

Netwerkbeheer met Windows Server 2019  
Deel 2



# **Netwerkbeheer met Windows Server 2019**

## **Deel 2**

**Beheer en beveiliging op een LAN**

Jan Smets

ISBN 978 90 5752 410 3 / NUR 124

Omslagontwerp: Proforma, Barcelona  
Redactie, opmaak en zetwerk: Henk Pel, Zeist

© 2019 Brinkman Uitgeverij, Amsterdam

Gehele of gedeeltelijke overneming of reproductie van de inhoud van deze uitgave, op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van de auteursrecht-  
hebbende is verboden, behoudens de beperkingen bij de wet gesteld. Het verbod betreft  
ook gehele of gedeeltelijke bewerking. De uitgever is met uitsluiting van ieder ander ge-  
rechtigd de door derden verschuldigde vergoedingen voor kopiëren, als bedoeld in artikel  
17 Auteurswet 1912 en in het KB van 20 juni 1974 (Stb. 351, 1974) ex artikel 16b Auteurswet  
1912, te innen en/of daartoe in en buiten rechte op te treden.

Correspondentie inzake overneming of reproductie richten aan:  
Brinkman Uitgeverij, Postbus 59686, 1040 LD Amsterdam  
[www.brinkman-uitgeverij.nl](http://www.brinkman-uitgeverij.nl)  
tel. 020-4120970  
e-mail: [brinkman@brinkman-uitgeverij.nl](mailto:brinkman@brinkman-uitgeverij.nl)

*Zon, maan en sterren,  
die schijnen van heel verre  
maar Madeliefje, altijd blij,  
die schijnt van heel dichtbij*

GUUS KUIJER



# Inhoud

<b>0</b>	<b>Inleiding</b>	<b>1</b>
0.0	In dit hoofdstuk	1
0.1	Dit boek	1
<b>1</b>	<b>Group policies</b>	<b>5</b>
1.0	In dit hoofdstuk	5
1.1	Inzicht	6
1.2	Policies in Group Policy Objects	18
1.3	Blokkeren en forceren	37
1.4	Policies bij PoliForma BV	51
1.5	Toepassingen van group policies in een AD domain	55
<b>2</b>	<b>Groepen</b>	<b>63</b>
2.0	In dit hoofdstuk	63
2.1	Overzicht	64
2.2	Standaard ingebouwde groepen	67
2.3	De basisgroepsstructuur bij PoliForma BV	87
<b>3</b>	<b>De toegangsbeveiliging tot een netwerk</b>	<b>101</b>
3.0	In dit hoofdstuk	101
3.1	Password en Account Policies	101
3.2	Password Policy	106
3.3	Account Lockout Policy	118
3.4	Kerberos Policy	126
<b>4</b>	<b>Structureel beveiligd netwerkbeheer</b>	<b>141</b>
4.0	In dit hoofdstuk	141
4.1	Gebruikersrechten	142
4.2	Structureel beveiligd netwerkbeheer bij PoliForma BV	150
4.3	Werkstations	159
4.4	Het user account van de domain Administrator	167
<b>5</b>	<b>De beveiligde toegang tot netwerkobjecten</b>	<b>169</b>
5.0	In dit hoofdstuk	169
5.1	Autorisatie	170
5.2	De toegang tot shared folders	171
5.3	Gebruikersgemak	211
5.4	DFS Replication in PoliForma.local	233
5.5	De toegang tot shared printers	250
5.6	De effectieve permissie	260
5.7	De toegang tot andere netwerkobjecten	263

<b>6</b>	<b>Backup en recovery</b>	<b>267</b>
6.0	In dit hoofdstuk	267
6.1	Ongestoorde file service	268
6.2	Backup-software en -hardware	270
6.3	Geagendeerd backups maken	274
6.4	Recovery	293
6.5	Eenmalige backups	307
6.6	Een set geagendeerde backups aanpassen	319
<b>7</b>	<b>Beveiliging tegen Malware en Software installation</b>	<b>327</b>
7.0	In dit hoofdstuk	327
7.1	Virusprotectie op DC PFSV1	329
7.2	F-Prot op DC PFSV1 voor de werkstations	344
7.3	Software-installatie op werkstations	350
7.4	F-Prot op werkstation PFWS1	357
7.5	Software de-installeren	364
7.6	Centraal beheer	368
<b>8</b>	<b>Gebruik en beheer op afstand met een VPN</b>	<b>371</b>
8.0	In dit hoofdstuk	371
8.1	VPN-server PFSV1	373
8.2	De VPN-client PFWS1	394
8.3	De VPN-verbinding gebruiken	405
<b>9</b>	<b>Controle over uw netwerk</b>	<b>411</b>
9.0	In dit hoofdstuk	411
9.1	Controle over de toegang tot een machine	412
9.2	Controle over de gebeurtenissen op een machine	416
9.3	De conditie van een machine evalueren	446
<b>10</b>	<b>Updates</b>	<b>469</b>
10.0	In dit hoofdstuk	469
10.1	Updates voor Windows Server 2019	471
10.2	WSUS: updates voor Windows 10-werkstations	478
10.3	Windows 10 op de werkstations	518
<b>A</b>	<b>Overname</b>	<b>521</b>
A.0	In deze bijlage	521
A.1	Uitgangssituatie	521
A.2	Verandering	521
A.3	Opdracht	524
A.4	Op te leveren producten	526
	<b>Register</b>	<b>527</b>



# Lijst van practica en opdrachten

- 1 Group policies 5**
  - 1.2.1 Policies in GPO's 9
  - 1.3.1 Verschil maken 37
  - 1.4.1 Groepsbeleid 52
  - 1.5.1 Vooraf 55
  - 1.5.2 Groepsbeleid ten aanzien van File Explorer 56
  - 1.5.3 Groepsbeleid ten aanzien van Internet Explorer 11 57
  - 1.5.4 Groepsbeleid ten aanzien van Microsoft Edge 59
  - 1.5.5 Firewalls 61
  
- 2 Groepen 63**
  - 2.2.1 Standaardgroepen 67
  - 2.3.1 Groepen aanmaken 88
  
- 3 De toegangsbeveiliging tot een netwerk 101**
  - 3.2.1 Wachtwoordinstellingen 107
  - 3.3.1 Inbraakbeveiliging 119
  - 3.4.1 Kerberos Policy 133
  
- 4 Structureel beveiligd netwerkbeheer 141**
  - 4.1.1 Rechten 142
  - 4.2.1 Structureel beheer 151
  - 4.2.2 Mutaties 159
  - 4.3.1 Computers lid maken 159
  - 4.3.2 Disablen en resetten 162
  
- 5 De beveiligde toegang tot netwerkobjecten 169**
  - 5.2.1 De afdelingsfolder voor de afdeling Administratie 171
  - 5.2.2 Owner 203**
  - 5.2.3 Afdelingsmappen delen 210
  - 5.3.1 Namespace 212
  - 5.3.2 Ingangen in de namespace 230
  - 5.3.3 Flipse 231
  - 5.3.4 Prikbord 232
  - 5.4.1 Bestandsrepliatie 233
  - 5.4.2 DataPFSV2 248
  - 5.4.3 Test bestandsrepliatie 250
  - 5.5.1 PFPR1 251
  - 5.5.2 Werkplaats 260
  - 5.6.1 Effectief 261

- 6 Backup en recovery 267**
  - 6.2.1 Configuratie en installatie 271
  - 6.3.1 Geagendeerd 274
  - 6.4.1 Restore 293
  - 6.4.2 System recovery 301
  - 6.5.1 Tussendoor 308
  - 6.6.1 Aanpassen 319
  - 6.6.2 Documenteren 324
  
- 7 Beveiliging tegen malware en software installatie 327**
  - 7.1.1 F-Prot op PFSV1 329
  - 7.2.1 Klarzetten 345
  - 7.3.1 Uitrollen via een GPO 352
  - 7.4.1 F-Prot op PFWS1 357
  - 7.5.1 De-installeren 365
  
- 8 Gebruik en beheer op afstand met een VPN 371**
  - 8.1.1 VPN installeren 374
  - 8.1.2 VPN configureren 383
  - 8.2.1 VPN op PFWS1 394
  - 8.3.1 VPN gebruiken 405
  
- 9 Controle over uw netwerk 411**
  - 9.1.1 Verbonden 413
  - 9.2.1 Logs en Events 417
  - 9.2.2 Audit 436
  - 9.3.1 Diagnose 448
  - 9.3.2 Prestatietellers 459
  - 9.3.3 Tellers bewaken 460
  
- 10 Updates 469**
  - 10.1.1 Updates Windows Server 2019 installeren 472
  - 10.2.1 Voorbereidingen 479
  - 10.2.2 WSUS-installatie 482
  - 10.2.3 WSUS-configuratie 489
  - 10.2.4 WSUS beheren 499
  - 10.2.5 Windows Update op de werkstations 503
  - 10.2.6 Goedkeuren 512
  - 10.3.1 PFWS1 bijwerken 518

# o Inleiding

## o.o In dit hoofdstuk

In dit inleidende hoofdstuk komen de volgende zaken aan de orde.

- Waarover gaat dit boek?
- De eindtermen die aan dit boek ten grondslag liggen.
- Veronderstelde voorkennis.
- Conventies in dit boek.
- Hoe u dit boek kunt doorwerken.
- Extra materiaal bij dit boek.

## o.1 Dit boek

Dit boek is het tweede van een serie boeken over netwerkbeheer met Windows Server 2019 en Windows 10. Dit deel behandelt de elementaire leerstof die voor het beheren en beveiligen van een client/server-bedrijfsnetwerk nodig is. Daarbij ligt in dit deel de nadruk op de beveiliging. Vandaar de ondertitel: Beheer en beveiliging op een LAN.

### De boekenserie

De boekenserie Netwerkbeheer met Windows Server 2019 bestaat uit de volgende delen:

- Deel 1 *Inrichting en beheer op een LAN*
- Deel 2 *Beheer en beveiliging op een LAN*

### Beginsituatie voor dit deel

Deel 2 bouwt voort op deel 1. Als beginsituatie voor de practica en opdrachten in dit deel wordt dus de eindsituatie van deel 1 gebruikt.

### Onderwerpen

Onder de elementaire leerstof moet u in dit deel de volgende onderwerpen verstaan:

- Het kunnen toepassen van group policies (hoofdstuk 1).
- Het gebruik van groepen en met name de groepen voor de beveiliging (hoofdstuk 2).
- De beveiliging van de toegang tot een netwerk (hoofdstuk 3).
- De wijze waarop u een netwerk structureel kunt beheren (hoofdstuk 4).
- Het beveiligen van de toegang tot netwerkobjecten (hoofdstuk 5).
- Het maken van backups en het uitvoeren van een recovery (hoofdstuk 6).
- De beveiliging tegen malware in een netwerk (hoofdstuk 7).
- Het gebruik van VPN-verbindingen voor eigen gebruik en beheer (hoofdstuk 8).

- De controle houden over een netwerk (hoofdstuk 9).
- Het distribueren van updates in een netwerk (hoofdstuk 10).

## Opleidingen

Voor HBO-opleidingen en MBO ICT-opleidingen waarin kennis van netwerkbeheer is vereist, zijn de delen 1 en 2 zonder meer in hun geheel nodig.

## Veronderstelde voorkennis voor dit deel

De behandeling van Windows Server 2019 veronderstelt een zekere voorkennis bij de lezer. Het gaat hierbij in het bijzonder om de volgende onderwerpen:

- Kennis van PC-hardware op het niveau van Digivaardig gevorderd of het ECDL (European Computer Driving License). Raadpleeg bijvoorbeeld [www.ecdl.nl](http://www.ecdl.nl). Denk hierbij aan zaken als processortypen, geheugen(typen), bussen, harde schijven, disk controllers en dergelijke.
- Kennis van en om kunnen gaan met het Windows 10-besturingssysteem op het niveau van Digivaardig gevorderd of het ECDL.
- Kennis van en om kunnen gaan met gangbare Windows-applicaties op het niveau van Digivaardig gevorderd of het ECDL.
- Kunnen surfen op, zoeken op en downloaden van het internet.
- Algemene netwerkkennis.
- Elementaire kennis van TCP/IPv4.
- De kennis die u aangereikt is in deel 1 *Inrichting en beheer op een LAN*. Dit deel bouwt daar immers op voort.

## U moet het doen

Voor het leren inrichten, beheren en beveiligen van een netwerk is theoretische kennis van het netwerkbesturingssysteem nodig. In dit boek is dat Windows Server 2019. Even belangrijk als theoretische kennis is echter praktische vaardigheid. Bij het uitvoeren van uw dagelijkse werkzaamheden als netwerkbeheerder moet u straks een boek als dit niet meer nodig hebben. U bent dan simpelweg niet productief genoeg. Praktische vaardigheid krijgt u door het te doen. Vandaar dat u in dit boek een groot aantal practica en opdrachten tegenkomt. U doet er verstandig aan deze daadwerkelijk uit te voeren. Bij de voortgang wordt dat ook verondersteld.

## Conventies in dit boek

- Windows Server 2019 Standard wordt in een Engelstalige edition gebruikt, Windows 10 in de Pro-edition en ook in een Engelstalige uitvoering.
- Volume-, map- en bestandsnamen worden in *cursief* weergegeven.
- Toetsen worden weergegeven in KLEINKAPITAAL.
- Schermtekst en keuzes in bijvoorbeeld dialoogvensters en uitschuiflijsten, namen van volumes, mappen en bestanden worden *cursief* weergegeven.
- Namen van objecten zoals machines, gebruikers en dergelijke worden *cursief* weergegeven.
- Letterlijk in te voeren tekst wordt *met deze cursieve letter* weergegeven.

- Afbeeldingen van schermen en dialoogvensters zijn afgedrukt met een resolutie van 1024 × 768.
- Afbeeldingen zijn per hoofdstuk opeenvolgend genummerd.
- Practica kunt u op twee manieren uitvoeren:
  - met behulp van de **Korte practicum instructies**: deze manier kunt u gebruiken als u denkt over voldoende kennis te beschikken over het practicumonderwerp. Een toelichting op de nodige begrippen vindt u steeds in de gedetailleerde practicumuitwerking;
  - met behulp van de **Gedetailleerde uitwerking van het practicum**: deze manier gebruikt u als u stap voor stap begeleid wilt worden en de bijbehorende theorie wilt bestuderen.
- Practica en opdrachten beginnen en eindigen met een grijze balk. Aan het begin van elk practicum of opdracht staat in de kantlijn een pictogram met de geschatte tijdsduur die nodig is voor de uitvoering van het practicum of de opdracht.



### Dit boek doorwerken

De practica en opdrachten uit dit boek werkt u het handigst door met behulp van virtuele machines. Virtuele machines stellen wat hogere eisen aan de processor-snelheid, de grootte van het intern geheugen en de beschikbare schijfcapaciteit. Geadviseerd wordt om een PC of laptop te gebruiken met de volgende specificaties. Het merk is niet zo zeer van belang.

- Intel Core i7 processor;
- 16 GB intern geheugen;
- 500 GB harde schijf of meer.

Voor welk virtualisatieproduct u kiest, is aan u. De meest gangbare – Hyper-V, VMware en VirtualBox – zijn allen bruikbaar.

### Extra materiaal voor de cursisten

Het extra materiaal voor de cursisten is beschikbaar via de website [www.netwerk-smets.nl](http://www.netwerk-smets.nl). Deze site is voor iedereen vrij toegankelijk.

Zoals bij deel 1 is ook bij deel 2 het volgende aanvullende materiaal beschikbaar:

- **Presentaties**

Voor elk hoofdstuk is een PowerPoint 2016-presentatie beschikbaar. Docenten/begeleiders kunnen deze gebruiken om de stof uit het desbetreffende hoofdstuk toe te lichten. Daarmee zijn cursisten voorbereid op wat hun tijdens de practica te wachten staat.

Ook voor lezers van dit boek die alleen werken, zijn die presentaties nuttig. Het levert hen een helikopterblik op het betreffende hoofdstuk.



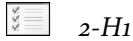
2\_H1

- **Werkbladen**

Het belang van goed documenteren kan niet voldoende benadrukt worden. Om u te helpen bij dat documenteren zijn per practicum en opdracht werkbladen beschikbaar. De werkbladen leren u hoe u het documenteren kunt aanpakken. Als bij een practicum werkbladen beschikbaar zijn, staat dit vermeld onder **Voor dit practicum heeft u nodig**. Daar wordt verwezen naar een Word 2016-document. Alle werkbladen zijn gebundeld af te drukken als een werkboek. U mag zoveel afdrukken maken als u wilt.

- **Toetsen**

Per hoofdstuk is er één toets beschikbaar. Met die toetsen kunt u bepalen hoe goed u de betreffende leerstof beheerst. De toetsen bestaan uit meerkeuzevragen. De toetsen maakt u op een computer. U krijgt na het maken van een vraag onmiddellijk het resultaat en de nodige feedback te zien. Aan het einde van de hoofdstukken waarbij een toets beschikbaar is, ziet u het onderstaande pictogram met daarbij de naam van de toets.



- **Instructievideo's**

Voor een aantal wat lastigere onderwerpen zijn er instructievideo's beschikbaar. Daar waar dat het geval is, staat in de kantlijn het onderstaande pictogram met daarbij de titel van de instructievideo.



- **Eindtoetsen**

Na het doorwerken van dit deel kunt u uzelf testen. Behalve een theorietoets die u op de gebruikelijke manier kunt maken, treft u in bijlage A van dit deel een eindproject aan. U mag dit eindproject zien als een praktisch proefexamen.

### **Extra materiaal voor de docenten**

Extra materiaal voor de docenten is beschikbaar via de website [www.brinkman-uitgeverij.nl](http://www.brinkman-uitgeverij.nl) achter het docentenaccount.

# 1 Group policies

## 1.0 In dit hoofdstuk



2\_H1

In deel 1 van deze boekenserie over netwerkbeheer zijn group policies al zijdelings ter sprake gekomen. Group policies leveren u uitgebreide mogelijkheden ten aanzien van het beheren en beveiligen van uw Windows Server 2019-netwerk. In dit hoofdstuk leert u group policies kennen en ermee omgaan. Daarbij concentreert u zich op het bepalen van de mogelijkheden van gebruikers op hun werkstations. Denk daarbij bijvoorbeeld aan het gebruik van het *Control Panel* en dergelijke.

Door de veelheid aan mogelijkheden met group policies kunt u snel in verwarring raken. Om dat te voorkomen, past u in de practica van dit hoofdstuk slechts twee policies toe. Die twee policies veroorzaken bovendien met opzet geheel verschillende effecten. Dat zorgt voor duidelijkheid. Met behulp van die twee policies leert u alle ins en outs van group policies kennen. Heeft u die kennis eenmaal onder de knie, dan kunt u dat in de slotopdrachten van dit hoofdstuk demonstreren.

U mist wellicht de twee tekeningen die de toestand van uw netwerk beschrijven aan het begin en aan het einde van dit hoofdstuk. Dat komt omdat group policies functioneel gezien niets wezenlijks aan uw netwerk veranderen. U beheert en/of beveiligt het slechts beter of anders.

Als u dit hoofdstuk heeft bestudeerd en de practica en de opdrachten heeft uitgevoerd, dan beschikt u over:

### A Kennis

- U kent de mogelijkheden van policies in een Windows Server 2019-netwerk (paragraaf 1.1).
- U kent het verschil tussen local policies en group policies gedefinieerd in een GPO (paragraaf 1.1).
- U kent de standaard aanwezige GPO's (paragraaf 1.2).
- U weet dat group policies in volgorde worden toegepast en overerven (paragraaf 1.2).
- U weet dat u policies kunt instellen voor gebruikers en computers (paragraaf 1.2).
- U weet dat u het effect van policies kunt controleren (paragraaf 1.2).
- U weet dat u de toepassing van GPO's kunt blokkeren en afdwingen (paragraaf 1.3).

## B Vaardigheden

- U kunt group policies op een machine handmatig verversen (practicum 1.2.1).
- U kunt een nieuw GPO aanmaken en dit op de juiste plaats in AD koppelen (practicum 1.2.1).
- U kunt policies in een GPO instellen (practicum 1.2.1).
- U kunt de GPO-informatie bekijken en interpreteren (practicum 1.2.1).
- U kunt voor een gebruiker de RSoP bepalen (practicum 1.2.1).
- U kunt een simpel inlogscript maken (practicum 1.3.1).
- U kunt de toepassing van GPO's op de juiste plaats blokkeren (practicum 1.3.1).
- U kunt de toepassing van GPO's afdwingen (practicum 1.3.1).
- U kunt met behulp van group policies in een geschikt GPO:
  - de mogelijkheden voor de gebruikers ten aanzien van File Explorer regelen;
  - de mogelijkheden voor de gebruikers ten aanzien van Internet Explorer 11 regelen;
  - de mogelijkheden voor de gebruikers ten aanzien van Microsoft Edge regelen;
  - de werking van de Windows (Defender) Firewall op de werkstations regelen.

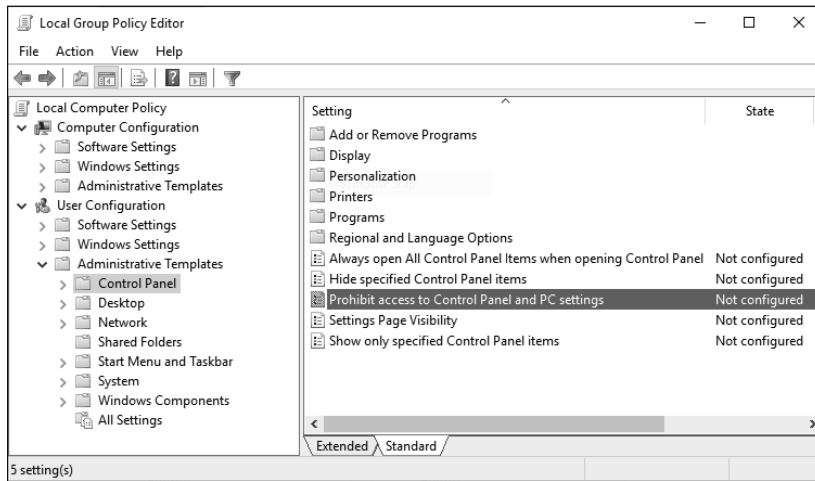
### 1.1 Inzicht

Met policies geeft u vorm aan beleid. Een **policy** is een beleidsregel. Het kan bijvoorbeeld een beleidsregel in een organisatie zijn die gebruikers het gebruik van het *Control Panel* op hun werkstations verbiedt. U regelt dat door de betreffende beleidsregel op hen van toepassing te laten zijn. In het vermelde geval is dat de policy *Prohibit access to Control Panel and PC settings* die u op de juiste plaats inschakelt. Policies zijn er te kust en te keur. Een onvolledige telling leert dat er in Windows Server 2019 ruim 3000 verschillende beschikbaar zijn. Bovendien installeren sommige applicaties ook nog hun eigen policies.

#### Local policies

Policies kunnen machine local worden ingesteld als **local policies** (afbeelding 1-1). Zij gelden op werkstations en member servers in een Windows Server 2019-netwerk en ook op standalone PC's. Belangrijk is het te weten dat local policies altijd als eerste worden uitgevoerd. Daarmee zijn local policies het minst krachtig. Straks zal blijken waarom dat zo is.





Afb. 1-1 Lokaal beleid voor het *Control Panel* op gebruikersniveau

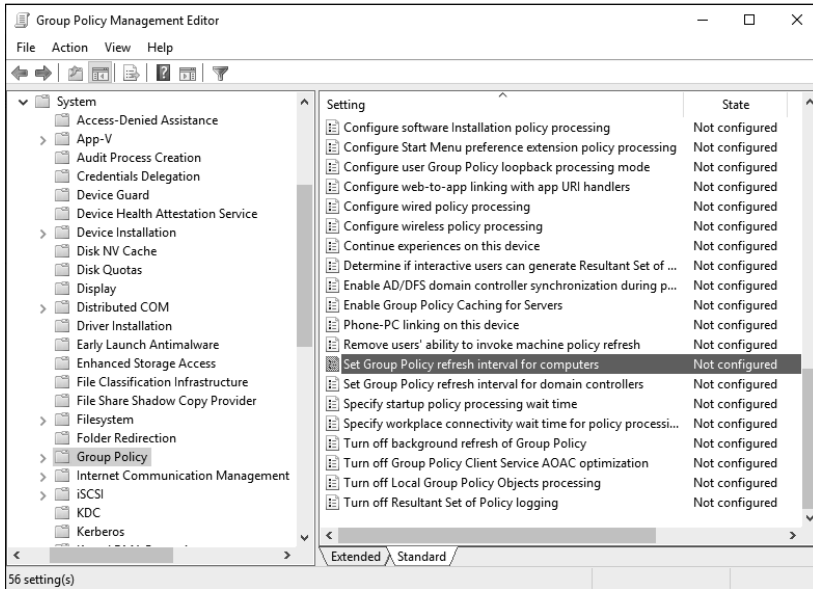
Voor u als netwerkbeheerder is het good practice het gebruik van local policies zoveel mogelijk te vermijden. Op Windows Server 2019-member- en -standalone-servers kunnen ze nog weleens toepasbaar zijn, op werkstations eigenlijk nooit. Local policies moet u namelijk per machine instellen. Van dat idee moet u inmiddels gruwen. Het staat immers haaks op de gedachte van centraal beheer.

## Group policies

In een Windows Server 2019-netwerk kunnen policies ook in AD (Active Directory) worden opgeslagen. Dat gebeurt in een **GPO** (Group Policy Object). Een GPO kan gekoppeld worden aan een site, een domain of een OU. Als een computer start en een gebruiker inlogt, wordt onderzocht welke GPO's op de computer en de gebruiker van toepassing zijn. Vervolgens worden de policies uit die GPO's in volgorde toegepast: eerst die op site-niveau, dan die op domain-niveau, dan die op OU-niveau. Deze volgorde van uitvoering is allesbepalend voor het uiteindelijke netto-effect van een policy. Uit het bovenstaande moet verder duidelijk zijn dat u voor het beheer van group policies twee tools nodig heeft: een om de GPO's te beheren en een om de policies in een GPO in te stellen.

## Group policies verversen

Group policies worden niet alleen bij het starten en inloggen toegepast. Op DC's worden ze standaard elke 5 minuten verversd. Op member servers en Windows 10-werkstations gebeurt dat elke 90 minuten. U kunt dit wijzigen. Waarin? In policies natuurlijk (afbeelding 1-2).



Afb. 1-2 Voor werkstations en member servers en daaronder voor DC's

Altijd kunt u het verversen van group policies op een machine forceren. U doet dit door in het venster *Windows PowerShell* of *Command Prompt* het commando `gpupdate /force` uit te voeren. Laat u de parameter `/force` weg, dan worden alleen wijzigingen toegepast. Meestal is dat voldoende.

### De mogelijkheden van group policies

Group policies geven u zoals vermeld veel mogelijkheden. De belangrijkste zijn:

- U kunt er de mogelijkheden van gebruikers op werkstations mee regelen.
- U kunt er start-, inlog-, shutdown- en uitlogs-scripts mee toewijzen.
- U kunt er software mee publiceren en toewijzen aan gebruikers en/of computers.
- U kunt er de functionaliteit van toepassingen als File Explorer, Microsoft Edge en Internet Explorer mee regelen.
- U kunt er gebruikersrechten mee instellen.

Van al deze mogelijkheden komen in dit hoofdstuk slechts enkele aan de orde. In de verdere leerstof van dit deel volgt meer, veel meer zelfs.

## 1.2 Policies in Group Policy Objects

In deze paragraaf leert u hoe u met group policies moet omgaan in een netwerk als dat van PoliForma BV. Ook leert u de beide beheertools voor group policies kennen. Ten gevolge van de installatie van AD is de beheertool *Group Policy Management* automatisch geïnstalleerd op de DC's *PFSV1* en *PFSV2*. Deze beheertool is beschikbaar in het menu *Tools* van de *Server Manager*. Het is deze beheertool die u gebruikt om met group policies om te gaan.



90 min.

## Practicum 1.2.1: Policies in GPO's

### In dit practicum:

- Leert u met policies in een GPO om te gaan.

### Voor dit practicum heeft u nodig:

- De DC's *PFSV1* en *PFSV2* zoals geconfigureerd na deel 1 van deze boekenserie.
- Werkstation *PFWS1* zoals geconfigureerd na deel 1 van deze boekenserie.
- Het werkblad bij practicum 1.2.1 waarop u uw werkzaamheden vastlegt.
- Tijd: ± 90 minuten.



Policies

### Korte practicuminstructies

Een toelichting op de nodige begrippen en werkwijzen vindt u in de gedetailleerde practicumuitwerking.

- Maak in de MMC *Group Policy Management* de site *PFBudel* zichtbaar.
- Bekijk de in het domain *PoliForma.local* standaard aanwezige GPO's.  
Zorg dat u weet welke GPO's door overerven op de OU *Domain Controllers* van toepassing zijn.
- Maak een nieuw GPO aan met de naam *PFGebruikersGPO*. Zorg dat dit gekoppeld is aan de OU *PFAfdelingen*. Het nieuwe GPO baseert u niet op een starter GPO.
- Onderzoek welke GPO's nu op alle afdelingen van toepassing zijn.
- Stel in het GPO *PFGebruikersGPO* de policy *Prohibit access to Control Panel and PC settings* in op *Enabled*.  
Vul als commentaar in: *Verhindert het gebruik van het Control Panel*.
- Haal de instelling uit punt e voor u in de MMC *Group Policy Management*.
- Controleer of u als domain *Administrator* op werkstation *PFWS1* het *Control Panel* kunt gebruiken. Verklaar waarom wel of niet.  
Controleer of u als *Doortje Heijnen* op werkstation *PFWS1* het *Control Panel* kunt gebruiken. Verklaar waarom wel of niet.  
Controleer of u met het user account van *Uzelf* op werkstation *PFWS1* het *Control Panel* kunt gebruiken. Verklaar waarom wel of niet.
- Controleer of u als domain *Administrator* op de DC's *PFSV1* en *PFSV2* het *Control Panel* kunt gebruiken. Verklaar waarom wel of niet.  
Controleer of u met het user account van *Uzelf* op de DC's *PFSV1* en *PFSV2* het *Control Panel* kunt gebruiken. Verklaar waarom wel of niet.

- i Bepaal de RSoP van het user account van *Uzelf* op DC *PFSV1*.  
Bekijk de settings van de ingestelde policy ten aanzien van het *Control Panel* in de RSoP.
- j Sluit alle machines in de juiste volgorde af.

### **Gedetailleerde uitwerking van het practicum**

Dit uitgebreide practicum valt in een aantal delen uiteen. Dit keer zijn het er nogal wat:

- Eerst maakt u kennis met de *MMC Group Policy Management*.
  - Dan zorgt u ervoor dat de site *PFBudel* in de *MMC Group Policy Management* te zien is.
  - Vervolgens bekijkt u de standaard gekoppelde GPO's in het domain *PoliForma.local*.
  - Dan bekijkt u het overerven van GPO's en de consequenties daarvan.
  - Vervolgens maakt u een nieuw GPO aan en koppelt dit aan de OU *PFafdelingen*.
  - Dan maakt u kennis met de *MMC Group Policy Management Editor* en stelt u daarmee een policy in.
  - Daarna bekijkt u de GPO-informatie van het nieuwe GPO.
  - Dan bekijkt u de gevolgen van de ingestelde policy voor verschillende gebruikers op werkstation *PFWS1* en op de DC's.
  - Tenslotte gebruikt u een wizard om te bekijken welke policies voor een gebruiker op een machine uiteindelijk van toepassing zijn.
- 1 Zorg dat u als domain *Administrator* bent ingelogd op de DC's *PFSV1* en *PFSV2*.  
Laat werkstation *PFWS1* uit staan.

#### **Het Group Policy Management Console**

Om te beginnen bekijkt u de *MMC Group Policy Management*.

- 2 Klik op DC *PFSV1* in het menu *Tools* van de *Server Manager* op de optie *Group Policy Management*.  
Vouw in de tree uit zoals in afbeelding 1-3.  
Selecteer in de tree de root *Group Policy Management*.