

Afb. 2-31 AD DS in de Server Manager

### Toelichting

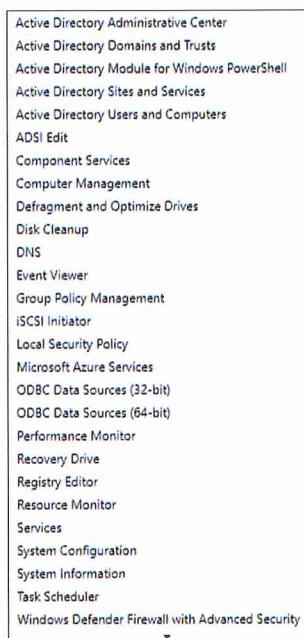
- Bovenin het detailvenster ziet u DC *PFSV1*. Dat is de machine die u bekijkt en waarop AD op dit moment draait.
- Als u in het detailvenster naar beneden scrollt, komt u achtereenvolgens de *EVENTS*, de *SERVICES*, de *BEST PRACTICES ANALYZER*, de *PERFORMANCE* en de *ROLES AND FEATURES* tegen.

Op al deze zaken wordt in het vervolg van deze boekenserie ingegaan. Op dit moment zijn ze nog niet zo van belang.

In de tree van de *Server Manager* ziet u ook de geïnstalleerde server role *DNS* (afbeelding 2-31). DNS is zo belangrijk voor de netwerkcommunicatie dat het gehele hoofdstuk 3 daarover gaat.

### Beheertools voor het bewerken van Active Directory

Als gevolg van een keuze van u (afbeelding 2-9) zijn er gelijk met de installatie van de *AD DS* standaard een aantal beheertools geïnstalleerd. Deze heeft u nodig voor het bewerken van AD. Enkele daarvan zijn opgenomen in het menu *Start*. Ze zijn allemaal opgenomen in het menu *Tools* van de *Server Manager* (afbeelding 2-32).



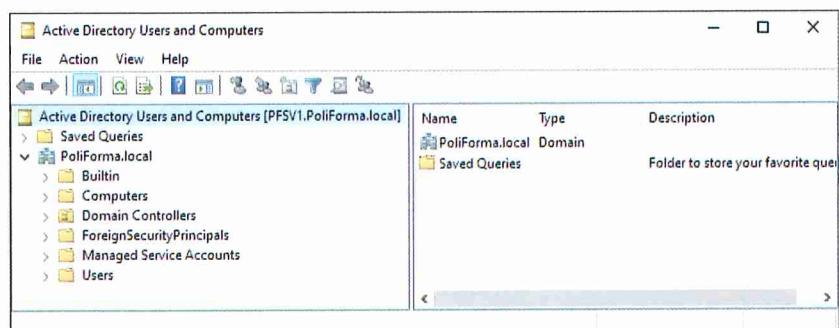
Afb. 2-32 De beheertools in het menu *Tools*

### Active Directory Users and Computers

De MMC *Active Directory Users and Computers* is verreweg de meest gebruikte tool voor het beheer van AD. U zult dat merken. Voor alles wat met het beheer van gebruikers, computers en dergelijke te maken heeft, gebruikt u meestal dit gereedschap. U leert nu hoe de MMC *Active Directory Users and Computers* is georganiseerd. Ook verandert u er enkele instellingen mee.

- 4 Klik in het menu *Tools* van de *Server Manager* op de optie *Active Directory Users and Computers*.

Vouw in de tree uit zoals in afbeelding 2-33.



Afb. 2-33 De MMC *Active Directory Users and Computers*

In de tree komen onder het domain *PoliForma.local* twee soorten pictogrammen voor.

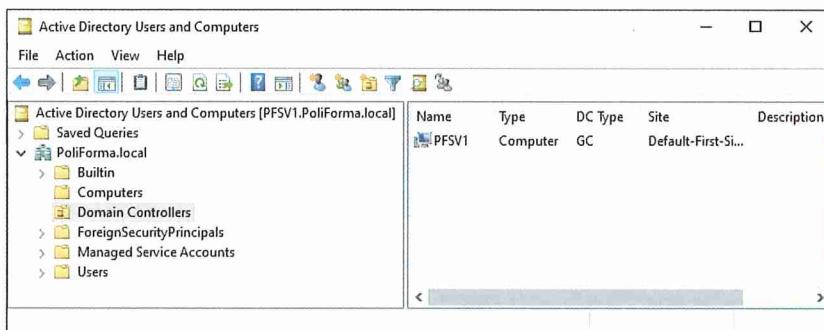
-  Dit pictogram staat voor een container.
-  Dit pictogram staat voor een OU (Organizational Unit). Een OU is ook een container maar dan met speciale mogelijkheden. In hoofdstuk 7 wordt er uitvoerig op ingegaan.

5 Klik in de tree op de container *Computers*.

In het detailvenster ziet u geen objecten. Dat klopt, want server *PFSV1* is een DC en dat is geen gewone computer in het netwerk.

6 Klik in de tree op de OU *Domain Controllers*.

In het detailvenster ziet u nu DC *PFSV1* (afbeelding 2-34).



Name	Type	DC Type	Site	Description
PFSV1	Computer	GC	Default-First-Site-Name	

Afb. 2-34 DC's worden in de OU *Domain Controllers* opgenomen

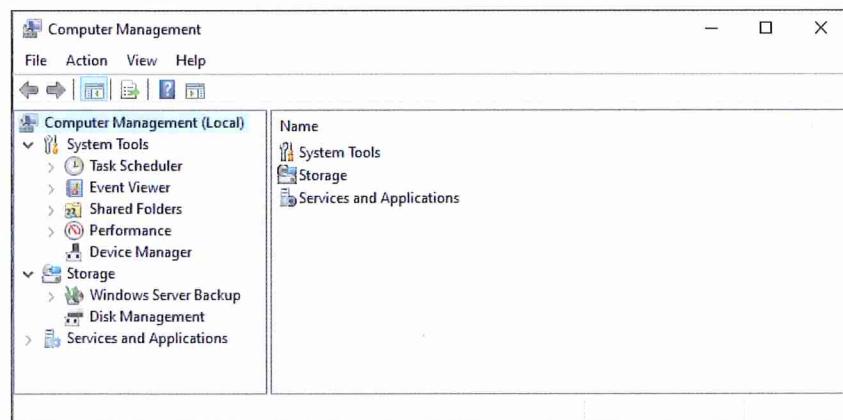
In het detailvenster ziet u het **computer account** *PFSV1*. In het logische computer account wordt de fysieke computer beschreven via eigenschappen. Precies zoals in hoofdstuk 1 het geval was met een user account. Verderop bekijkt u die eigenschappen.

Verder ziet u:

- Dat het *DC Type* ingesteld staat op *GC*. DC *PFSV1* is dus een GCS (afbeelding 2-22).
- Dat DC *PFSV1* is opgenomen in de *Site* met de naam *Default-First-Site-Name*. Die naam wijzigt u direct in een voor PoliForma BV toepasselijke naam.

In hoofdstuk 1 (afbeelding 1-29) heeft u de gebruikers bekeken op een stand-alone server, de machine local users. U doet dat nu opnieuw.

7 Open op DC *PFSV1* de MMC *Computer Management* (afbeelding 2-35).



Afb. 2-35 Geen machine local users en machine local groups op een DC

Vergelijk afbeelding 2-35 met afbeelding 1-29. U ziet in de tree dat op een DC de container *Local Users and Groups* niet bestaat. Op een DC komen dus geen machine local users en geen machine local groups voor. Machine local users en machine local groups worden opgeslagen in de SAM. De conclusie is dus dat op een DC de SAM niet voor dit doel wordt gebruikt. Dat is ook logisch. De SAM was er de oorzaak van dat het beheer in een peer-to-peer-netwerk **decentraal** is georganiseerd. In bedrijfsnetwerken is een van de belangrijkste kenmerken dat het beheer per domain **centraal** is georganiseerd. Daarin past het gebruik van de SAM niet, daarin past AD. AD werkt immers als een soort van Wikipedia voor het gehele netwerk.

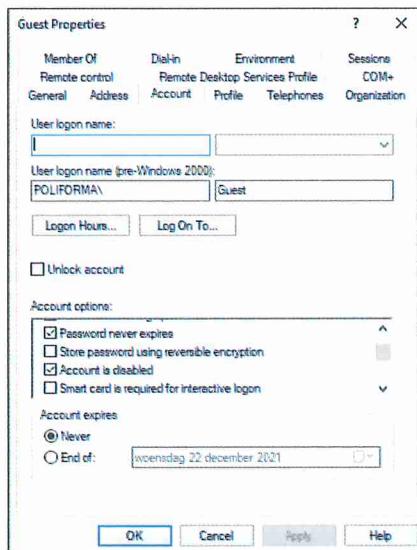
- 8 Sluit alle vensters behalve dat van de MMC *Active Directory Users and Computers*. Klik nu in de tree op de container *Users* van het domain *PoliForma.local* (afbeelding 2-36).

Active Directory Users and Computers			
	Name	Type	Description
> Active Directory Users and Computers [PFSV1.PoliForma.local]	Administrator	User	Built-in
> Saved Queries	Allowed RODC Password Replication Group	Security Group - Domain Local	Members
> PoliForma.local	Cert Publishers	Security Group - Domain Local	Members
> Builtin	Cloneable Domain Controllers	Security Group - Global	Members
> Computers	Denied RODC Password Replication Group	Security Group - Domain Local	Members
> Domain Controllers	DnsAdmins	Security Group - Domain Local	DNS Ad
> ForeignSecurityPrincipals	DnsUpdateProxy	Security Group - Global	DNS clie
> Managed Service Accounts	Domain Admins	Security Group - Global	Designa
> Users	Domain Computers	Security Group - Global	All work
	Domain Controllers	Security Group - Global	All dom
	Domain Guests	Security Group - Global	All dom
	Domain Users	Security Group - Global	All dom
	Enterprise Admins	Security Group - Universal	Designa
	Enterprise Key Admins	Security Group - Universal	Members
	Enterprise Read-only Domain Controllers	Security Group - Universal	Members
	Group Policy Creator Owners	Security Group - Global	Members
	Guest	User	Built-in
	Key Admins	Security Group - Global	Members
	Protected Users	Security Group - Global	Members
	RAS and IAS Servers	Security Group - Domain Local	Servers i
	Read-only Domain Controllers	Security Group - Global	Members
	Schema Admins	Security Group - Universal	Designa

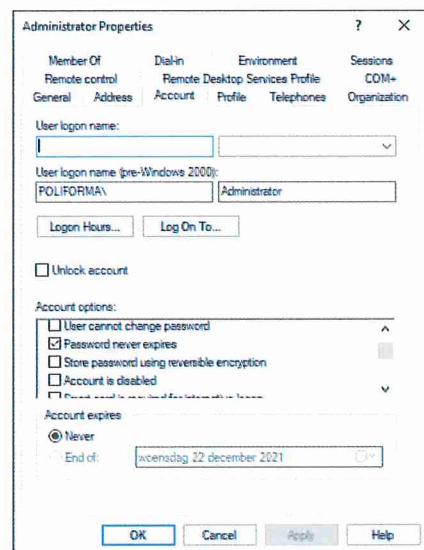
Afb. 2-36 Standaardgebruikers en groepen in AD

U ziet de standaard in AD aangemaakte gebruikers en groepen. U herkent de gebruikers **Administrator** en **Guest**. Hier zijn dat geen machine local users maar **domain users**. Ook de groepen zijn van een ander type – geen machine local groups maar **security groups** van de typen **Domain Local**, **Global** en **Universal**. Op security groups wordt dieper ingegaan in deel 2 *Beheer en beveiliging*.

- 9 Vergelijk de eigenschappenvensters van de domain users *Guest* en *Administrator* met de machine local users *Guest* en *Administrator* (afbeelding 1-30 versus 2-37 en afbeelding 1-31 versus 2-38).



Afb. 2-37 Ook in AD is het account *Guest* uitgeschakeld



Afb. 2-38 Het account van de domain *Administrator*

- 10 Plaats in het account *Guest* op het tabblad *Account* zo nodig een vink voor *Account is disabled* zodat dit in elk geval uitgeschakeld staat (afbeelding 2-37).
  - 11 Schakel voor de domain *Administrator* zo nodig de eigenschap *Password never expires* in.  
  
*Password never expires* voorzien van een vink zorgt ervoor dat u als domain *Administrator* gedurende deze cursus hetzelfde password kunt blijven gebruiken. In de praktijk is dit natuurlijk sterk af te raden.
  - 12 Sluit alle eigenschappenvensters door op de knop *OK* te klikken.
- Behalve de groepen in de container *Users* zijn er nog groepen van het type **Builtin**. Dat zijn de standaard ingebouwde groepen in AD.
- 13 Klik in de tree van de MMC *Active Directory Users and Computers* op de container *Builtin* van het domain *PoliForma.local*.  
  
U ziet de bedoelde ingebouwde groepen (afbeelding 2-39). Het zijn allemaal security groups van het type **Domain Local**.

The screenshot shows the Active Directory Users and Computers snap-in window. The left pane displays a tree view of the domain structure under 'PFSV1.PeliFerma.local'. The 'Builtin' container is expanded, showing categories like 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'. The right pane lists a large number of built-in security groups, each with a small icon, their name, type ('Security Group - Domain Local'), and a brief description. Some descriptions are truncated with '...'.

Name	Type	Description
Access Control Assistance Operators	Security Group - Domain Local	Members of thi
Account Operators	Security Group - Domain Local	Members can a
Administrators	Security Group - Domain Local	Administrators
Backup Operators	Security Group - Domain Local	Backup Operat
Certificate Service DCOM Access	Security Group - Domain Local	Members of thi
Cryptographic Operators	Security Group - Domain Local	Members are at
Distributed COM Users	Security Group - Domain Local	Members are al
Event Log Readers	Security Group - Domain Local	Members of thi
Guest	Security Group - Domain Local	Guests have the
Hyper-V Administrators	Security Group - Domain Local	Members of thi
IIS_IUSRS	Security Group - Domain Local	Built-in group t
Incoming Forest Trust Builders	Security Group - Domain Local	Members of thi
Network Configuration Operators	Security Group - Domain Local	Members in thi
Performance Log Users	Security Group - Domain Local	Members of thi
Performance Monitor Users	Security Group - Domain Local	Members of thi
Pre-Windows 2000 Compatible Access	Security Group - Domain Local	A backward co
Print Operators	Security Group - Domain Local	Members can a
RDS Endpoint Servers	Security Group - Domain Local	Servers in this g
RDS Management Servers	Security Group - Domain Local	Servers in this g
RDS Remote Access Servers	Security Group - Domain Local	Servers in this g
Remote Desktop Users	Security Group - Domain Local	Members in thi
Remote Management Users	Security Group - Domain Local	Members of thi
Replicator	Security Group - Domain Local	Supports file re
Server Operators	Security Group - Domain Local	Members can a
Storage Replica Administrators	Security Group - Domain Local	Members of thi
Terminal Server License Servers	Security Group - Domain Local	Members of thi
Users	Security Group - Domain Local	Users are preve
Windows Authorization Access Group	Security Group - Domain Local	Members of thi

Afb. 2-39 Ingebouwde groepen

Voorlopig worden in dit boek alle groepen die in het domain bekend zijn, aangegeven met **domain groups**. Dit om ze te onderscheiden van machine local groups.

- 14 Vergelijk de ingebouwde domain groups met de machine local groups op een standalone server (afbeelding 1-32 versus 2-36/39).

#### Het computer account PFSV1

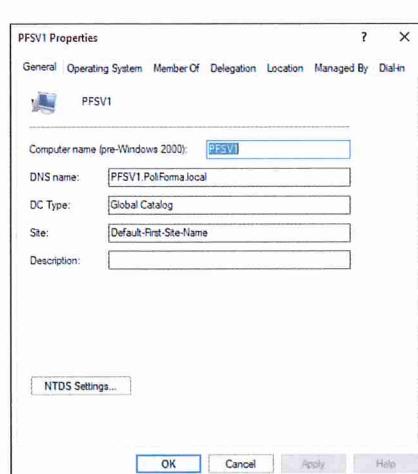
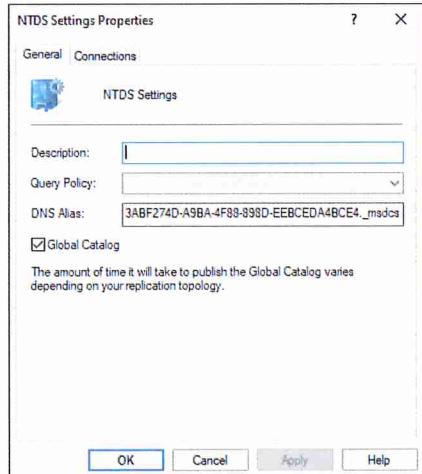
Tenslotte past u met de MMC *Active Directory Users and Computers* het computer account van DC *PFSV1* aan.

- 15 Selecteer in de tree van de MMC *Active Directory Users and Computers* de OU *Domain Controllers*.

Open in het detailvenster bij DC *PFSV1* het snelmenu.

Klik op de optie *Properties*.

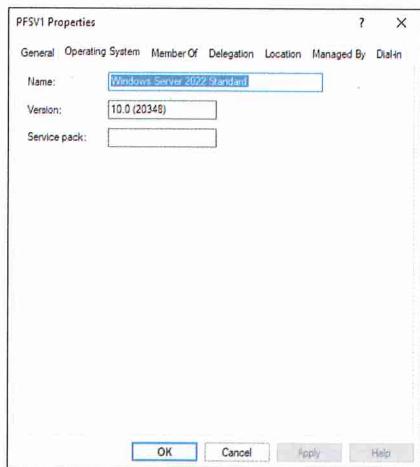
Het eigenschappenvenster van DC *PFSV1* verschijnt (afbeelding 2-40).

Afb. 2-40 Het tabblad *General*Afb. 2-41 DC *PFSV1* is een GCS

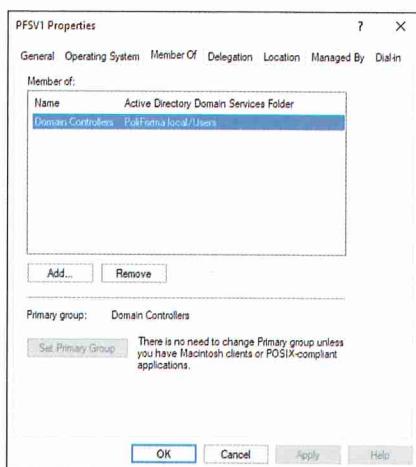
- 16 Herken de getoonde eigenschappen op het tabblad *General*.  
 Vul het tekstvak *Description* met: *DC in het domain PoliForma.local*  
 Klik op de knop *Apply*.  
 Klik op de knop *NTDS Settings*.

Het venster *NTDS Settings Properties* verschijnt (afbeelding 2-41). AD is opgeslagen in het databasebestand *ntds.dit* op DC *PFSV1*. In het venster van afbeelding 2-41 ziet u daarvan de settings. Ook hier ziet u dat DC *PFSV1* een GCS is. Als u ooit op een DC de *Global Catalog* wilt verwijderen, kunt u dat hier doen. Bij de eerste of de laatste DC in het domain kan dat natuurlijk niet. Een domain kan niet bestaan zonder tenminste één GCS.

- 17 Vul het tekstvak *Description* met: *AD van het domain PoliForma.local*  
 Klik op de knop *Apply*.  
 Klik op de knop *OK*.  
 Haal het tabblad *Operating System* voor u (afbeelding 2-42).



Afb. 2-42 Het besturingssysteem

Afb. 2-43 Lid van de domain group  
*Domain Controllers*

U ziet het geïnstalleerde besturingssysteem.

- 18 Haal het tabblad *Member Of* voor u (afbeelding 2-43).

U ziet dat DC *PFSV1* lid is van de domain group *Domain Controllers*. Deze domain group is geplaatst in de container *Users* van het domain *PoliForma.local* (afbeelding 2-36).

- 19 Sluit het eigenschappenvenster door op de knop *OK* te klikken.

Sluit ook de MMC *Active Directory Users and Computers*.

#### **Active Directory Sites and Services**

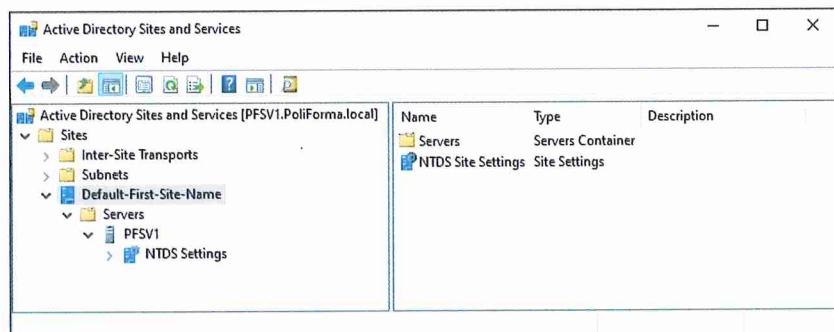
Een andere beheertool die voor AD is geïnstalleerd, is de MMC *Active Directory Sites and Services*. Omdat u in dit boek met één site en één domain werkt, heeft u deze beheertool niet vaak nodig. Eenmaal ingesteld heeft u er nauwelijks nog omkijken naar.

U voorziet nu de site van PoliForma BV van een toepasselijke naam. Ook de plaats van de vestiging van PoliForma BV kan worden ingevuld. Zoals u uit hoofdstuk o weet, is dat Budel.

- 20 Klik in het menu *Tools* van de *Server Manager* op de optie *Active Directory Sites and Services*.

Vouw de tree zoveel mogelijk uit zoals in afbeelding 2-44.

Selecteer in de tree de site *Default-First-Site-Name* zoals in afbeelding 2-44.

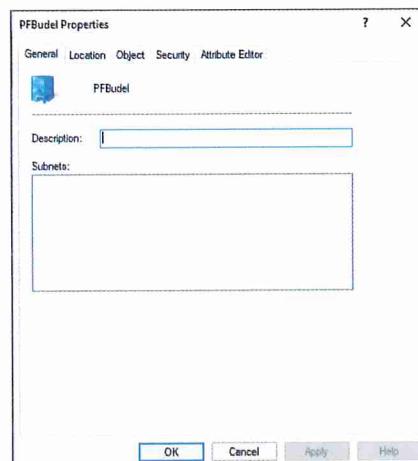


Afb. 2-44 De MMC Active Directory Sites and Services

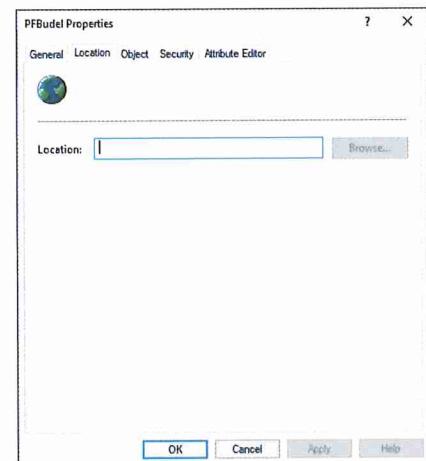
In de vorige paragraaf installeerde u AD voor het domain *PoliForma.local*. Het domain is een logische afspiegeling van PoliForma BV. De fysieke afspiegeling is een site. De site is het LAN in de gebouwen waarin PoliForma BV is gevestigd. De site die tijdens de installatie is aangemaakt, heeft de naam *Default-First-Site-Name* gekregen. In afbeelding 2-44 ziet u in de tree dat DC *PFSV1* daar fysiek staat opgesteld.

In dit boek wordt de site van een toepasselijke naam en locatie voorzien.

- 21 Open in de tree het snelmenu bij *Default-First-Site-Name*.
- Klik op de optie *Rename*.
- Wijzig de naam in *PFBudel* ENTER.
- Open in de tree het eigenschappenvenster van de site *PFBudel*.
- Vul op het tabblad *General* (afbeelding 2-45) het tekstvak *Description* met: *Vestiging van PoliForma BV*
- Vul op het tabblad *Location* (afbeelding 2-46) het tekstvak *Location* met: *Budel*
- Klik op de knop *Apply*.
- Klik op de knop *OK*.



Afb. 2-45 Ook een site heeft eigenschappen



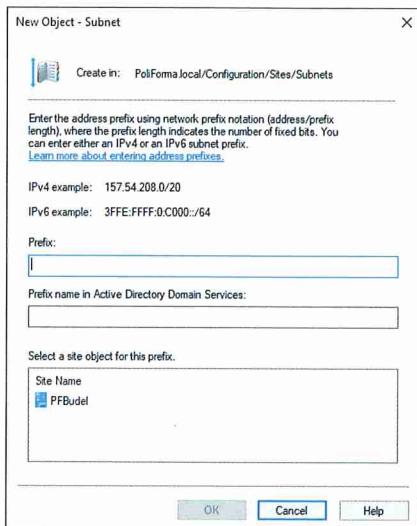
Afb. 2-46 Waar op de wereld?

Vervolgens koppelen we het IPv4-netwerk dat bij PoliForma BV wordt gebruikt nog aan de site *PFBudel*.

- 22 Klik in de tree van de MMC *Active Directory Sites and Services* op de container *Subnets*.

- 23 Open in het detailvenster het snelmenu en klik op de optie *New subnet*.

Daarop verschijnt het dialoogvenster *New Object - Subnet* van afbeelding 2-47.



Afb. 2-47 Een site koppelen aan een IPv4-netwerk

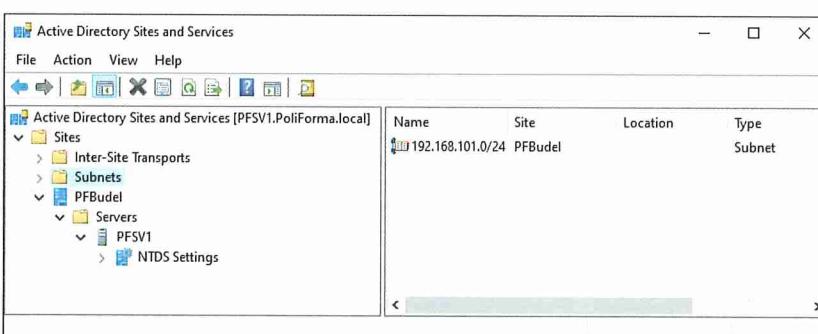
Bij PoliForma BV wordt gebruikgemaakt van het IPv4-netwerk 192.168.101.0/24 (hoofdstuk 1 en bijlage B).

- 24 Vul het tekstvak *Prefix* met: 192.168.101.0/24

Selecteer in de lijst *Select a site object for this prefix* de site *PFBudel*.

Klik nog op de knop *OK*.

IPv4-netwerk en site zijn nu aan elkaar gekoppeld (afbeelding 2-48).



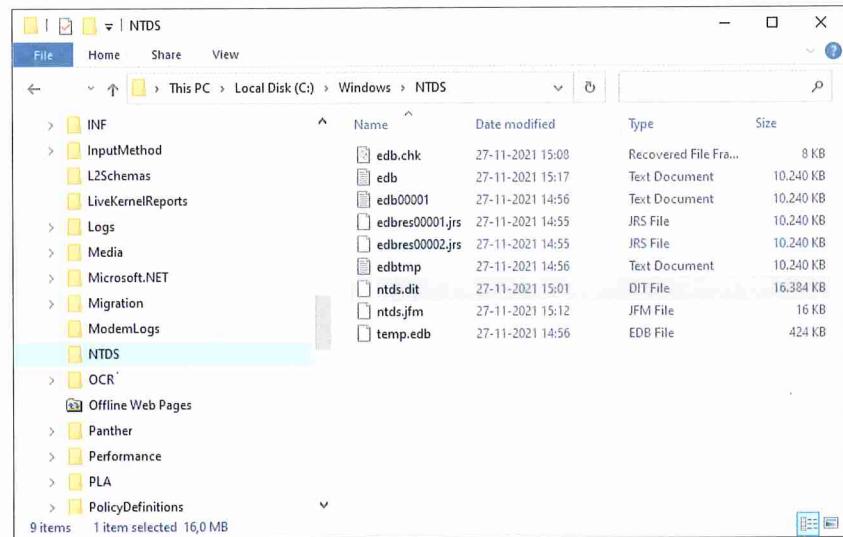
Afb. 2-48 Een IPv4-netwerk gekoppeld aan een site

25 Sluit de MMC Active Directory Sites and Services.

#### De plaats van AD op server PFSV1

Tijdens de installatie van AD heeft u aangegeven waar AD moest worden opgeslagen (afbeelding 2-25). U controleert daarvan het resultaat.

26 Open File Explorer en haal de map C:\Windows\NTDS voor u (afbeelding 2-49).



Afb. 2-49 AD in File Explorer

In het detailvenster ziet u AD. Zoals u weet is dat het bestand *ntds.dit*.

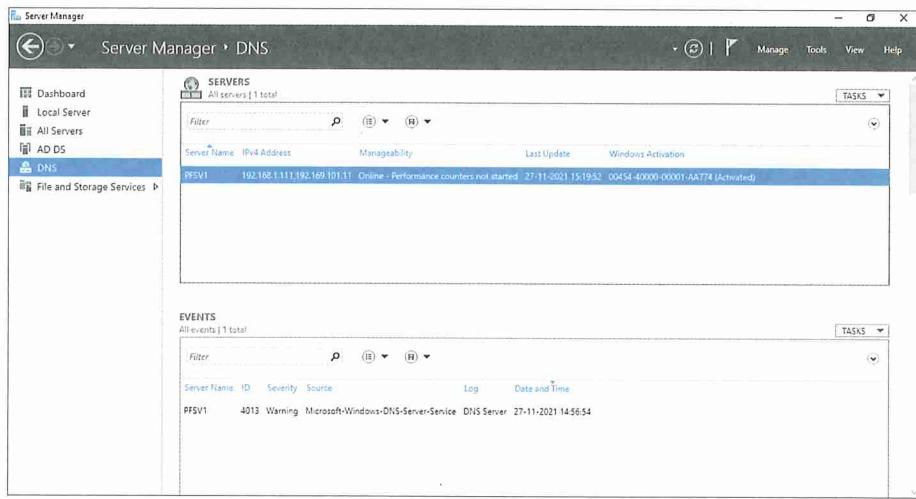
27 Sluit File Explorer.

#### De server role DNS Server

U weet inmiddels dat AD absoluut niet zonder DNS kan. Daarom heeft u tijdens de installatie van AD gelijk ook DNS laten installeren (afbeelding 2-22). U bekijkt nu globaal deze server role. In hoofdstuk 3 wordt er dieper op ingegaan.

28 Start zo nodig de Server Manager.

Selecteer in de Server Manager de server role DNS (afbeelding 2-50).



Afb. 2-50 Het overzicht van de server role *DNS Server*

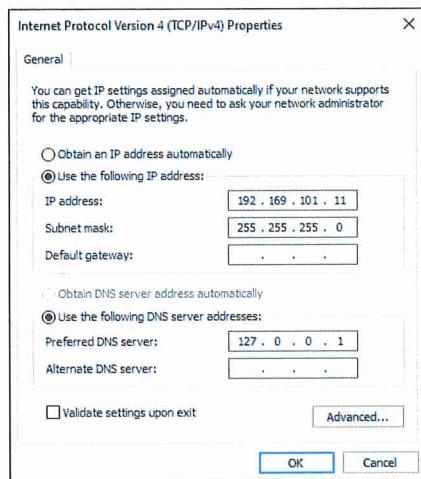
Van deze server role ziet u in het overzichtsvenster:

- de DNS-server en dat is dus *PFSV1*
- de *EVENTS*
- en lager:
- de *SERVICES*
- de *BEST PRACTICES ANALYZER*
- de *PERFORMANCE*
- de *ROLES AND FEATURES*

Het overzichtsvenster past zich aan de aard van de server role aan. Zoals vermeld wordt later in deze cursus op de verschillende onderdelen teruggekomen.

DNS dient ervoor om het IPv4-adres van een computer op te sporen met behulp van zijn computernaam. Pas in het volgende hoofdstuk zult u zien waar en hoe u dit kunt bekijken. De omzetting van computernaam naar IPv4-adres gaat dus via DNS. Elke computer in het netwerk moet dus weten welke server de DNS-server is, ook DC en DNS-server *PFSV1* zelf.

- 29 Open op DC *PFSV1* het venster *Internet Protocol Version 4 (TCP/IPv4) Properties* van de NIC *LANConnectie* (afbeelding 2-51).

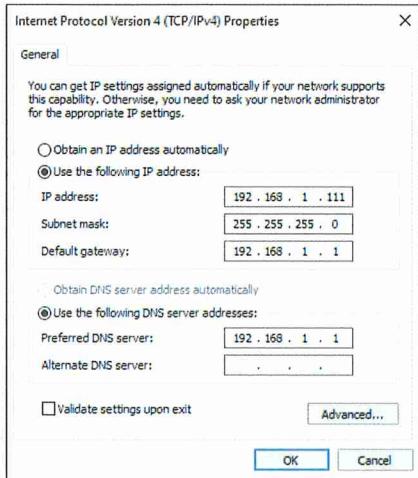


Afb. 2-51 Het IPv4-adres van de DNS-server voor de NIC *LANConnectie* op server *PFSV1*

U ziet dat in het tekstvak *Preferred DNS server* ingevuld is: *127.0.0.1*. Elk IPv4-adres dat met 127 begint, is een **loopback address**. Een loopback address verwijst naar de machine zelf (bijlage B). Eigenlijk staat er in afbeelding 2-51: De DNS-server, dat ben ik zelf. Overigens had de *Active Directory Domain Services Configuration Wizard* al aangekondigd dit voor u te zullen regelen (afbeelding 2-26).

- 30 Sluit de vensters over de NIC *LANConnectie* telkens met de knop *OK* en eventueel *Close*.

Controleer ook de IPv4-instellingen van de NIC *InternetConnectie*. Daarop moeten de IPv4-instellingen die u van uw docent heeft gekregen staan ingevuld, ook het IPv4-adres van de DNS-server. Herstel als dat nodig is (afbeelding 2-52 zoals in dit boek gebruikt). Meestal wordt dit IPv4-adres ook veranderd in *127.0.0.1* en dat is nadrukkelijk niet de bedoeling omdat daardoor de internetverbinding niet meer zal werken.



Afb. 2-52 De IPv4-instellingen voor de NIC *InternetConnectie* zijn bij u anders

- 31 Controleer op DC *PFSV1* de verbinding met het internet. Die moet nog steeds goed werken.
- 32 Sluit op server *PFSV1* alle vensters op de gebruikelijke manier.  
Sluit uw virtuele server *PFSV1* geordend af.

### 2.3 Member servers

Door de installatie van AD is de kern van uw nieuwe netwerk in bedrijf. In deze paragraaf neemt u standalone server *PFSV2*, die inmiddels onder die naam is opgenomen in de werkgroep *PFWERKGROEP*, op in het domain *PoliForma.local*. Daardoor wordt server *PFSV2* een **member server** in dat domain. Vervolgens stelt u vast welke veranderingen er daardoor op die server zijn doorgevoerd. Ze zullen niet zo ingrijpend blijken te zijn als bij een DC. Toch zijn er fundamentele verschillen met een standalone server.

Eerst maakt u standalone server *PFSV2* lid van het domain *PoliForma.local*.



#### Practicum 2.3.1: Member server PFSV2

45 min.

##### In dit practicum:

- Zorgt u ervoor dat standalone server *PFSV2* weet dat DC *PFSV1* ook de DNS-server van het domain *PoliForma.local* is.
- Maakt u van standalone server *PFSV2* een member server in het domain *PoliForma.local*.

**Voor dit practicum heeft u nodig:**

- De virtuele machines *PFSV1* en *PFSV2* zoals geconfigureerd na de vorige opdracht:
  - server *PFSV1* is DC en DNS-server in het domain *PoliForma.local*;
  - server *PFSV2* is standalone server in de werkgroep *PFWERKGROEP*.
- Het werkblad bij practicum 2.3.1 waarop u uw werkzaamheden vastlegt.
- Tijd: ± 45 minuten.



*Member server*

**Korte practicuminstructies**

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

- a Configureer op server *PFSV2* de *Preferred DNS server* met het IPv4-adres van de NIC *LANConnectie* van DC *PFSV1*.
- b Maak server *PFSV2* lid van het domain *PoliForma.local*.
- c Log als domain *Administrator* in op server *PFSV2*.

**Gedetailleerde uitwerking van het practicum**

Het opnemen van standalone server *PFSV2* in het domain *PoliForma.local* valt in twee delen uiteen:

- Standalone server *PFSV2* moet eerst weten welke server de DNS-server is van het domain *PoliForma.local*. Anders wordt op standalone server *PFSV2* de DNS-naam *PoliForma.local* niet begrepen.
  - Standalone server *PFSV2* kan daarna lid worden gemaakt van het domain.
- 1 Start de virtuele server *PFSV1* en log in als domain *Administrator*.  
Als server *PFSV1* correct draait, start dan de virtuele standalone server *PFSV2* en log daarop in als machine local *Administrator*.

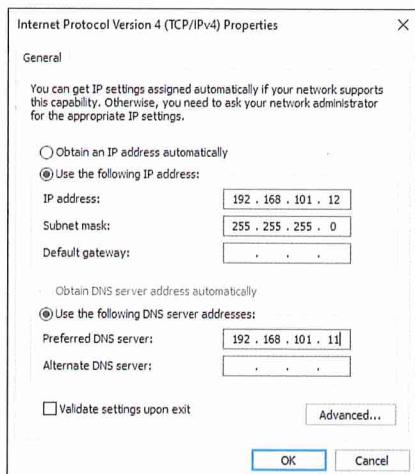
**Het IPv4-adres van de DNS-server op standalone server PFSV2**

Eerst dus standalone server *PFSV2* laten weten dat server *PFSV1* de DNS-server is in het domain *PoliForma.local*. Dat gaat via een IPv4-adres. U vult op standalone server *PFSV2* het IPv4-adres van de NIC *LANConnectie* van DC *PFSV1* in als *Preferred DNS server*. Dat IPv4-adres is zoals u weet *192.168.101.11*.

- 2 Haal op standalone server *PFSV2* het venster met de IPv4-configuratie van de NIC *LANConnectie* voor u.  
Vul het tekstvak achter *Preferred DNS server* met: *192.168.101.11*  
Vergelijk het venster met dat van afbeelding 2-53. Herstel als dat nodig is.

Klik op de knop *OK*.

Sluit alle vensters op de gebruikelijke manier behalve dat van de *Server Manager*.



Afb. 2-53 De DNS-server staat ingesteld op standalone server *PFSV2*

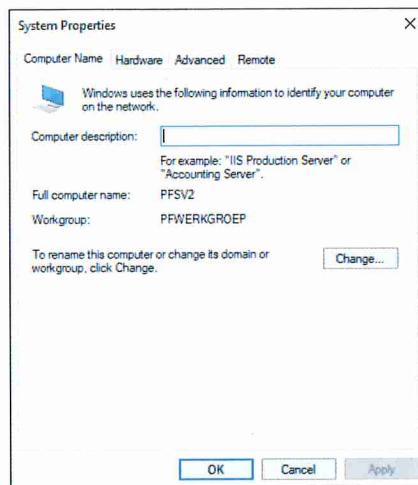
#### **Standalone server *PFSV2* lid maken van het domain *PoliForma.local***

Standalone server *PFSV2* weet nu dus welke server de DNS-server in het domein *PoliForma.local* is. U kunt vervolgens standalone server *PFSV2* lid maken van dat domein. Veel van deze procedure heeft u hiervoor al gezien. Het veranderen van werkgroep verloopt namelijk op bijna dezelfde manier.

- 3 Klik op server *PFSV2* in de tree van de *Server Manager* op *Local Server*, vervolgens in het detailvenster op de link *PFSV2* achter *Computer name* of *PFWERKGROEP* achter *Workgroup*. Welke maakt niet uit.



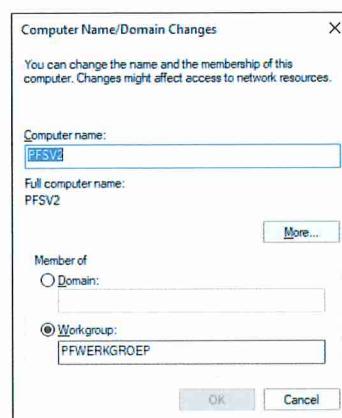
Het venster *System Properties* verschijnt. Het tabblad *Computer Name* ligt boven (afbeelding 2-54).



Afb. 2-54 De computernaam en werkgroep

- 4 Klik op de knop *Change*.

Het venster *Computer Name/Domain Changes* verschijnt (afbeelding 2-55).



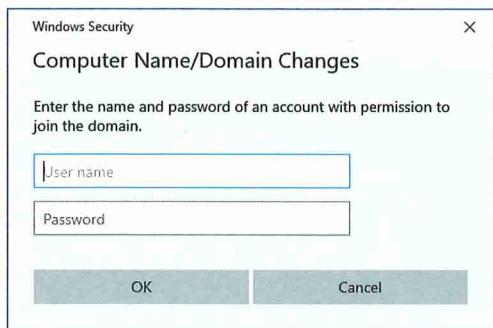
Afb. 2-55 Wijzigen

- 5 Selecteer in het kader *Member of* de optie *Domain*.

Vul het tekstvak daaronder met: *PoliForma.local*

Klik op de knop *OK*.

Nu verschijnt het venster *Windows Security* (afbeelding 2-56). De beveiliging van Windows Server 2022 blokkeert de voortgang.



Afb. 2-56 Dit gaat niet zomaar

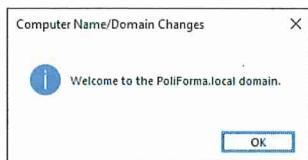
Op standalone server *PFSV2* bent u ingelogd als de machine local *Administrator*. Die heeft niets met het domain *PoliForma.local* te maken. Daarom is deze ook niet gerechtigd om standalone server *PFSV2* lid te maken van dat domain. Wie dan wel? De domain *Administrator* van het domain *PoliForma.local* natuurlijk.

- 6 Vul het tekstvak *User name* met: *POLIFORMA\Administrator* of *Administrator@PoliForma.local*

Vul het tekstvak *Password* met uw administratorpassword.

Klik op de knop *OK*.

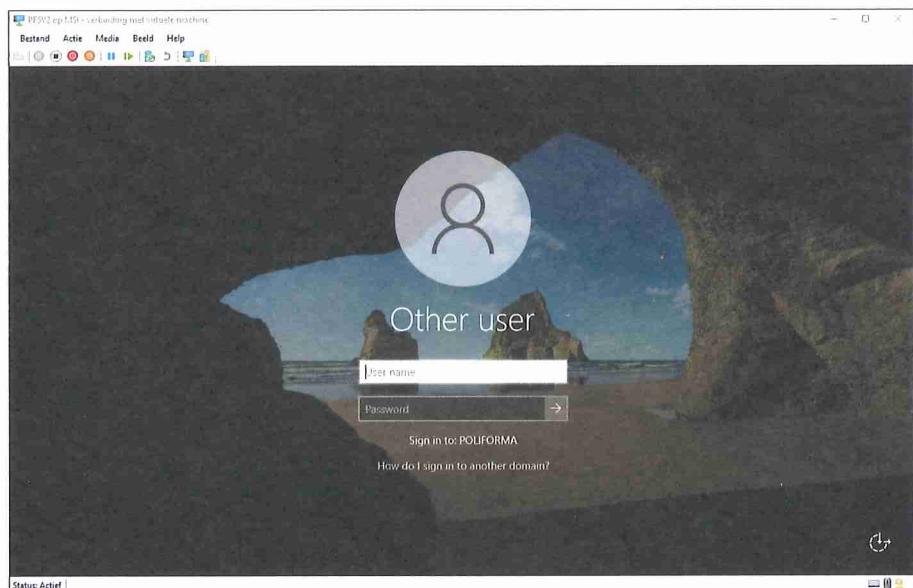
Na de nodige controles wordt u welkom geheten in het domain *PoliForma.local* (afbeelding 2-57).



Afb. 2-57 Vriendelijk

- 7 Klik op de knop *OK* in het venster waarin u welkom wordt geheten.  
Server *PFSV2* moet nu herstart worden.
- 8 Klik op de knop *OK* in het venster met de herstartmededeling.  
Klik op de knop *Close* van het venster *System Properties*.  
Laat server *PFSV2* nu herstarten door op de knop *Restart Now* te klikken.

Na het herstarten verschijnt het inlogscherm van afbeelding 2-58.



Afb. 2-58 Inloggen op server *PFSV2*

Nu server *PFSV2* lid is van het domain *PoliForma.nl* kunt u daarop inloggen als domain Administrator.

- 9 Vul het tekstvak *User name* met: *POLIFORMA\Administrator* of *Administrator@PoliForma.local*  
Vul het tekstvak *Password* met uw administratorpassword.  
Log in.

Server *PFSV2* is dus lid van het domain *PoliForma.local*. Een dergelijke server wordt een **member server** genoemd. In het venster van de *Server Manager* kunt u dit controleren in het detailvenster van het venster *Local Server* (afbeelding 2-59).

Computer name	PFSV2
Domain	<i>PoliForma.local</i>
<hr/>	
Microsoft Defender Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
LANConnectie	192.168.101.12

Afb. 2-59 Lid van het domain *PoliForma.local*

- 10 Sluit nu eerst member server *PFSV2* af.  
Sluit daarna server *PFSV1* af.

U bent nu zover dat u in uw domain *PoliForma.local* beschikt over één DC (*PFSV1*) en één member server (*PFSV2*). In de volgende opdracht bekijkt u de verschillen tussen de beide typen servers.



### Opdracht 2.3.2: Kijk en vergelijk

30 min.

#### In deze opdracht:

- Leert u een aantal zaken die karakteristiek zijn voor een member server.

#### Voor deze opdracht heeft u nodig:

- De virtuele machines *PFSV1* en *PFSV2* zoals geconfigureerd na het vorige prakticum.
  - Server *PFSV1* is DC en DNS-server in het domain *PoliForma.local*.
  - Server *PFSV2* is member server in het domain *PoliForma.local*.
- Het werkblad bij opdracht 2.3.2 waarop u uw werkzaamheden vastlegt.
- Tijd: ± 30 minuten.

#### Opdrachtinstructies

- Log als domain *Administrator* in op de virtuele server *PFSV1*.  
Log als machine local *Administrator* in op de virtuele member server *PFSV2* (*PFSV2\Administrator* met password).
- Welke server roles zijn er op member server *PFSV2* geïnstalleerd?
- Komen er op member server *PFSV2* nog machine local users en machine local groups voor? Zo ja, welke?
- Open op DC *PFSV1* de container *Users* in MMC *Active Directory Users and Computers*.  
Haal het tabblad *Members* van het eigenschappenvenster van de domain group *Domain Admins* voor u.  
Wie is er lid van deze groep?
- Open op member server *PFSV2* het eigenschappenvenster van de machine local group *Administrators*.  
Wie is er lid van deze groep?  
Vergelijk dit resultaat met afbeelding 1-33 dat geldt voor de machine local *Administrator* op een standalone server.
- Log op member server *PFSV2* uit. Gebruik daarvoor de optie *Sign out* bij het menu van *Administrator* in het menu *Start*.  
Log vervolgens op member server *PFSV2* in met het user account van de domain *Administrator*.

- 7 Zijn er op member server *PFSV2* in het menu *Tools* van de *Server Manager* opties opgenomen voor het beheer van AD?
- 8 In welke container of OU van AD is het computer account van member server *PFSV2* opgenomen?
- 9 Zet op de juiste plaats kruisjes in tabel 2-1 van het werkblad.

	<b>Standalone server</b>	<b>Member server</b>	<b>Domain Controller</b>
Bevat de map <i>C:\Windows\NTDS</i>			
Bevat de map <i>C:\Windows\SYSVOL</i>			
Bevat machine local users en machine local groups			
Bevat domain groups			
Bevat tools om AD te bewerken			

Tabel 2-1 Vergelijken

## 2.4 Fouttolerante/Redundante Active Directory Domain Services

Een domain waarin maar één DC draait, is niet **fouttolerant/redundant**. Zodra die DC uitvalt, zijn de *AD DS* niet meer beschikbaar. Daarmee stopt de dienstverlening van het netwerk aan de organisatie. Uw soort van Wikipedia is dan immers niet meer beschikbaar. Het is daarom altijd nodig minimaal twee DC's in een domain te laten draaien. Daarmee maakt u AD in het domain **fouttolerant/redundant**: u voert het dubbel uit. U creëert daarmee aanzienlijk meer bedrijfszekerheid. Valt er een DC uit dan draait het netwerk meestal gewoon door.

Heeft u eenmaal twee DC's in uw domain dan wordt AD op de beide DC's gelijk gehouden door een proces dat **replicatie** heet. Dat replicatieproces kunt u niet configureren als beide DC's in dezelfde site zijn ondergebracht. Dit omdat binnen een vestiging snelle en goedkope LAN-verbindingen worden gebruikt. Zijn de DC's in verschillende sites ondergebracht, dan kunt u dit wel configureren. Dit omdat tussen twee sites doorgaans een WAN-verbinding wordt gebruikt. Die zijn vaak trager, duurder en soms zelfs niet continu beschikbaar.

Wat hierboven voor de *AD DS* geldt, geldt ook voor de DNS-service. Ook daarvoor zorgt u voor een dubbele uitvoering.

Onder Windows Server 2022 zijn er verschillende DC-typen. De eerste DC in het root domain van het forest is per definitie een GCS. Een volgende DC in datzelfde domain hoeft dat niet te zijn. Verder kunt u onder Windows Server 2022 RODC's

installeren. De eerste DC in het root domain van het forest is per definitie geen RODC. Een volgende DC in datzelfde domain kan dat wel zijn. Beide begrippen bent u in het voorgaande al een keer tegengekomen (afbeelding 2-22). In het volgende practicum gebeurt dat opnieuw.



### Practicum 2.4.1: Dubbel

60 min.

#### In dit practicum:

- Leert u de verschillende DC-typen die onder Windows Server 2022 mogelijk zijn.
- Maakt u van member server *PFSV2* een tweede DC in het domain *PoliForma.local*.
- Controleert u het replicatieproces.

#### Voor dit practicum heeft u nodig:

- De virtuele machines *PFSV1* en *PFSV2* zoals geconfigureerd na de vorige paragraaf.
  - Server *PFSV1* is DC en DNS-server in het domain *PoliForma.local*.
  - Server *PFSV2* is member server in het domain *PoliForma.local*.
- Het werkblad bij practicum 2.4.1 waarop u uw werkzaamheden vastlegt.
- Tijd: ± 60 minuten.



2 DC's

#### Korte practicuminstructies

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

- Zorg dat u als domain *Administrator* bent ingelogd op server *PFSV1*.  
Log op member server *PFSV2* in als domain *Administrator*.
- Installeer op member server *PFSV2* de server role *AD DS*.
- Installeer AD op member server *PFSV2* met de volgende instellingen:
  - Member server *PFSV2* wordt een DC in het bestaande domain *PoliForma.local*.
  - Member server *PFSV2* wordt ook DNS-server.
  - De DC *PFSV2* zal ook GCS zijn.
  - DC *PFSV2* wordt geen RODC.
  - Member server *PFSV2* wordt als DC opgenomen in de site *PFBudel*.
  - Geen DNS delegation toepassen.
  - Het repliceren vindt over het LAN plaats vanaf DC *PFSV1*.

- d Controleer de gelijkwaardigheid van de DC's *PFSV1* en *PFSV2* zowel voor *AD DS* als *DNS*.
- e Controleer het repliceren met behulp van de omschrijving *DC in het domain PoliForma.local* voor DC *PFSV2*.

### Gedetailleerde uitwerking van het practicum

Het opwaarderen van member server *PFSV2* tot DC in het domain *PoliForma.local* valt in twee delen uiteen:

- Op member server *PFSV2* moet de server role *AD DS* worden geïnstalleerd.
- *AD* moet op member server *PFSV2* worden geïnstalleerd en een kopie worden van *AD* op DC *PFSV1*.

- 1 Start DC *PFSV1* en log in als domain *Administrator*.

Start member server *PFSV2* en log in als domain *Administrator*.

#### De server role Active Directory Domain Services installeren op member server PFSV2

- 2 Installeer op member server *PFSV2* zoals in practicum 2.1.1 de server role *AD DS* maar sluit de *Add Roles and Features Wizard* niet af.

#### Member server PFSV2 opwaarderen tot DC

Member server *PFSV2* moet nu een DC worden in het bestaande domain *PoliForma.local*. Dat domain is het root domain van een bestaand forest. Het is tevens het root domain van de enige tree in dat forest.

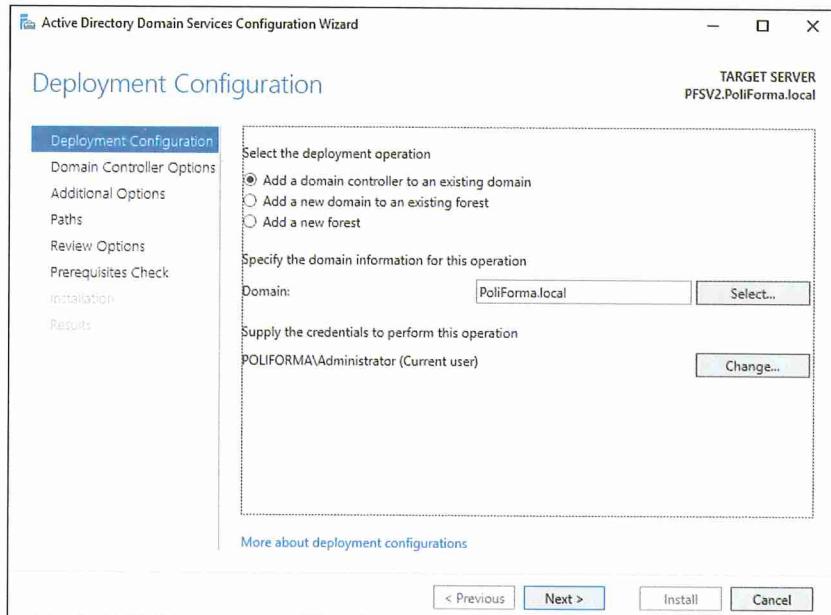
- 3 Start vanuit de *Add Roles and Features Wizard* de *Active Directory Domain Services Installation Wizard* door op de link *Promote this server to a domain controller* te klikken.

Selecteer in het wizardvenster *Deployment Configuration* zo nodig de optie *Add a domain controller to an existing domain* (afbeelding 2-60).

Als *Domain* staat *PoliForma.local* geselecteerd. In de huidige situatie valt er niet veel te kiezen. De voorgestelde keuze is ook de juiste.

Een **credential** is een geloofsbrief, een soort paspoort. Met een geloofsbrief toont u aan dat u gemachtigd bent om iets te doen. Omdat u op member server *PFSV2* bent ingelogd als domain *Administrator* beschikt u over de juiste geloofsbriefen om *AD* op member server *PFSV2* te installeren. Daarom staat onder *Supply the credentials to perform this operation* de gebruiker *POLIFORMA\Administrator (Current user)* geselecteerd.

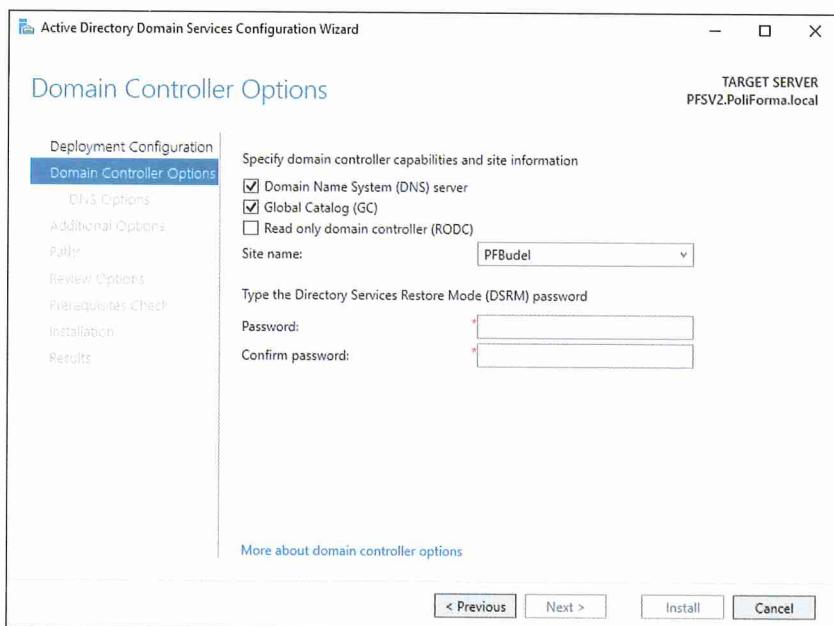
- 4 Vergelijk het wizardvenster *Deployment Configuration* met dat van afbeelding 2-60. Herstel als dat nodig is.



Afb. 2-60 *Deployment Configuration*

5 Klik op de knop *Next >*.

Het wizardvenster *Domain Controller Options* staat nu voor u (afbeelding 2-61). Nu is er wel wat te kiezen.



Afb. 2-61 Het DC-type bepalen

### Toelichting

- Voorgesteld wordt om de nieuwe DC ook DNS-server te laten zijn. Die keuze is verstandig omdat daarmee ook DNS fouttolerant/redundant wordt.
- Voorgesteld wordt ook om de nieuwe DC ook GCS te laten zijn. Om dezelfde reden is dat een verstandige keuze.
- Dan de keuze *Read only domain controller (RODC)*.

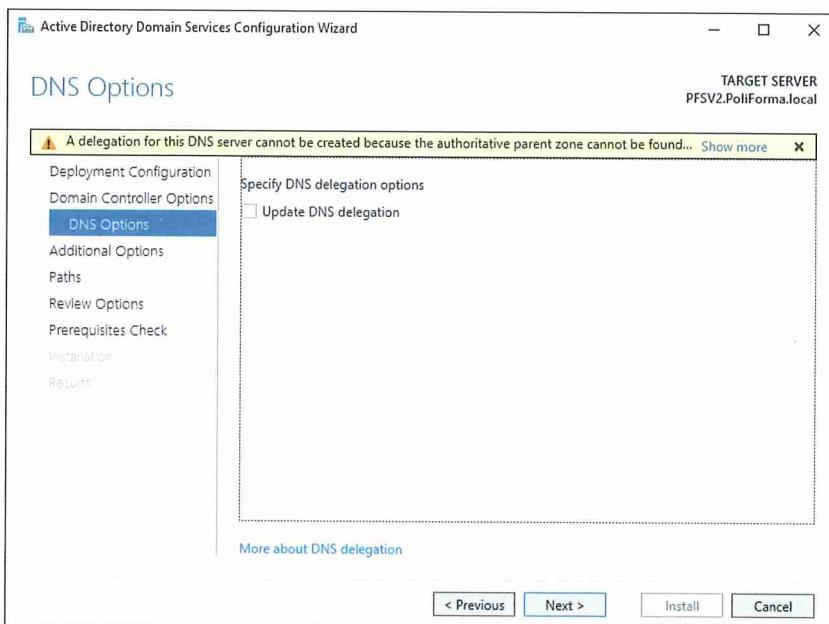
Een RODC is een DC met de volgende eigenschappen:

- Op een RODC is een read only-kopie van AD beschikbaar.
- Die kopie wordt via replicatie verkregen. Die replicatie verloopt van een DC naar een RODC en niet omgekeerd.
- De kopie op een RODC is niet helemaal compleet. Passwords worden er namelijk standaard niet in bewaard. Dit houdt bijvoorbeeld in dat als er een gebruiker inlogt voor de geloofsbriefen even in een DC gekeken moet worden. Zo verkregen credentials worden wel op een RODC gecachet tot ze veranderen.
- RODC's zijn bestemd voor bijvoorbeeld sites waar geen beheer met de bevoegdheden van een domain *Administrator* mogelijk is. Meestal omdat daarvoor de deskundigheid ontbreekt. Op die site levert een RODC de *Active Directory Domain Services* zonder de WAN-verbinding al te zwaar te beladen.
- Een RODC biedt u tevens de nodige bescherming als er geen afsluitbare serverruimte beschikbaar is.

In dit boek wordt een fouttolerante/redundante *AD DS* en *DNS* ingericht op één site. Een RODC past daar dus niet in.

- Als *Site name* staat *PFBudel* geselecteerd. Omdat dit de enige site is waarover u op dit moment beschikt, is dat de juiste keuze.
- 6 Configureer zo nodig de sectie *Specify domain controller capabilities and site information* van het wizardvenster *Domain Controller Options* zoals in afbeelding 2-61.
- Vul het password voor de *DSRM* tweemaal in. Gebruik uw eigen administrator password.
- Klik op de knop *Next >*.

Vervolgens verschijnt het wizardvenster *DNS Options* van afbeelding 2-62.

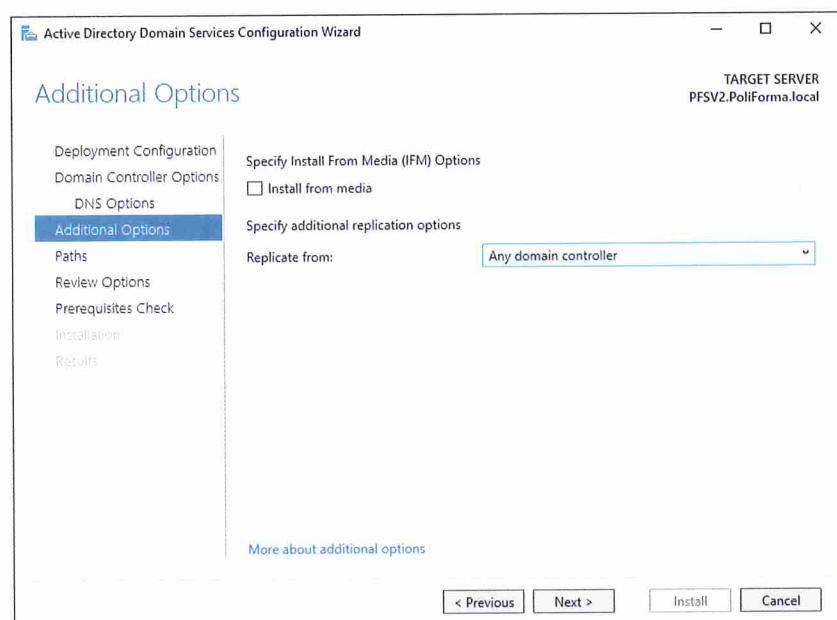


Afb. 2-62 DNS Delegation

Aan de bestaande DNS-omgeving wijzigt u voorlopig niets. Pas in hoofdstuk 3 wordt nader op DNS ingegaan.

- 7 Klik de foutmelding weg.  
Klik op de knop *Next >*.

Vervolgens verschijnt het wizardvenster *Additional Options* van afbeelding 2-63.



Afb. 2-63 De replicatie

### IFM

Als u een additionele DC configureert, moet er een kopie van AD op worden geïnstalleerd. Bij een DC is dat een read/write-kopie. Bij een RODC is dat een read only-kopie. U kunt die kopie over het netwerk laten ophalen bij een DC. U kunt ook van tevoren een kopie maken op een opslagmedium, bijvoorbeeld op een dvd. IFM (Install From Media) gebruikt een kopie op een opslagmedium.

In dit boek wordt het netwerk gebruikt om de kopie over te brengen vanaf DC *PFSV1*.

- 8 Selecteer met de keuzelijst *Replicate from* de optie *PFSV1.PoliForma.local*. Klik op de knop *Next >*.

Het laatste wizardvenster is *Paths* met de daarin bekende plaats van de bestanden.

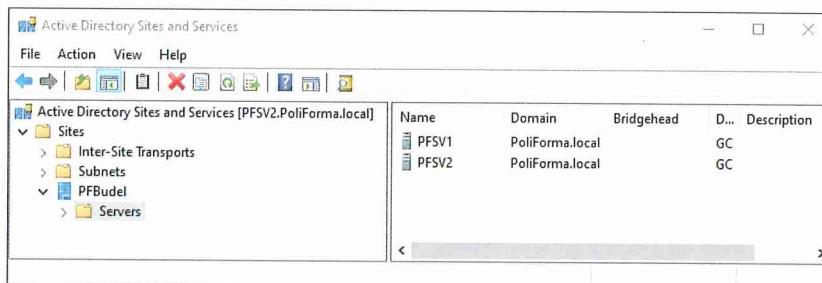
- 9 Breng in het wizardvenster *Paths* geen wijzigingen aan. Klik op de knop *Next >*.

De gebruikelijke samenvatting verschijnt in het wizardvenster *Review Options*.

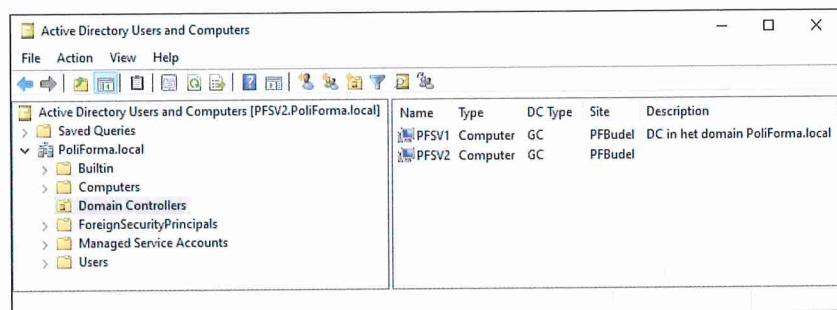
- 10 Controleer de instellingen. Herstel als dat nodig is. Klik op de knop *Next >*.

De *Prerequisites Check* wordt uitgevoerd. Deze mag geen problemen opleveren anders heeft u de *Active Directory Domain Services Configuration Wizard* niet goed ingesteld. Gebruik in dat geval de knop *Previous* en herstel.

- 11 Klik op de knop *Install*.
  - De installatie gaat nu van start. De voortgang kunt u volgen. In de huidige situatie duurt het gehele proces ongeveer 5 minuten. Na afloop verschijnt het bekende slotvenster *Results* van de wizard. Daarna wordt automatisch server *PFSV2* herstart.
- 12 Log na het herstarten op DC *PFSV2* in als domain *Administrator*.  
Controleer op DC *PFSV2* het onderstaande.
  - Op het *Dashboard* van de *Server Manager* moeten de server roles *AD DS* en *DNS* te zien zijn. Het kan even duren voordat deze verschijnen.
  - *AD DS* en *DNS* zijn nu fouttolerant/redundant.
    - In afbeelding 2-64 ziet u dat DC *PFSV2* in de MMC *Active Directory Sites and Services* is opgenomen in de site *PFBudel*. Tevens ziet u dat DC *PFSV2* een GCS is.
    - In afbeelding 2-65 ziet u dat DC *PFSV2* in de MMC *Active Directory Users and Computers* verhuisd is van de container *Computers* naar de OU *Domain Controllers*. Tevens ziet u ook hier dat DC *PFSV2* een GCS is.
- 13 Controleer op DC *PFSV2* de instellingen van de afbeeldingen 2-64 en 2-65.  
Sluit daarna op beide DC's alle vensters behalve de *Server Manager*.



Afb. 2-64 Gelijkwaardig



Afb. 2-65 Ook gelijkwaardig

## Controle op correct repliceren

Beide servers zijn nu gelijkwaardige DC's in het domain *PoliForma.local*. AD wordt op beide DC's gelijk gehouden door het **replicatieproces**. Beide DC's zijn elkaar replicatiepartners. Omdat beide DC's zijn opgenomen in de site *PFBudel* gaat het repliceren via het LAN. Dat gaat snel en pleegt nauwelijks een aanslag op de netwerkcapaciteit. Als het *Domain Functional Level* staat ingesteld op *Windows Server 2016* of hoger wordt er 15/3 gerepliceerd. Elke wijziging op een van de replicatiepartners wordt binnen 15 seconden nadat de verandering is aangebracht op de andere ook doorgevoerd. Daarbij kan het 3 seconden duren voordat de replicatiepartner wordt gewaarschuwd.

Het repliceren bekijkt u nu met behulp van een eigenschap van DC PFSV2. In afbeelding 2-65 ziet u dat de eigenschap *Description* van DC PFSV1 gevuld is met *DC in het domain PoliForma.local*. Op DC PFSV1 geeft u DC PFSV2 dezelfde omschrijving. De replicatie zal er daarna voor zorgen dat ook op DC PFSV2 die eigenschap wordt gevuld met dezelfde inhoud.

- 14 Start op DC PFSV1 de MMC Active Directory Users and Computers.

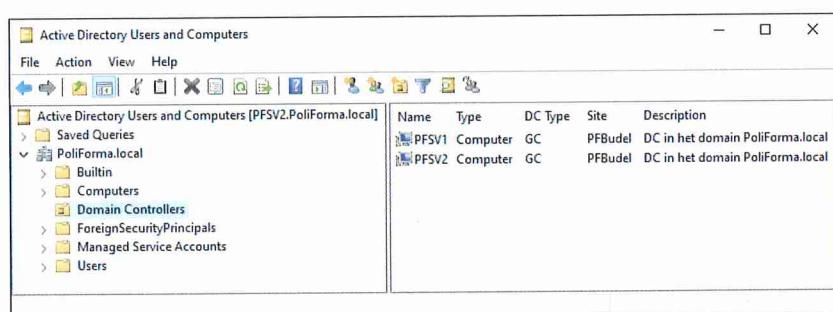
Haal het tabblad *General* van het eigenschappenvenster van DC PFSV2 voor u.

Vul de eigenschap *Description* met *DC in het domain Poliforma.local*

Klik op de knoppen *Apply* en *OK*.

Start ook op DC PFSV2 de MMC Active Directory Users and Computers.

Haal de inhoud van de OU Domain Controllers voor u (afbeelding 2-66).



Afb. 2-66 Er is gerepliceerd

U ziet dat de replicatie inmiddels heeft plaatsgevonden. De eigenschap *Description* is ook op DC PFSV2 ingevuld.

- 15 Sluit op beide servers alle vensters.

Sluit beide servers af.

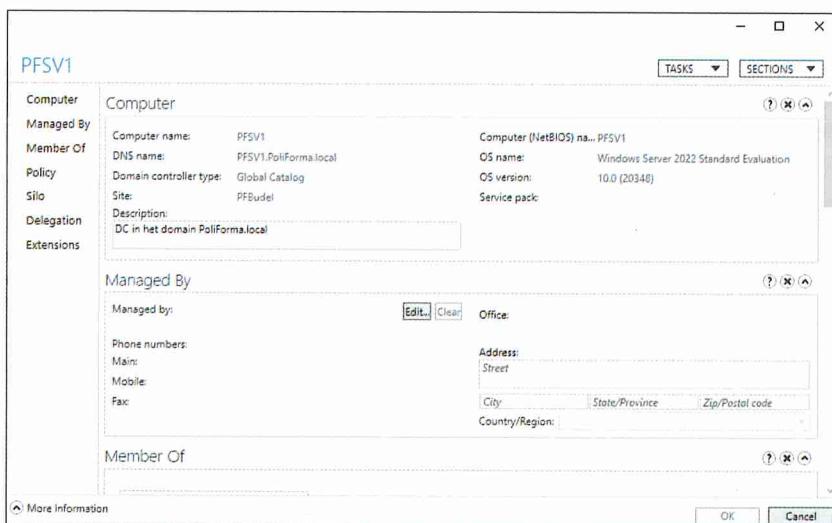
U heeft AD DS en DNS fouttolerant gemaakt in het domain *PoliForma.local* van uw testnetwerk. Het repliceren werkt zoals het hoort.

## 2.5 Opdrachten

Het *Active Directory Administrative Center* is een uitgebreide beheertool. Deze is geïntroduceerd in Windows Server 2012. Het *Active Directory Administrative Center* is bedoeld voor het dagelijks onderhoud. Het is ook daarvoor ontworpen.

De MMC *Active Directory Users and Computers* die u hiervoor al gebruikt heeft, is strak georganiseerd op computers, DC's, gebruikers, groepen enzovoort. Hetzelfde geldt voor de MMC *Active Directory Sites and Services*. Daarin organiseert u sites met hun IPv4-adressen en beheert u eventueel de verbindingen tussen die sites. De eigenschappen van een object zijn in deze MMC's gerangschikt op tabbladen in het bijbehorende eigenschappenvensster. U beschikt over alle mogelijkheden.

Het *Active Directory Administrative Center* is daarentegen taakgeoriënteerd. U beschikt over veel, maar niet alle mogelijkheden. In afbeelding 2-67 ziet u als voorbeeld de eigenschappen van DC PFSV1. Vergelijk met de afbeeldingen 2-40 t/m 43. Allerlei keuzes geven u verder de mogelijkheid deze beheertool naar uw eigen werkstandigheden in te richten.



Afb. 2-67 De eigenschappen van DC PFSV1 in het *Active Directory Administrative Center*



### Opdracht 2.5.1: AD Administrative Center

30 min.

#### In deze opdracht:

- Richt u het *Active Directory Administrative Center* voor uw testnetwerk in naar uw persoonlijke wensen.

#### Voor deze opdracht heeft u nodig:

- De virtuele machines *PFSV1* en *PFSV2* zoals geconfigureerd na de vorige paraagraaf.
- Het werkblad bij opdracht 2.5.1 waarop u uw werkzaamheden vastlegt.
- Tijd: ± 30 minuten.

#### Opdrachтинstructies

- Experimenteer met het *Active Directory Administrative Center* zodat u weet hoe deze tool werkt. Wijzig geen instellingen zodat alles hetzelfde blijft functioneren.
- Richt het *Active Directory Administrative Center* voorlopig zo in, dat u uw DC's eenvoudig kunt selecteren om de eigenschappen ervan in het detailvenster te kunnen bekijken en bewerken (afbeelding 2-67). Bestudeer enkele eigenschappen van uw DC's om vertrouwd te raken met de manier waarop u deze tool kunt gebruiken.

## 2.6 Damage control 2

Tot slot van dit hoofdstuk exporteert u de beide virtuele machines weer. Mochten uw virtuele machines in het volgende hoofdstuk in de problemen komen, dan kunt u daarop terugvallen.



### Opdracht 2.6.1: Veilig stellen

10 min.

#### In deze opdracht:

- Exporteert u uw virtuele machines.

#### Voor deze opdracht heeft u nodig:

- Uw virtuele servers *PFSV1* en *PFSV2*.
- Het werkblad bij opdracht 2.6.1 waarop u de instellingen vastlegt.
- Tijd: ± 10 minuten.

#### Opdrachтинstructies

In het voorgaande heeft u de virtuele machines *PFSV1* en *PFSV2* geëxporteerd naar de map *\VMsNaHo1*.

- 1 Verwijder de map \VMsNaHo1 met inhoud en al.
  - 2 Maak op dezelfde plaats de map \VMsNaHo2 aan.
  - 3 Exporteer vanuit *Hyper-V-beheer* de beide virtuele machines *PFSV1* en *PFSV2* naar de map \VMsNaHo2.
  - 4 Sluit geordend *Hyper-V-beheer* af.
- 



1-Ho2

