range is 0 to 44640 minutes (31 days).

Minutes:

This is a random time added to the refresh interval to prevent all clients from requesting Group Policy at the same time.

The range is 0 to 1440 minutes (24 hours)

Minutes:

Help:

This policy setting specifies how often Group Policy for computers is updated while the computer is in use (in the background). This setting specifies a background update rate only for Group Policies in the Computer Configuration folder.

In addition to background updates, Group Policy for the computer is always updated when the system starts.

By default, computer Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes.

If you enable this setting, you can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

If you disable this setting, Group Policy is updated every 90 minutes (the default). To specify that Group Policy should never be updated while the computer is in use, select the "Turn off

OK Cancel Apply

# GPO TROUBLESHOOTING

# Group Policy Infrastructure Status

- Status van de group policies en de consistentie over alle domain controllers

Group Policy Management

Forest: local.test

Domains

> local.test

Sites

Group Policy Modeling

Group Policy Results

local.test

StatusLinked Group Policy ObjectsGroup Policy InheritanceDelegation

This page shows the status of Active Directory and SYSVOL (DFS) replication for this domain as it relates to Group Policy.

Status Details

⌵

DC1.local.test is the baseline domain controller for this domain.

Site Name	Default-First-Site-Name
IP Address	fe80::a81f:a8fa:33f4:7a13%4
GPOs	3

?

⌵0 Domain controller(s) with replication in progress

✓

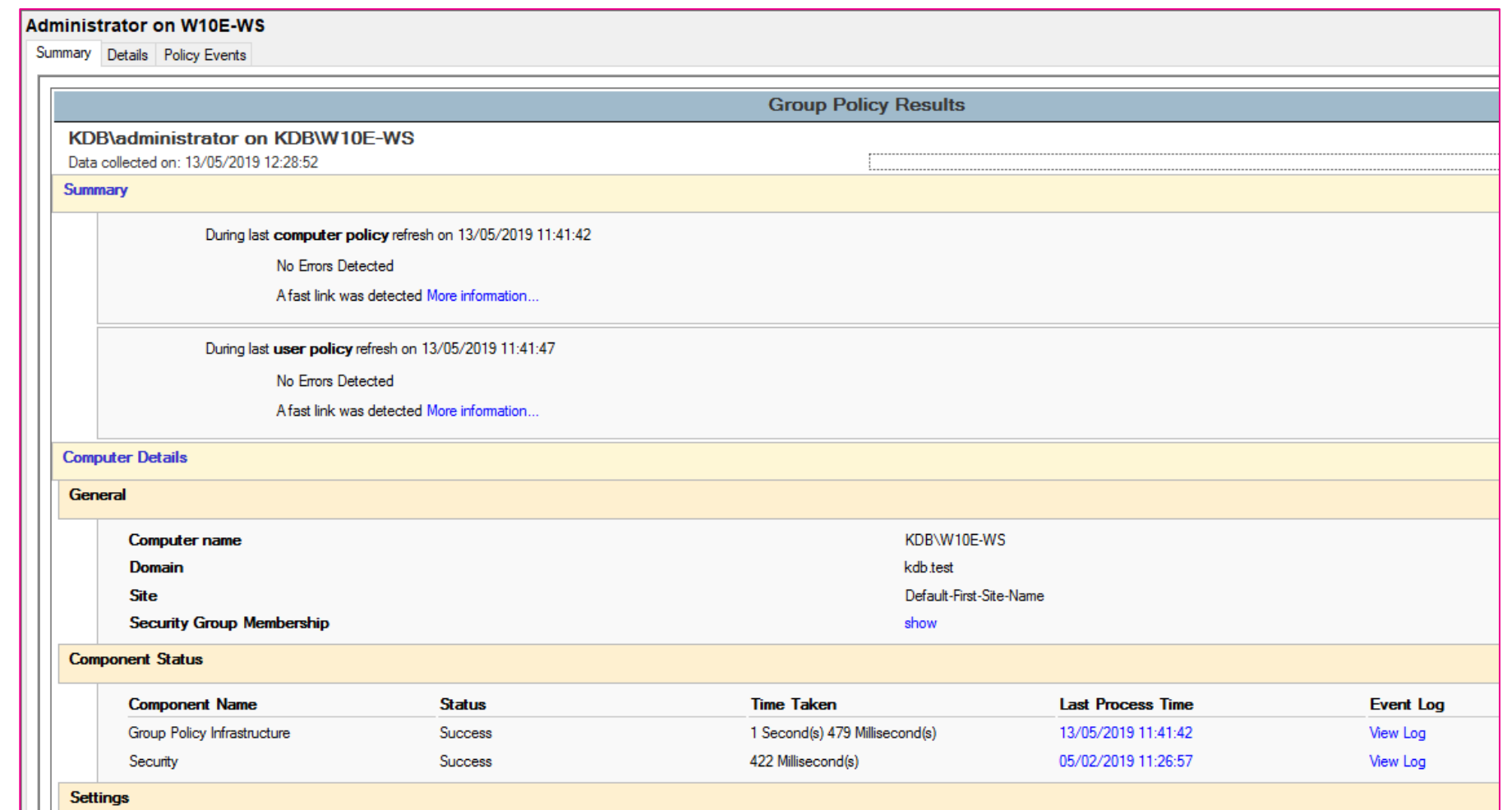
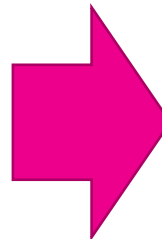
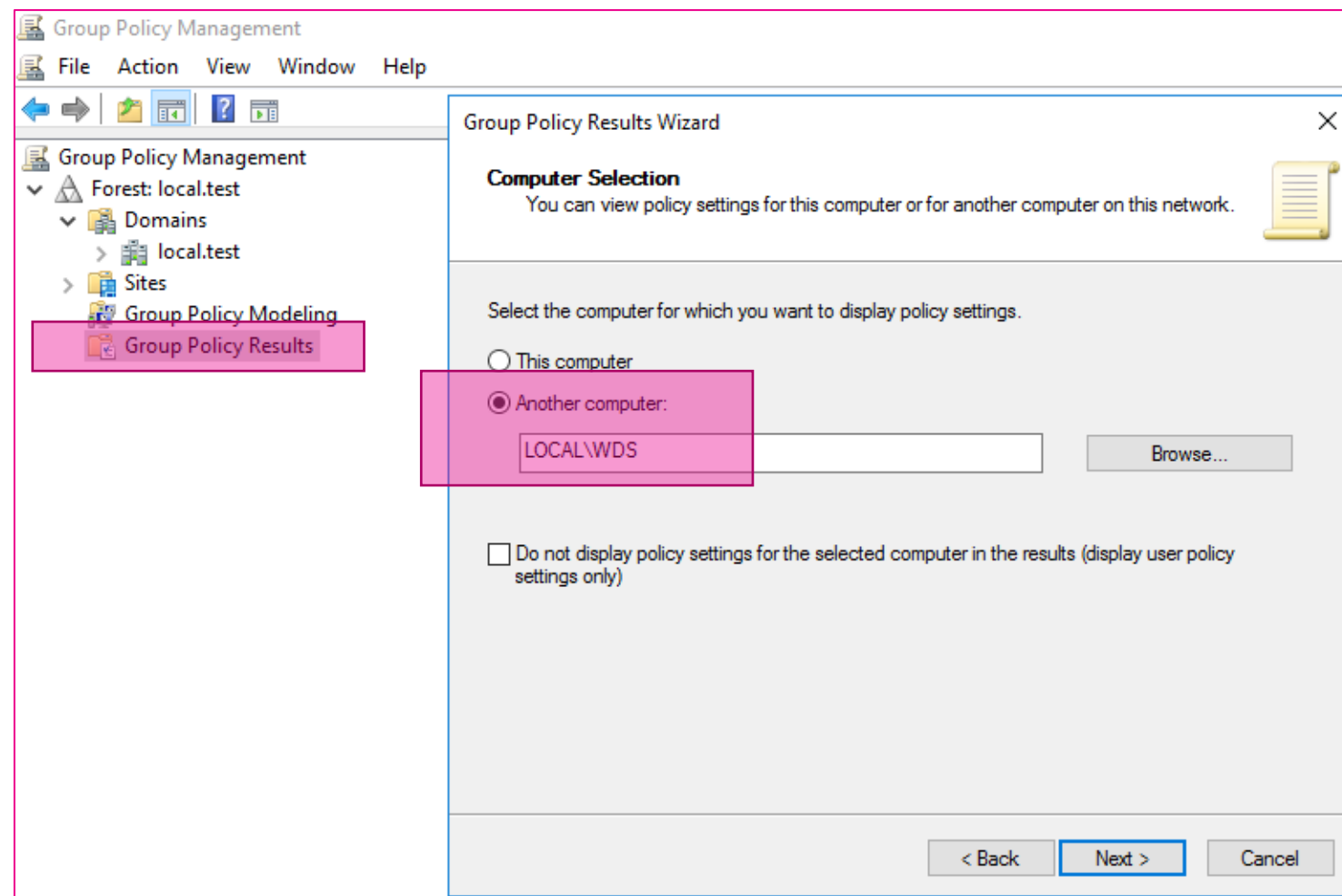
⌵1 Domain controller(s) with replication in sync

Name (FQDN)	Site Name	IP Address
DC2.local.test	Default-First-Site-Name	192.168.200.151



# Group Policy Results Wizard

- Tool om de RSoP te bekomen van een gebruiker of computer
  - Resultant Set of Policies
  - Een overzicht van alle toegepaste policies voor een gebruiker of computer



# GPRresult

---

- CLI
  - “gprresult /r”
    - RSoP samenvatting
  - “gprresult /v”
    - RSoP gedetailleerde informatie
  - “gprresult /v /USER username”
    - RSoP informatie voor een specifieke gebruiker
  - “gprresult /v /S computernaam”
    - RSoP informatie voor een bepaalde computer
  - “gprresult /H”
    - RSoP samenvatting in HTML formaat

# Juiste GPO instelling vinden

- Filteren van instellingen

The screenshot shows the 'Filter Options' dialog box, which is used to configure filters for Administrative Templates. The dialog has a title bar with a close button (X). Below the title bar, there is a funnel icon and a description: 'Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.' Below this, there is a section titled 'Select the type of policy settings to display.' which contains three dropdown menus: 'Managed:' (set to 'Yes'), 'Configured:' (set to 'Any'), and 'Commented:' (set to 'Any'). Below these, there is a checkbox labeled 'Enable Keyword Filters' which is checked. Under this checkbox, there is a text box labeled 'Filter for word(s):' containing the word 'security', and a dropdown menu set to 'Any'. Below the text box, there is a 'Within:' label followed by three checkboxes: 'Policy Setting Title' (checked), 'Help Text' (checked), and 'Comment' (checked). Below this, there is a checkbox labeled 'Enable Requirements Filters' which is unchecked. Under this checkbox, there is a section titled 'Select the desired platform and application filter(s):' which contains a dropdown menu set to 'Include settings that match any of the selected platforms.' and a list of checkboxes for various platforms and applications: BITS 1.5, BITS 2.0, BITS 3.5, BITS 4.0, Internet Explorer 10, Internet Explorer 11, Internet Explorer 3, and Internet Explorer 4. To the right of the list, there are two buttons: 'Select All' and 'Clear All'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Filter Options

Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.

Select the type of policy settings to display.

Managed: Yes Configured: Any Commented: Any

☒ Enable Keyword Filters

Filter for word(s): security Any

Within: ☒ Policy Setting Title ☒ Help Text ☒ Comment

☐ Enable Requirements Filters

Select the desired platform and application filter(s):

Include settings that match any of the selected platforms.

☐ BITS 1.5  
☐ BITS 2.0  
☐ BITS 3.5  
☐ BITS 4.0  
☐ Internet Explorer 10  
☐ Internet Explorer 11  
☐ Internet Explorer 3  
☐ Internet Explorer 4

Select All  
Clear All

OK Cancel

# Event Viewer (1/2)

- Event Viewer
  - Logfiles van alle gebeurtenissen op een Windows omgeving
  - Per categorie

**Event Viewer (Local)**

**Overview and Summary**

**Overview**

To view events that have occurred on your computer, select the appropriate source, log or custom view node. The selected node contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

**Summary of Administrative Events**

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊕ Critical	-	-	-	1	1	2
⊕ Error	-	-	-	7	7	31
⊕ Warning	-	-	-	75	75	280
⊕ Information	-	-	-	236	236	966
⊕ Audit Success	-	-	-	268	268	3,947
⊕ Audit Failure	-	-	-	0	0	2

**Recently Viewed Nodes**

Name	Description	Modified	Created
Applications and Service...	N/A	11/1/2019 2:41:07 PM	2/6/2018 8:49:20 PM

# Event Viewer (2/2)

The screenshot displays the Windows Event Viewer interface. On the left, the 'Event Viewer' tree is expanded to 'GroupPolicy > Operational'. The main pane shows a list of 18 events, all of level 'Information' and source 'GroupPolicy (Microsoft-Windows-GroupPolicy)', occurring on 11/1/2019 at 2:42:41 PM. The details pane for event 6339 is open, showing the message 'Group Policy Winlogon Start Shell handling completed.' and various metadata.

Level	Date and Time	Source	Event ID	Task Category
Information	11/1/2019 2:42:41 PM	GroupPolicy (Microsoft-Win...	6339	None
Information	11/1/2019 2:42:41 PM	GroupPolicy (Microsoft-Win...	5324	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5315	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5117	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5351	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	6338	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	8001	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5320	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5320	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5320	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5313	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5312	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5126	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5257	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5017	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	4017	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5314	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5327	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	4257	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	4126	None
Information	11/1/2019 2:42:40 PM	GroupPolicy (Microsoft-Win...	5311	None

Event 6339, GroupPolicy (Microsoft-Windows-GroupPolicy)

General Details

Group Policy Winlogon Start Shell handling completed.

Log Name: Microsoft-Windows-GroupPolicy/Operational  
Source: GroupPolicy (Microsoft-Win... Logged: 11/1/2019 2:42:41 PM  
Event ID: 6339 Task Category: None  
Level: Information Keywords:  
User: SYSTEM Computer: DC1.local.test  
OpCode: Info  
More Information: [Event Log Online Help](#)

# GPO EXTRA

# Software installeren via GPO

---

- Enkel .msi install (.mst transform en .msp patch)
  - Er bestaan converters van .exe naar .msi
- Beschikbaar maken via netwerkshare – leesrechten!
- Assign

Users: installatie van het programma gebeurt zodra de gebruiker op de snelkoppeling klikt

Computer: automatische installatie na herstart
- Publish

Users: programma te installeren via configuratiescherm of (instelbaar) als de gebruiker een bestand probeert te openen die aan die applicatie gekoppeld is.

Computer: publish niet mogelijk

# Scheduling

Task Scheduler



# Task Scheduler?

---

- Laat je toe om routinetaken of andere automatisch uit te voeren op een gekozen computer.
  - Taken
    - Applicatie starten
    - Email versturen
    - Boodschap tonen op scherm
    - Script starten
  - A.d.h.v. triggers
    - Bijvoorbeeld
      - Dagelijks om 3:00 uur
      - Wanneer een specifieke event plaatsvindt
      - Wanneer een gebruiker aanmeldt
      - Wanneer het systeem opstart
      - ...

# Bronnen

---

- Microsoft documentatie: <https://docs.microsoft.com/en-us/windows/win32/taskschd/task-scheduler-start-page>

Vragen?