

2 Active Directory

2.0 In dit hoofdstuk

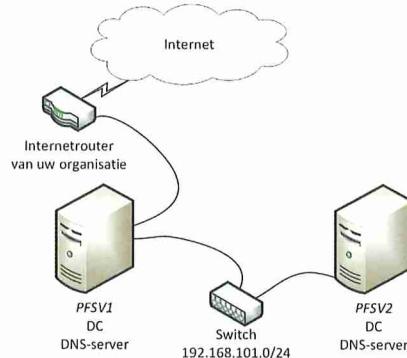
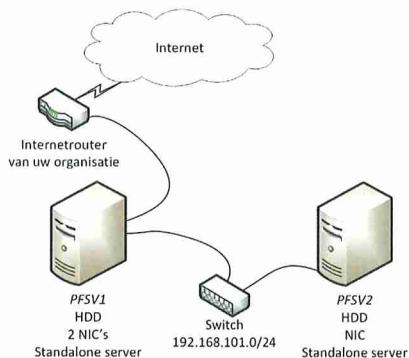


1_Ho2

Na het vorige hoofdstuk beschikt u in uw testopstelling over twee virtuele stand-alone Windows Server 2022-servers (afbeelding 2-1). In dit hoofdstuk begint u met de opbouw van het **bedrijfsnetwerk** voor PoliForma BV. Een bedrijfsnetwerk wordt ook wel een **client/server-netwerk** genoemd. In een bedrijfsnetwerk vervullen servers functies (diensten) voor het netwerk. Van die diensten kan door de clients (werkstations) in het netwerk gebruikgemaakt worden.

In dit hoofdstuk zet u de eerste stap op weg naar dat bedrijfsnetwerk. U promoveert daarvoor standalone server *PFSV1* tot DC (Domain Controller). Voor **fout-tolerantie/redundantie** maakt u van server *PFSV2* eerst een member server en daarna een tweede DC. In het verloop van dit hoofdstuk worden al deze begrippen uitvoerig toegelicht. Van elk type server leert u de belangrijkste karakteristieken.

Na dit hoofdstuk heeft u dan een testnetwerkomgeving waarin twee virtuele servers als DC actief zijn (afbeelding 2-2).



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

A Kennis

- U weet dat peer-to-peer-netwerken decentraal beheerd worden en client/server-netwerken centraal (paragraaf 2.1).

- U weet wat Active Directory is. U kent de daaraan gerelateerde begrippen en hun onderlinge samenhang (paragraaf 2.1).
- U weet wat een server role, een role service, een feature en een service is. U begrijpt hun onderlinge samenhang (paragraaf 2.1).
- U kent de belangrijkste kenmerken en eigenschappen van een DC (paragraaf 2.2).
- U kent de belangrijkste kenmerken van een member server (paragraaf 2.3).
- U weet wat er nodig is om een domain fouttolerant/redundant te laten werken (paragraaf 2.4).

B Vaardigheden

- U kunt server roles installeren (practicum 2.1.1).
- U kunt Active Directory op een server installeren (practicum 2.1.1).
- U weet de weg te vinden in de MMC's *Active Directory Users and Computers* en *Active Directory Sites and Services* (practicum 2.2.1).
- U kunt van een standalone server een member server maken in een domain (practicum 2.3.1).
- U kunt een domain fouttolerant/redundant maken door daarin een tweede DC op te nemen (practicum 2.4.1).
- U kunt de replicatie tussen twee DC's controleren (practicum 2.4.1).
- U kunt het *Active Directory Administrative Center* naar uw eigen idee inrichten (opdracht 2.5.1).

2.1 Active Directory

In het vorige hoofdstuk heeft u de standalone server *PFSV1* ingericht en geconfigureerd met de basisinstellingen. Kenmerkend voor een standalone server is dat onder andere de gebruikersgegevens worden opgeslagen in de SAM. Elke machine beschikt over een eigen SAM. Het beheer bij verschillende machines in een peer-to-peer-netwerk moet daarom op elke machine afzonderlijk worden uitgevoerd (bijlage A). **Decentraal beheer** wordt dat genoemd.

In een client/server-bedrijfsnetwerk is juist sprake van **centraal beheer**. De gegevens van de netwerkgebruikers worden in één database bewaard (bijlage A). Overigens niet alleen de gebruikersgegevens, maar in algemene zin de gegevens van alle **netwerkobjecten**. Daarmee fungeert die database als een soort Wikipedia voor het netwerk. In een client/server-bedrijfsnetwerk met Windows Server 2022 als netwerkbesturingssysteem heet die database **AD** (Active Directory). AD werd voor het eerst geïntroduceerd bij het verschijnen van Windows 2000 Server.

AD is dus een database. Die database wordt bewaard in het bestand *ntds.dit*. NTDS is een afkorting van New Technology Directory Service. DIT is een afkorting van Data Information Table. Voor het bewerken van een database gebruikt u een databaseprogramma. De database AD wordt bewerkt met een databaseprogramma dat **Directories** heet. Dat databaseprogramma zit in Windows Server 2022 ingebouwd.

De database AD en het databaseprogramma Directories worden samen de **AD DS** (Active Directory Domain Services) genoemd. Een Windows Server 2022-machine waarop AD is geïnstalleerd, wordt een **DC** (Domain Controller) genoemd. De open standaard waarop AD is gebaseerd, is **LDAP** (Lightweight Directory Access Protocol).

AD is zo ontworpen dat het naadloos aansluit bij de geldende internetstandaarden. Zo heeft AD onder andere **DNS** (Domain Name System) nodig. Voorlopig is het voldoende als u weet dat via DNS een computer kan worden opgespoord via zijn computernaam. In de loop van dit hoofdstuk leert u DNS al een beetje kennen. In hoofdstuk 3 wordt er dieper op ingegaan.

Azure Active Directory

In de Azure cloud van Microsoft is Azure Active Directory beschikbaar. Azure Active Directory is de identiteits- en toegangsbeheerservice in die cloudomgeving waarmee medewerkers van een organisatie zich kunnen aanmelden en toegang kunnen krijgen tot resources, zoals:

- interne resources. Denk daarbij aan apps op het bedrijfsnetwerk en intranet samen met cloud apps die door de eigen organisatie als maatwerk zijn ontwikkeld.
- externe resources. Denk daarbij aan omgevingen zoals Microsoft 365, de Azure-portal en tal van andere SAAS-toepassingen.

Ook in de Amazon cloud AWS (Amazon Web Services) bestaat een dergelijke voorziening.



Practicum 2.1.1: Domain Controller PFSV1

90 min.

In dit practicum:

- Installeert u op server *PFSV1* de server role *Active Directory Domain Services*.
- Maakt u van server *PFSV1* een DC.

Voor dit practicum heeft u nodig:

- De virtuele standalone server *PFSV1* van uw testnetwerk uit afbeelding 2-1 zoals geconfigureerd na het vorige hoofdstuk.
- Het werkblad bij practicum 2.1.1 waarop u uw werkzaamheden vastlegt.
- Tijd: ± 90 minuten.



Server role & AD installeren

Korte practicuminstructies

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

- a Zorg dat op uw virtuele standalone server *PFSV1* de server role *Active Directory Domain Services* is geïnstalleerd.

- b Configureer *AD DS* op server *PFSV1* met de volgende instellingen:
- Het nieuwe domain is het eerste domain van de eerste tree in een nieuw forest.
 - De naam voor het forest root domain is *PoliForma.local*.
 - Het *Forest Functional Level* is de jongste versie van *Windows Server*.
 - Het *Domain Functional Level* is ook de jongste versie van *Windows Server*.
 - Maak van server *PFSV1* gelijk ook een DNS-server.
 - Gebruik uw administrator password ook voor de *DSRM*.
 - Stel geen DNS delegation in.
 - De NetBIOS-naam van het domain is: *POLIFORMA*.
 - De map voor *ntds.dit* is *C:\Windows\NTDS*.
 - De map voor de logs is ook *C:\Windows\NTDS*.
 - De *SYSVOL*-map is *C:\Windows\SYSVOL*.
- Log na het herstarten van server *PFSV1* in als *Administrator* van het domain.

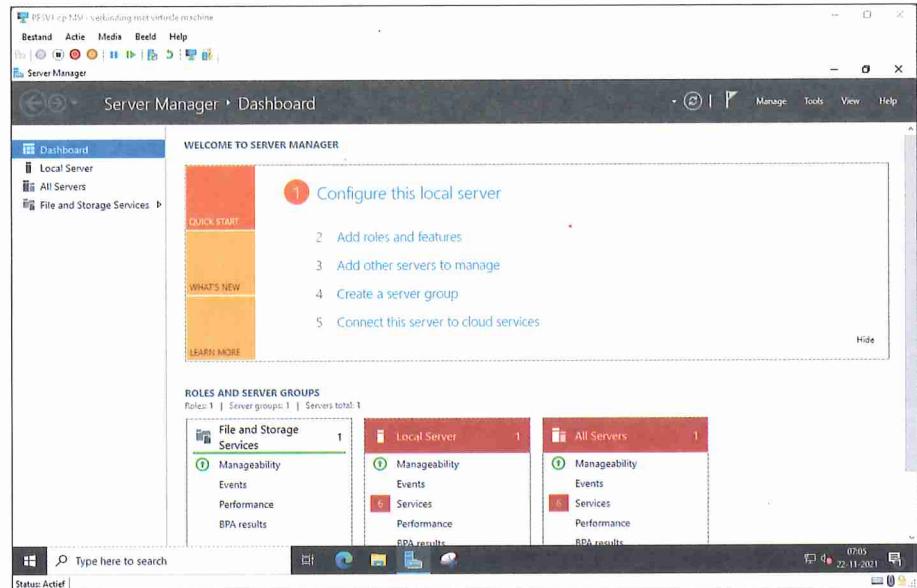
Gedetailleerde uitwerking van het practicum

Het promoveren van standalone server *PFSV1* tot DC vult in twee delen uiteen:

- Als eerste installeert u op uw virtuele standalone server *PFSV1* de server role *Active Directory Domain Services*.
- Als tweede configureert u die server role. Daarmee installeert u AD op standalone server *PFSV1* en wordt deze daarmee een DC.

- 1 Zorg dat u als *Administrator* ingelogd bent op uw virtuele standalone server *PFSV1*.

Zorg zo nodig dat de *Server Manager* voor u staat (afbeelding 2-3).



Afb. 2-3 De *Server Manager* op server *PFSV1*

Op server PFSV1 de server role Active Directory Domain Services installeren

Als eerste moet dus de server role AD DS (Active Directory Domain Services) geïnstalleerd worden. Nu zijn er in Windows Server 2022 server roles, role services, features en services. Pas als u ermee werkt, zullen deze begrippen echt betekenis voor u krijgen. Hieronder alvast een toelichting.

Server roles, role services, features en services

Een **server role** stelt een server in staat een specifieke totaalfunctie te vervullen in het netwerk. Een dergelijke totaalfunctie wordt ook wel een **role** genoemd. Op een server kunnen één of verschillende server roles geïnstalleerd worden. Een server kan in een netwerk dus tegelijkertijd verschillende roles vervullen. In het vervolg gaat u dit zien.

Voorbeeld: Als u later van server PFSV1 een print server maakt, installeert u daarvoor de server role *Print and Document Services*.

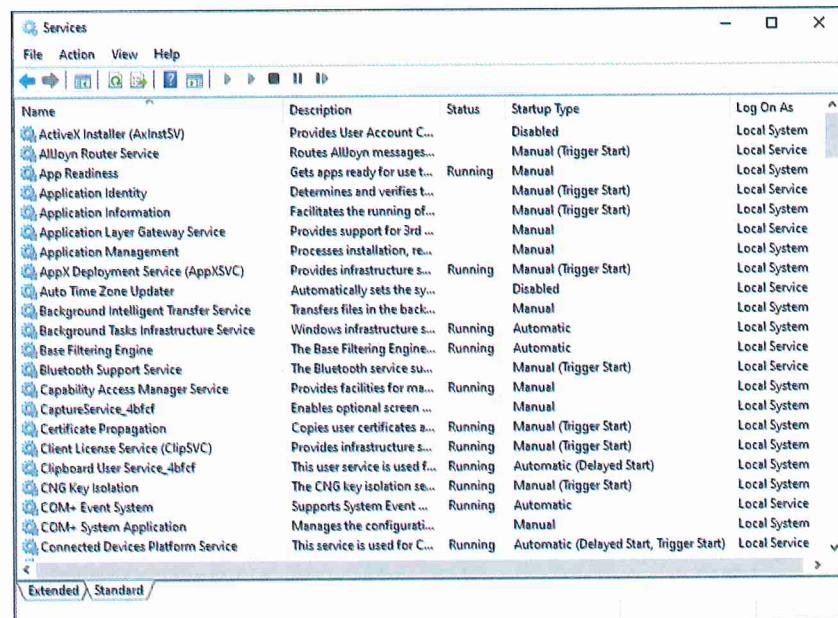
Een **role service** is een onderdeel van een server role. Geïnstalleerd verzorgt een role service een deelfunctie van de betreffende server role. Role services vullen dus de betreffende server role met passende functionaliteit. Door geschikte role services te installeren, kunt u zeer precies de deelfunctie van de server role instellen. Tussen role services kunnen **dependencies** (afhankelijkheden) bestaan. Dit betekent dat een role service andere role services nodig kan hebben. Gelukkig geeft de *Add Roles and Features Wizard* dat voor u aan als dat het geval is. Er zijn overigens ook server roles waarvan de functionaliteit bepaald wordt door één role service. Daarbij zijn dependencies natuurlijk niet van toepassing.

Voorbeeld: Als u later van server PFSV1 een print server maakt, installeert u daarvoor de server role *Print and Document Services*. De server role *Print and Document Services* bestaat uit de role services *Print Server*, *Internet Printing* en *LPD Service*. Als er geen Unix-machines in het netwerk draaien, is de role service *LPD Service* niet nodig. Als het printen via het internet niet van toepassing is, is ook de role service *Internet Printing* niet nodig. Moet er via het internet wel geprint kunnen worden, dan is de role service *Internet Printing* wel nodig. Deze laatste heeft echter de role service *Print Server* nodig om te kunnen werken. Die is daarvan afhankelijk.

Een **feature** levert een aanvullende functie op de server. Vaak ondersteunen features ook server roles en role services door te zorgen voor verbeterde samenwerking en beheertools. Dat heeft ook meestal verbetering van de performance tot gevolg. Features worden daarom vaak (semi-)automatisch geïnstalleerd als gevolg van het installeren van een server role of role service. Ook daarvoor zorgt dan de *Add Roles and Features Wizard*.

Voorbeeld: Als u later van server *PFSV1* een print server maakt, installeert u daarvoor de role service *Print Server* uit de server role *Print and Documents Services*. Tijdens die installatie kunt u de feature *Print and Document Services Tools* laten installeren. Daarmee is de tool *Print Management* om uw printomgeving in te richten en te beheren na de installatieprocedure direct beschikbaar.

Server roles, role services en features zijn er om het beheer voor u inzichtelijk te maken. Op machineniveau komen server roles, role services en features neer op combinaties van geïnstalleerde services. Een **service** is een programma van het besturingssysteem dat op de achtergrond draait. Een service voorziet een machine van functionaliteit. Ook services kunnen dependencies vertonen. In afbeelding 2-4 ziet u welke services er allemaal al draaien om een standalone server te laten functioneren.



The screenshot shows the Windows Services console window. The title bar reads "Services". The menu bar includes "File", "Action", "View", and "Help". Below the menu is a toolbar with icons for search, refresh, and other actions. The main area is a table with columns: "Name", "Description", "Status", "Startup Type", and "Log On As". The table lists numerous services, such as ActiveX Installer, Allboyn Router Service, App Readiness, Application Identity, Application Information, Application Layer Gateway Service, Application Management, AppX Deployment Service, Auto Time Zone Updater, Background Intelligent Transfer Service, Background Tasks Infrastructure Service, Base Filtering Engine, Bluetooth Support Service, Capability Access Manager Service, CaptureService, Certificate Propagation, Client License Service, Clipboard User Service, CNG Key Isolation, COM+ Event System, COM+ System Application, and Connected Devices Platform Service. Most services are set to "Running" status. The "Log On As" column indicates whether the service runs under "Local System", "Local Service", or "Local Service (Delayed Start)". At the bottom of the table, there are tabs for "Extended" and "Standard".

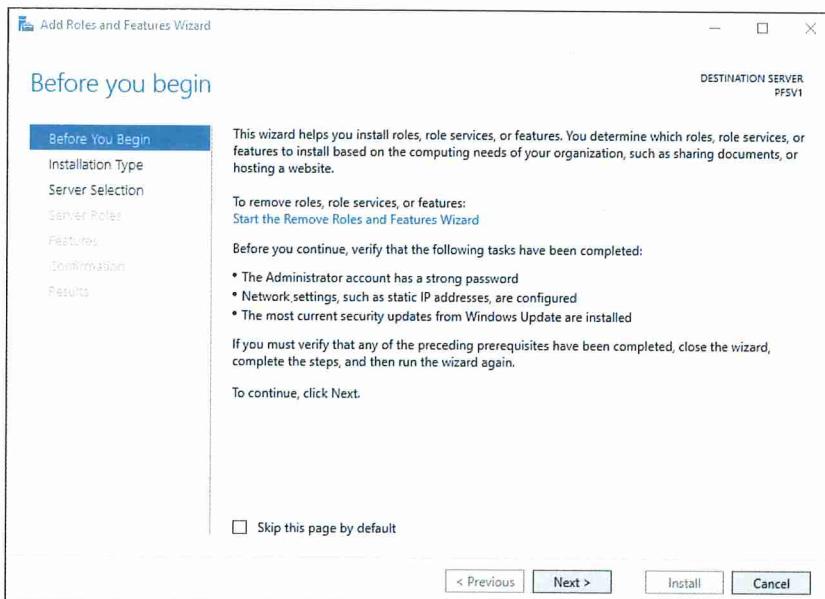
Afb. 2-4 Services op standalone server *PFSV1*

Nu dan de installatie van de server role *AD DS*. Daarvoor doorloopt u de wizard *Add Roles and Features*. Omdat dit voor u de eerste keer is worden alle wizardvensters getoond en toegelicht.

- 2 Klik in het detailvenster van het *Dashboard* van de *Server Manager* op de optie *2 Add roles and features*. U kunt ook op de optie *Add Roles and Features* klikken in het menu *Manage*.

 [2 Add roles and features](#)

De *Add Roles and Features Wizard* gaat van start met het wizardvenster *Before you begin* (afbeelding 2-5).



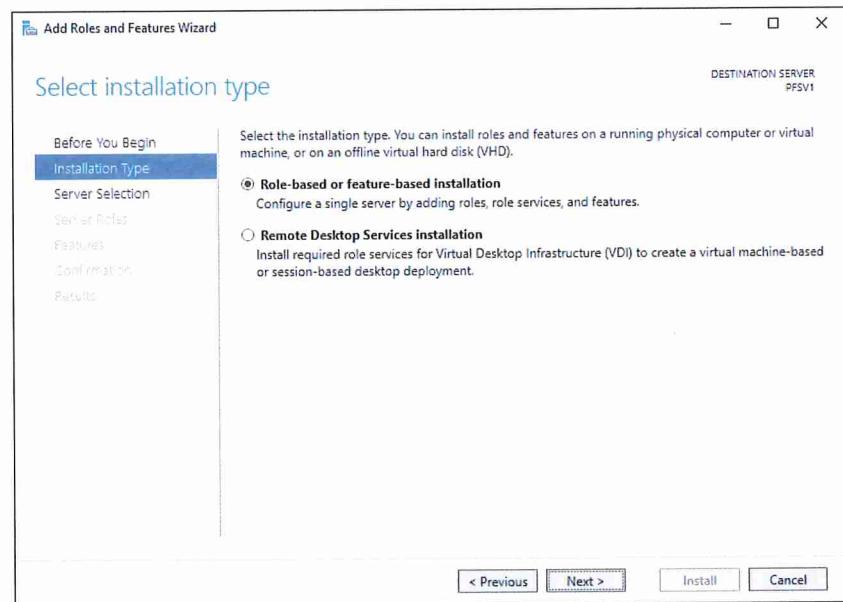
Afb. 2-5 Server roles, role services en features installeert u met een wizard

3 Lees de informatie op het scherm.

Dit wizardvenster is telkens hetzelfde. Plaats daarom een vink voor *Skip this page by default*.

Klik op de knop *Next >*.

Het wizardvenster *Select installation type* van afbeelding 2-6 verschijnt.

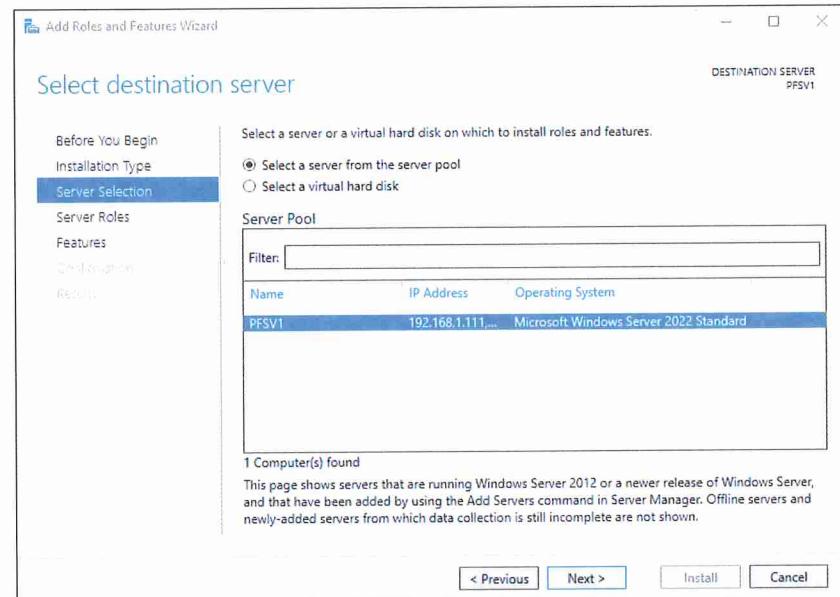


Afb. 2-6 Alleen *Role-based or feature-based installation*

De installatie van de server role AD DS moet alleen op standalone server PFSV1 gebeuren.

- 4 Selecteer zo nodig *Role-based or feature-based installation*. Klik op de knop *Next >*.

Nu verschijnt het wizardvenster *Select destination server* (afbeelding 2-7).

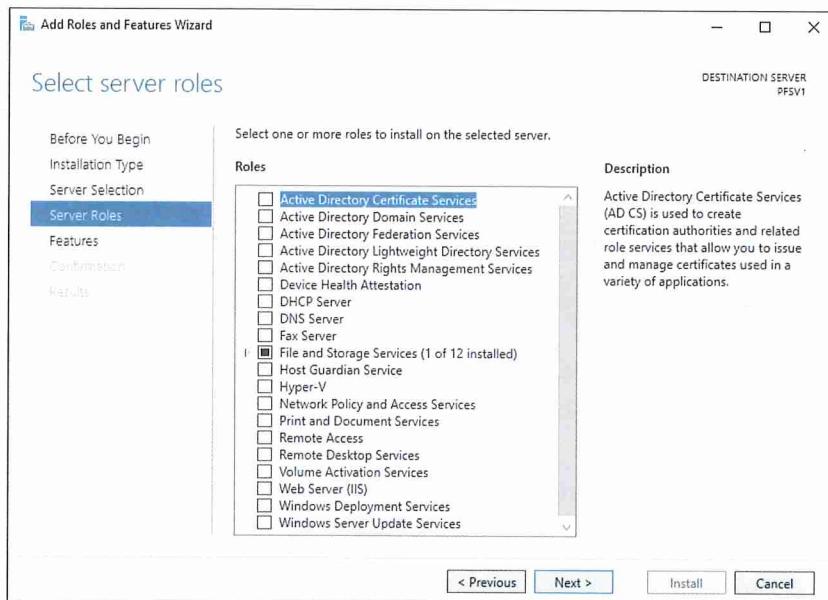


Afb. 2-7 Op welke server

Server *PFSV1* staat al voor u geselecteerd.

- 5 Klik op de knop *Next >*.

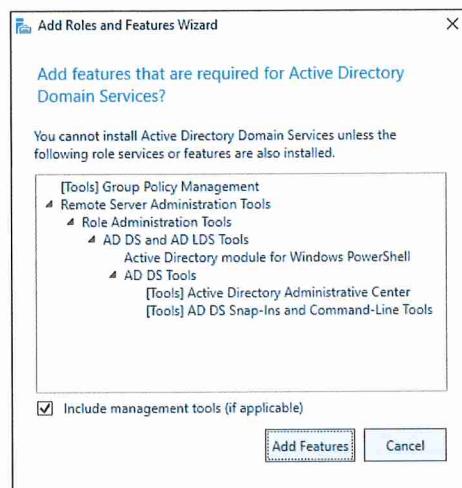
Het volgende wizardvenster heet *Select server roles* (afbeelding 2-8). Daarin kunt u de te installeren server role(s) selecteren door deze te voorzien van een vink.



Afb. 2-8 Welke server role(s) installeren

- 6 Plaats in de keuzelijst *Roles* een vink voor de server role *Active Directory Domain Services*.

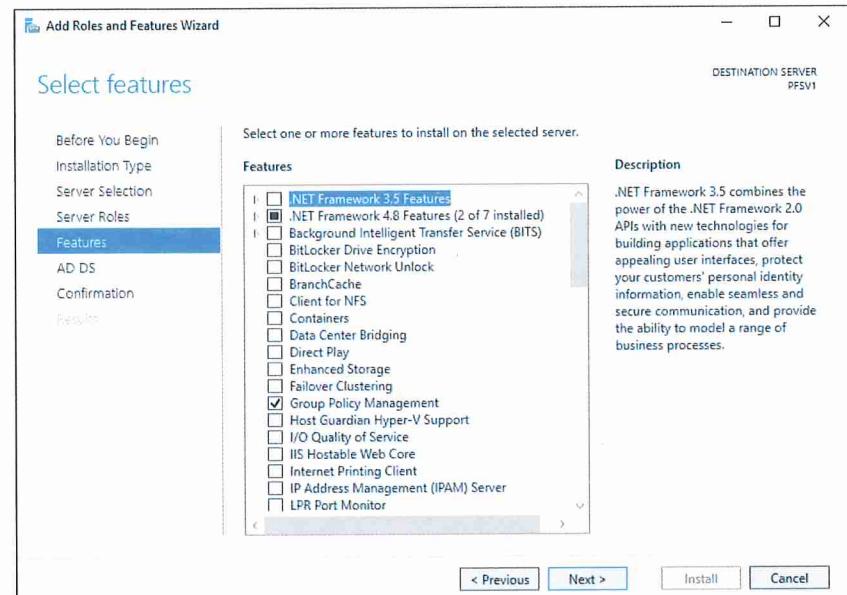
Gelijk verschijnt het venster *Add Roles and Features Wizard* van afbeelding 2-9. Door de keuze van de server role *AD DS* kunt u gelijk een aantal bijbehorende features laten installeren. Pas later zult u het effect hiervan zien.



Afb. 2-9 Deze features zijn absoluut nodig

- 7 Plaats zo nodig een vink voor *Include management tools (if applicable)*. Klik op de knop *Add Features* en de server role AD DS zal voorzien zijn van een vink. Klik op de knop *Next >*.

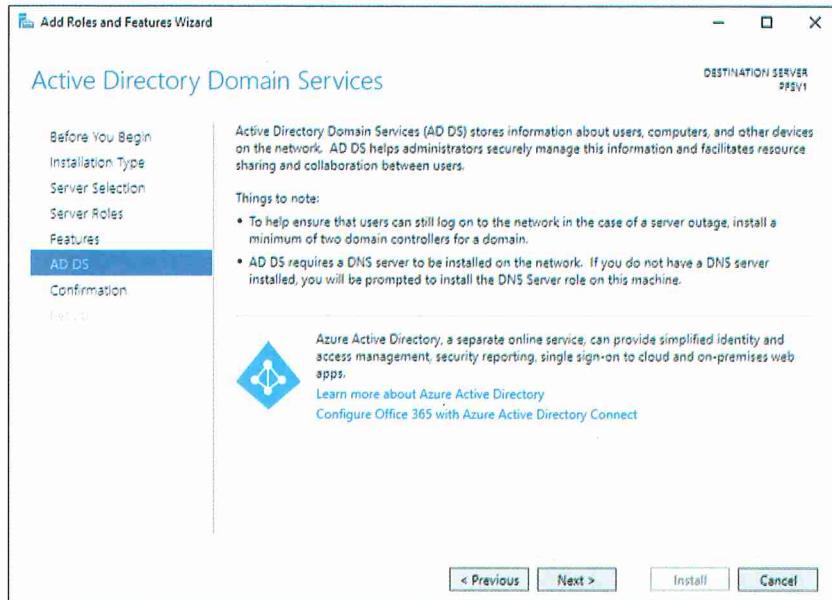
Voor het geval u nog andere features wilt installeren, verschijnt vervolgens het wizardvenster *Select features* (afbeelding 2-10). Op dit moment is dit niet nodig. Onder andere de features *Group Policy Management* en *Remote Server Administration Tools* zijn door de wizard zelf voorzien van een vink. Laat die vinken gewoon staan.



Afb. 2-10 Geen bijkomende features nodig

8 Klik op de knop *Next >*.

Vervolgens verschijnt het wizardvenster *Active Directory Domain Services* van afbeelding 2-11.



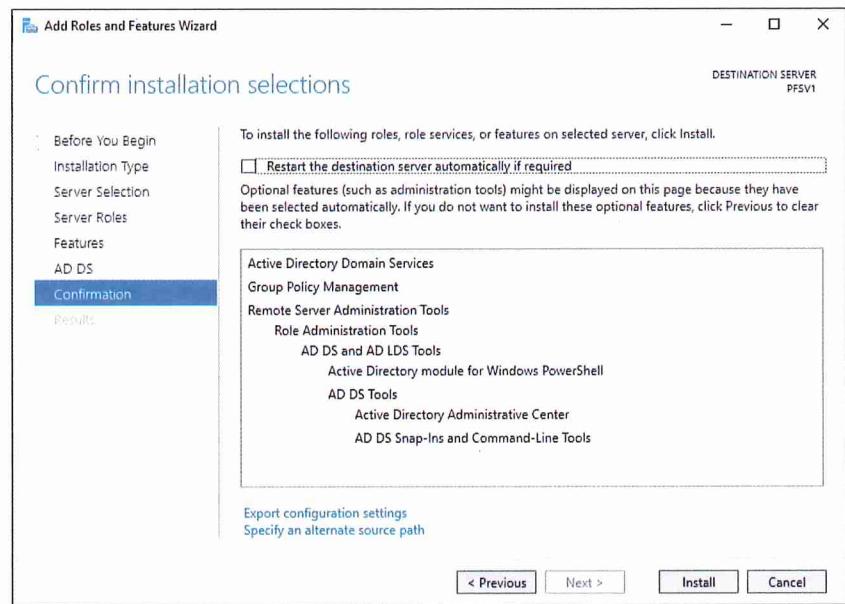
Afb. 2-11 Opmerkingen bij de installatie van *AD DS*

Toelichting

- De eerste opmerking gaat over bedrijfszekerheid. Daarvoor zijn in een productieomgeving altijd tenminste twee DC's nodig om te zorgen voor **fouttolerantie/redundantie**. Als een van de DC's uitvalt, werkt het netwerk gewoon door omdat de andere nog functioneert. In het vervolg van dit hoofdstuk zorgt u daar dan ook voor.
- De tweede opmerking gaat over DNS. DNS is absoluut noodzakelijk. Daarom zal er op een aanwezige DNS-omgeving worden gecontroleerd.

9 Klik op de knop *Next >*.

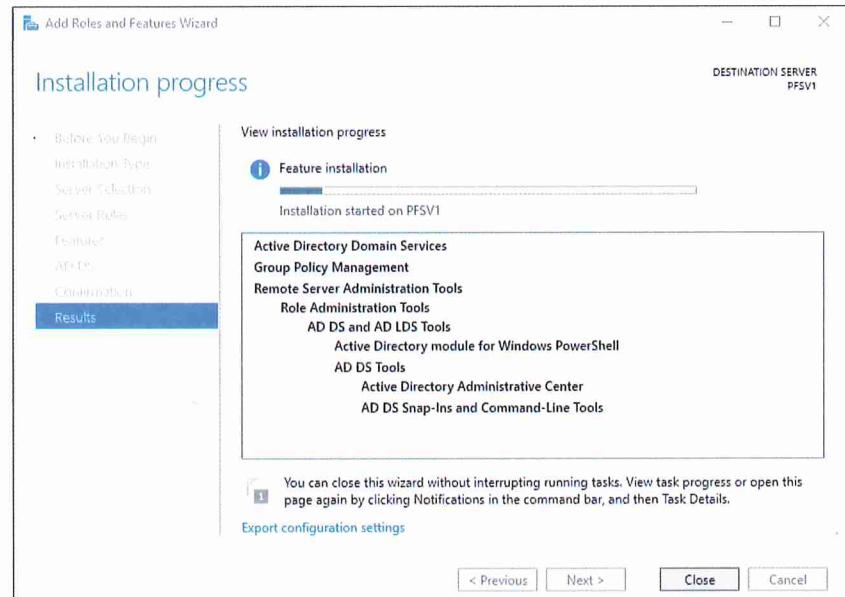
Tenslotte verschijnt er nog een wizardvenster met informatie over de gemaakte keuzes (afbeelding 2-12). In het wizardvenster *Confirm installation selections* kunt u aangeven dat de machine automatisch herstart na de installatie als dat nodig is. Omdat na de installatie van *AD DS* ook nog AD geïnstalleerd moet worden, laat u niet automatisch herstarten.



Afb. 2-12 Informatie over AD DS zoals dat zal worden geïnstalleerd

- 10 Zorg er zo nodig voor dat er **geen** vink staat voor *Restart the destination server automatically if required*. Bevestig de gemaakte keuzes door op de knop *Install* te klikken en de installatie te laten beginnen.

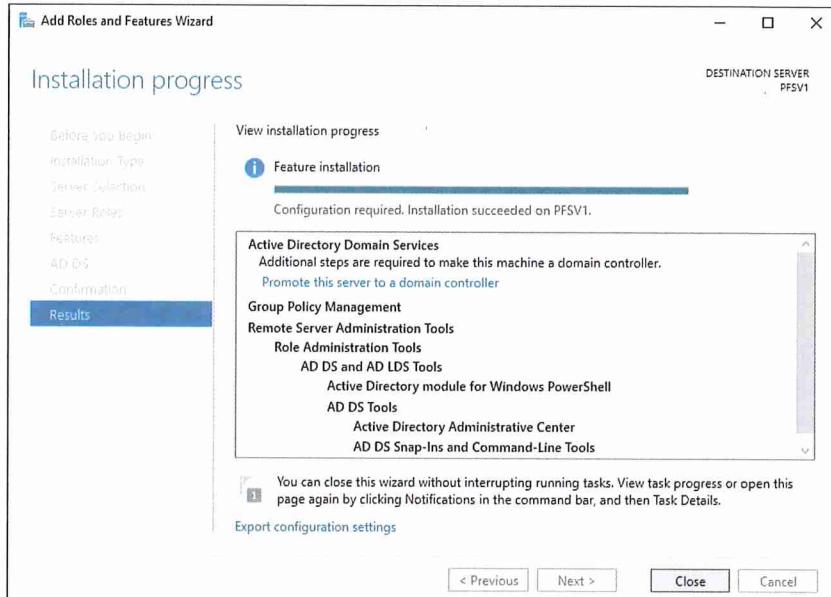
De vordering van de installatie kunt u volgen in het wizardvenster *Installation progress* (afbeelding 2-13). De installatie duurt een paar minuten.



Afb. 2-13 De installatie

Pas op! Klik niet op de knop *Close*.

Na de installatie ziet u of de installatie geslaagd is (afbeelding 2-14). Om van de machine een Domain Controller te maken, is echter nog meer nodig. In het voorgaande is dat al aangekondigd. U ziet daarom dat u direct van een advies wordt voorzien: de link *Promote this server to a domain controller*. Dat advies volgt u direct ook op.



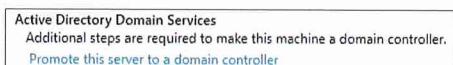
Afb. 2-14 Het installatieresultaat

- 11 Laat dit wizardvenster zo voor u staan.

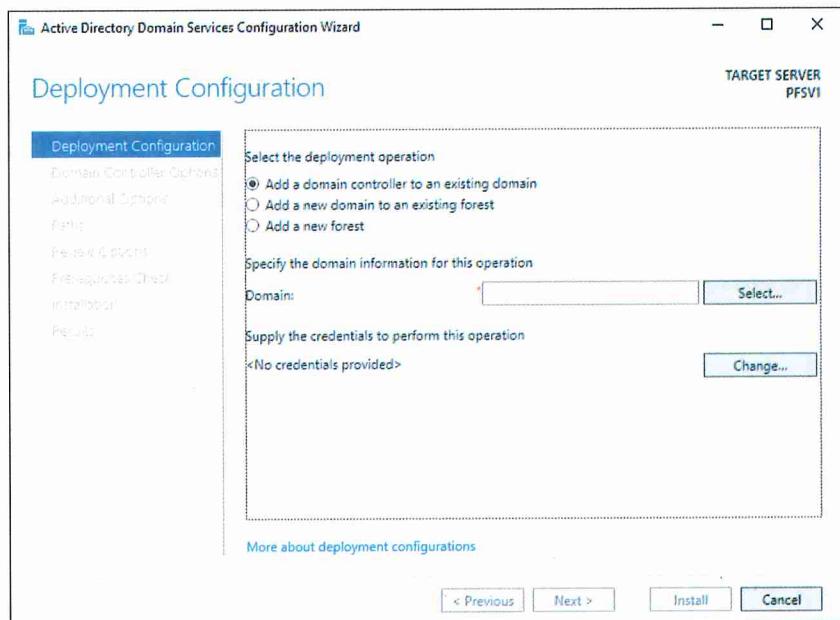
De promotie van server PFSV1 tot Domain Controller

De tweede stap is het configureren van de server role *AD DS*. Concreet is dat het promoveren van server *PFSV1* tot DC. Dat komt neer op het installeren van AD op server *PFSV1*.

- 12 Klik in het wizardvenster op de link *Promote this server to a domain controller*.



Daarmee start binnen de *Add Roles and Features Wizard* de *Active Directory Domain Services Configuration Wizard*. Het eerste wizardvenster is *Deployment Configuration* (afbeelding 2-15).



Afb. 2-15 De promotie tot DC gaat van start

De keuzes die u in dit wizardvenster moet maken, zijn werkelijk essentieel. U moet een keuze maken uit drie mogelijke acties. Om die te begrijpen eerst een korte toelichting op de begrippen domain, site, forest en tree zoals die in Windows Server 2022 worden gebruikt.

Domain

Een **domain** is een verzameling netwerkobjecten die gezamenlijk opgenomen zijn in één AD DS. Zoals u weet, bestaat de AD DS uit de database Active Directory (*ntds.dit*) en het databaseprogramma Directories. Met de netwerkobjecten worden gebruikers, gebruikersgroepen en computers bedoeld. Ook mappen en printers die aan gebruikers ter beschikking zijn gesteld, kunnen tot die netwerkobjecten behoren. Juist het feit dat de netwerkobjecten in één AD DS zijn opgenomen, maakt centraal beheer daarvan mogelijk. In tekeningen wordt een domain met een driehoek weergegeven.

Site

In wezen is een **site** een IPv4-(sub)net. Een IPv4-(sub)net hoort bij computers, routers, printers en dergelijke. Die gebruiken de IPv4-adressen om te kunnen communiceren (bijlage B). Die apparatuur staat in een vestiging van de organisatie als een LAN opgesteld. De vestiging kan een gebouw of gebouwencomplex zijn. Een site is dus ook de representatie van een fysiek LAN van de organisatie. In tekeningen wordt een site met een rechthoek aangegeven.

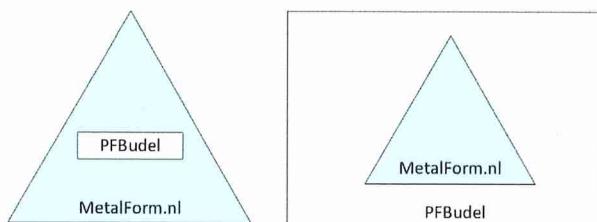
Domains en sites

Hoe domains en sites in een organisatie samenhangen, wordt bepaald door:

- Hoe een organisatie het beheer geregeld wil zien: centraal of decentraal. Dat bepaalt of er één of meer domains moeten worden gedefinieerd.
- Hoe een organisatie de beschikbare IPv4-adressen inzet. Is er sprake van een LAN of een WAN? Dat kan bepalen of er één of meer sites moeten worden gedefinieerd.

Alles is nu mogelijk.

- Organisaties die op één locatie gehuisvest zijn, gebruiken doorgaans een LAN. Zij kunnen met één domain en één site volstaan (afbeelding 2-16).



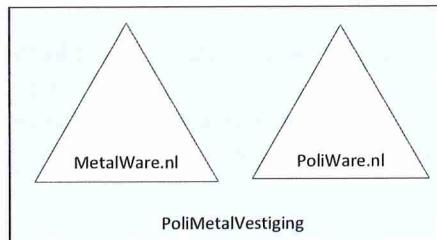
Afb. 2-16 Een organisatie met één domain en één site kan op twee manieren worden getekend

- Ook als een organisatie gevestigd is op verschillende locaties kan volstaan worden met één domain. Per vestiging kan er voor elk LAN een aparte site worden gedefinieerd (afbeelding 2-17). Daarvoor is wel noodzakelijk dat er WAN-verbindingen bestaan tussen de LAN's. Die WAN-verbindingen kunnen tegenwoordig overigens zo snel zijn dat het geheel weer kan functioneren als één LAN.



Afb. 2-17 Een organisatie met één domain en twee sites

- Meer dan één domain is eigenlijk alleen maar nodig als er sprake is van absoluut gescheiden en zelfstandig eigen beheer. **Autonomo** beheer wordt dat genoemd. Twee domains op één site kan zoals in afbeelding 2-18. Dat kan ook op verschillende sites. Het laatste is dan vergelijkbaar met 2 x afbeelding 2-16.



Afb. 2-18 Een organisatie met één site en twee domains

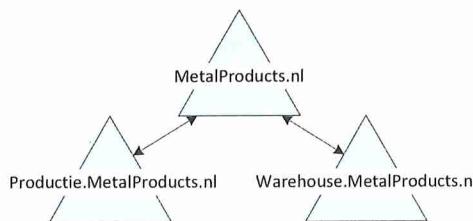
Forest

Daar waar een domain de kleinste beheerseenheid is, is een forest de **grootste**. Het belangrijkste is echter dat een forest de beveiliging van de gehele organisatie afbakt. Een forest kan bestaan uit één domain of uit verschillende domains. De belangrijkste eigenschap van een forest is, dat verschillende domains elkaar **vertrouwen**. Tussen de domains bestaat er een **trust relationship** (vertrouwensrelatie). Die trust relationship wordt in de tekeningen weergegeven met een dubbele pijl. Door die vertrouwensrelatie kunnen alle organisatieonderdelen met elkaar samenwerken. Domains die niet tot het forest behoren, worden niet vertrouwd.

Het eerste domain dat u in een nieuw forest aanmaakt, wordt het **root domain** van dat forest genoemd.

Tree

Een tree is een structuur van domains in een forest.

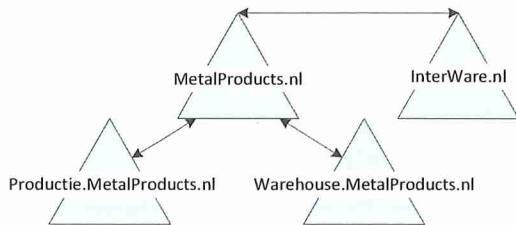


Afb. 2-19 Een tree met drie domains

In afbeelding 2-19 ziet u een voorbeeld van een tree. Het domain *MetalProducts.nl* is het **root domain** van de tree. Dat domain heeft twee **child domains**: *Productie.MetalProducts.nl* en *Warehouse.MetalProducts.nl*. Elk child domain heeft een **parent domain**. Voor de child domains *Productie.MetalProducts.nl* en *Warehouse.MetalProducts.nl* is dat *MetalProducts.nl*. Het root domain is geen child domain en heeft dus ook geen parent domain.

In een tree vormen de namen van de domains een **contiguous namespace**, een aaneengesloten naamruimte. Behalve het root domain heeft elk domain een eigen naamdeel gevuld door de naam van het parent domain. Ga dat na in afbeelding 2-19.

Als een forest maar één domain bevat, is dat het root domain van het forest. Het is tevens het root domain van de enige tree in dat forest. Bevat een forest verschillende trees dan vertrouwen de root domains van de trees elkaar (afbeelding 2-20).

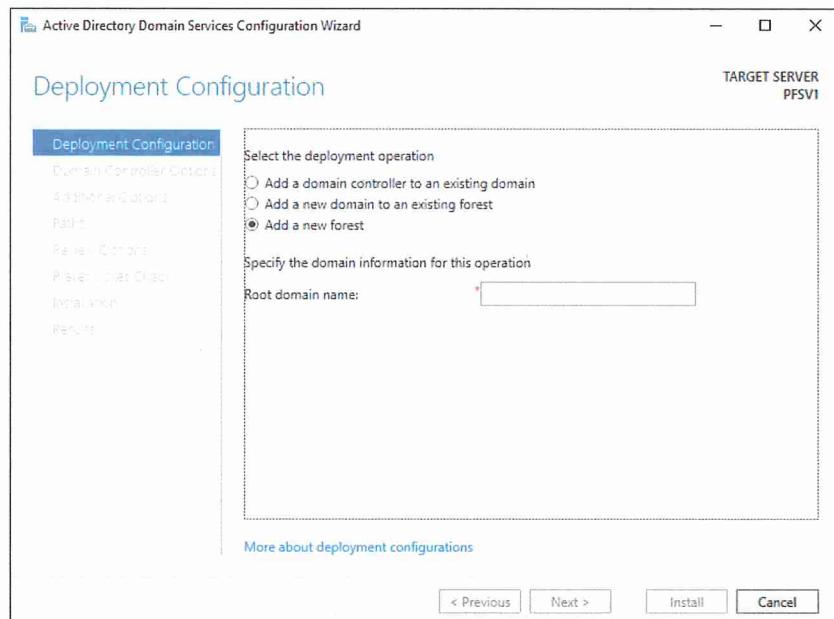


Afb. 2-20 Een forest met twee trees

In dit boek wordt een nieuw netwerk voor de organisatie PoliForma BV opgebouwd. Er is dus nog geen forest, dus ook geen tree en geen domain. De keuze die u in het wizardvenster van afbeelding 2-15 moet maken, is nu duidelijk.

- 13 Selecteer in het wizardvenster *Deployment Configuration* de optie *Add a new forest*.

Daardoor verandert het wizardvenster *Deployment Configuration* (afbeelding 2-21). U moet de *Root domain name* invullen. Daarvoor gebruikt u een FQDN (Fully Qualified Domain Name).



Afb. 2-21 De domain name is nodig

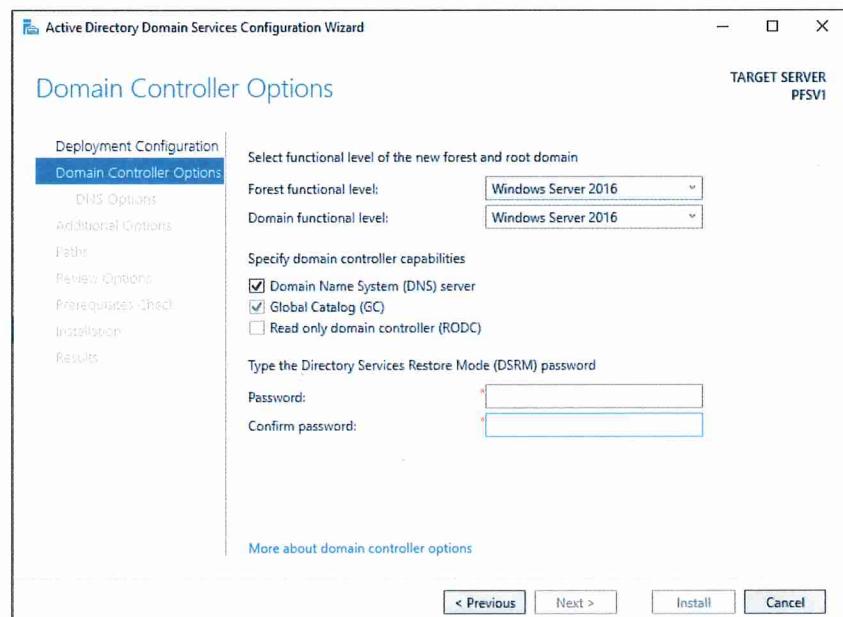
FQDN

Voorlopig is het voldoende als u weet dat hier met de FQDN de DNS-naam van het domain bedoeld wordt. Later wordt er verder op ingegaan. In dit boek wordt als domain name *PoliForma.local* gebruikt.

- 14 Vul het tekstvak *Root domain name* met: *PoliForma.local*

Klik op de knop *Next >*.

Nadat gecontroleerd is of de naam al bestaat, verschijnt het wizardvenster *Domain Controller Options* (afbeelding 2-22).



Afb. 2-22 Van alles in te stellen

Forest Functional Level en Domain Functional Level

Tekens als er een nieuwe versie van het Windows serverbesturingssysteem verschijnt, heeft dat gevlogen. Dat komt omdat nieuw ook geavanceerde betekent, geavanceerde wat werking en mogelijkheden betreft. Met het *Forest* en het *Domain Functional Level* geeft u aan welke Windows serverbesturingssystemen u in uw netwerk wilt kunnen gebruiken.

- Het **Forest Functional Level** legt u vast bij de installatie van AD in het root domain van het forest. Dat is wat u nu aan het doen bent. U stelt dit in op de **oudste** versie waarvan er nog een server in het forest moet kunnen draaien.
- Een afgeleide van het *Forest Functional Level* is het **Domain Functional Level**. Het *Domain Functional Level* kunt u alleen maar gelijk laten aan of op een **jongere** versie instellen dan het *Forest Functional Level*.

In dit boek wordt het *Forest Functional Level* ingesteld op de jongste beschikbare versie. Daarmee wordt ook het *Domain Functional Level* ingesteld op diezelfde versie. Oudere versies worden in deze cursus niet gebruikt.

- 15 Selecteer zo nodig met de uitschuiflijst *Forest Functional Level* de optie met de jongste versie van Windows Server uit de lijst.

Omdat u het *Forest Functional Level* heeft ingesteld op de jongste versie, kunt u het *Domain Functional Level* niet instellen op een oudere versie.
- 16 Controleer het *Domain Functional Level*. Dat moet automatisch ook op dezelfde versie ingesteld staan.

Dan de lijst *Specify domain controller capabilities*:

- De optie *Domain Name System (DNS) server* is voorzien van een vink. Bij eerdere controle is er op standalone server PFSV1 geen DNS-omgeving aangetroffen. Omdat AD niet zonder DNS kan, wordt hier voorgesteld gelijk ook DNS te installeren.
- Voor de optie *Global Catalog (GC)* staat een grijze vink. Die kunt u dus niet wegklikken.

Global Catalog

In uitgebreide domain-structuren kan de af te leggen weg van het ene domain naar het andere lang zijn. Als domains diep in verschillende trees van een forest liggen, is dat bijvoorbeeld het geval. Dan kost het veel tijd en netwerkcapaciteit om informatie uit het andere domain op te halen. Daarom gebruikt AD de **Global Catalog**. De Global Catalog wordt in elk geval geïnstalleerd op de eerste DC van een domain. Daarmee is die DC een **GCS** (Global Catalog Server). Andere DC's kunnen naar behoefte opgewaardeerd worden tot GCS.

De Global Catalog is een database waarin:

- van alle netwerkobjecten uit het eigen domain alle eigenschappen worden bijgehouden;
- van de netwerkobjecten uit de overige domains van het forest een deel van de eigenschappen wordt bijgehouden.

De Global Catalog wordt op alle GCS'en gelijk gehouden door het **replicatieproces**. Daarover later meer.

- De optie *Read only domain controller (RODC)* is helemaal grijs en dus niet te gebruiken.

RODC

Een RODC is een DC die een read-only kopie bevat van een andere DC. Juist omdat u de eerste DC inricht, bestaat er dus nog geen andere. RODC's worden met name ingezet op plaatsen waar geen deskundig beheer mogelijk is.

Tenslotte het wachtwoord voor de DSRM (Directory Services Restore Mode).

DSRM

Via de DSRM bent u in staat een backup van AD terug te plaatsen. Daarmee kunt u een beschadigde AD vervangen door een oudere werkende versie. Natuurlijk moet u die backup wel vooraf gemaakt hebben. Als u een dergelijke backup terug wilt zetten, moet u daarvoor beschikken over een apart password. Dat password moet u hier invoeren.

In dit boek wordt het password voor de *Administrator* ook voor de DSRM gebruikt.

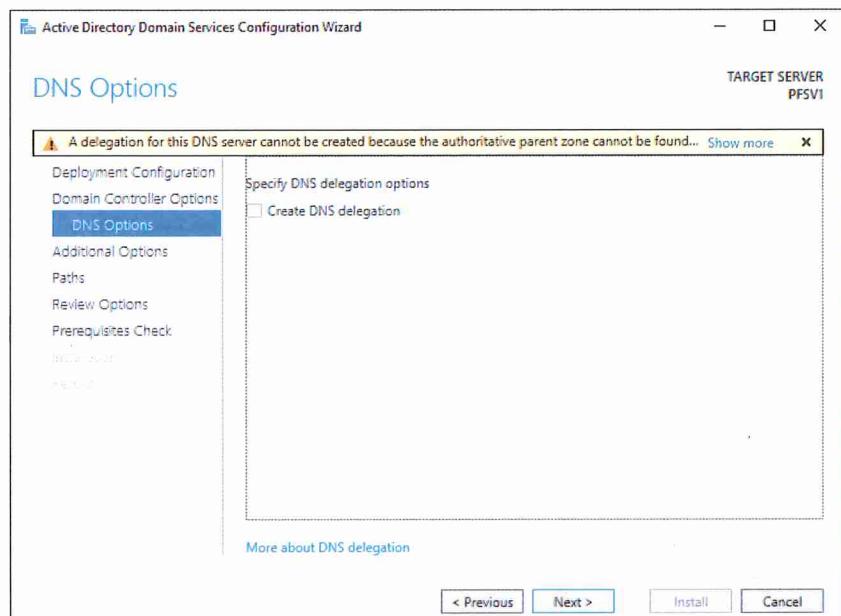
- 17 Laat de instellingen staan zoals in afbeelding 2-22.

Typ in het tekstvak *Password* uw secure administrator password.

Herhaal dat voor de controle in het tekstvak *Confirm password*.

Klik op de knop *Next >*.

Vervolgens wordt er geconstateerd dat het domain *PoliForma.local* niet bereikbaar is. Daarom verschijnt het wizardvenster *DNS Options* van afbeelding 2-23 met daarin een foutmelding.



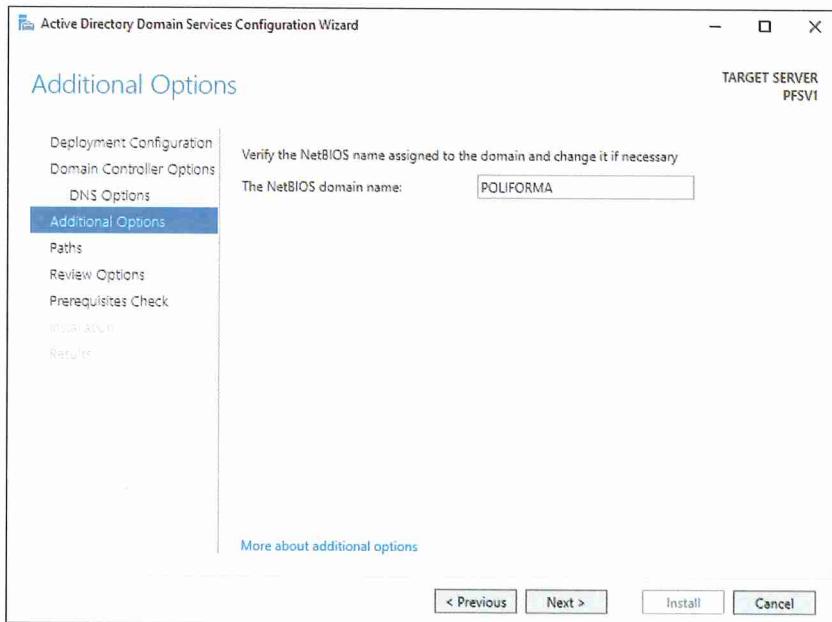
Afb. 2-23 Geen *PoliForma.local* gevonden

U negeert deze foutmelding. U gebruikt straks uw eigen DNS-omgeving.

18 Klik op het sluitknopje van de foutmelding.

Klik op de knop *Next >*.

De wizard vervolgt met het wizardvenster *Additional Options* van afbeelding 2-24.



Afb. 2-24 De voorgestelde NetBIOS-naam

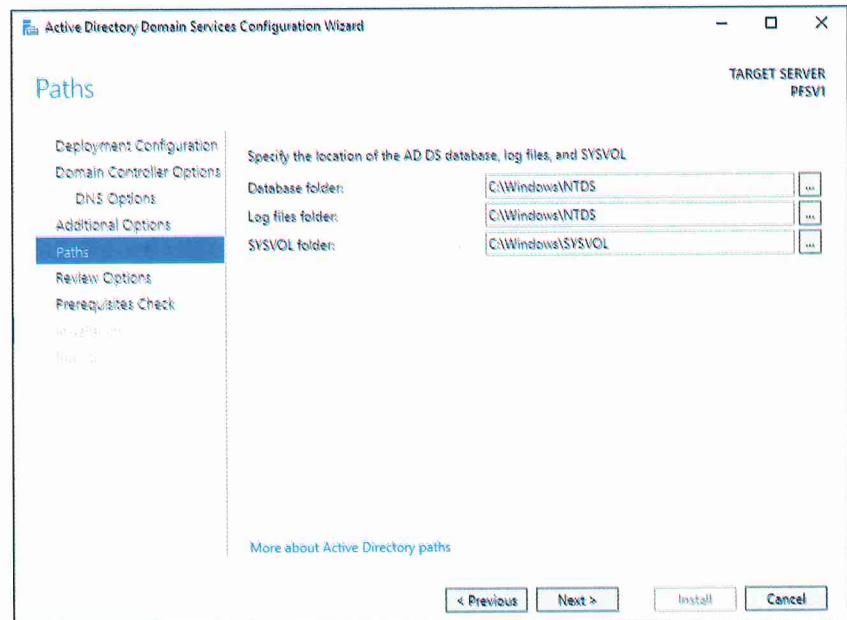
NetBIOS

NetBIOS (Network Basic Input Output System) werd als naamidentificatie gebruikt in de oude netwerkbesturingssystemen van Microsoft. Pas in Windows 2000 is overgestapt op DNS. Hoewel de NetBIOS-naamgeving nergens meer gebruikt wordt, wordt de ondersteuning van NetBIOS in Windows Server 2022 nog steeds gehandhaafd.

19 Accepteer de voorgestelde NetBIOS-naam *POLIFORMA*.

Klik op de knop *Next >*.

De wizard vervolgt met het wizardvenster *Paths* van afbeelding 2-25.



Afb. 2-25 De plaats van de bestanden

Bestandslocaties

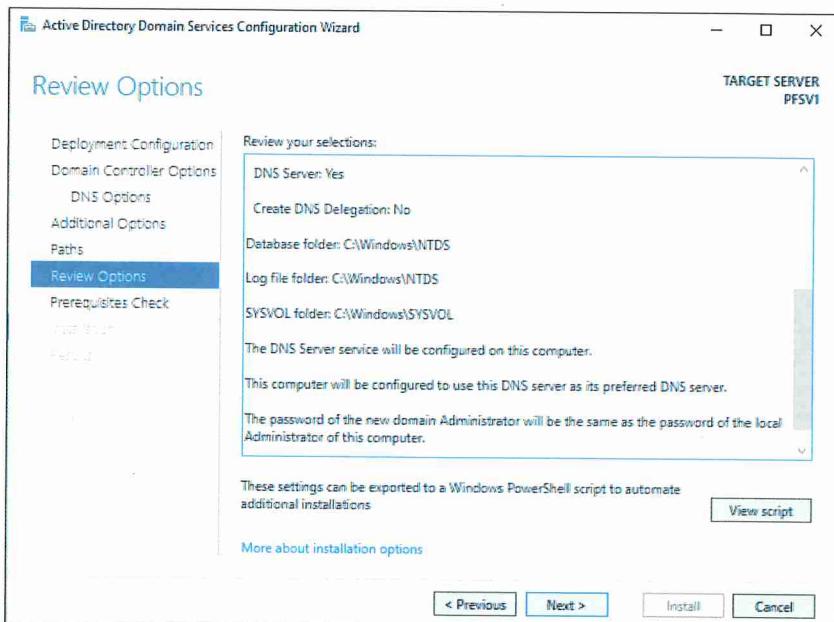
- *Database folder* is de map waar AD zelf wordt opgeslagen.
- *Log files folder* is de map waar de logs in worden opgeslagen. In logs worden gebeurtenissen geregistreerd. Pas in deel 2 *Beheer en beveiliging* wordt hierop ingegaan.
- *SYSVOL folder* is de map waar bestanden in worden opgeslagen die voor elke netwerkgebruiker toegankelijk zijn.

In dit boek worden de voorgestelde mappen gebruikt.

20 Laat de voorgestelde mappen ongemoeid.

Klik op de knop *Next >*.

Vervolgens verschijnt het wizardvenster *Review Options* van afbeelding 2-26.



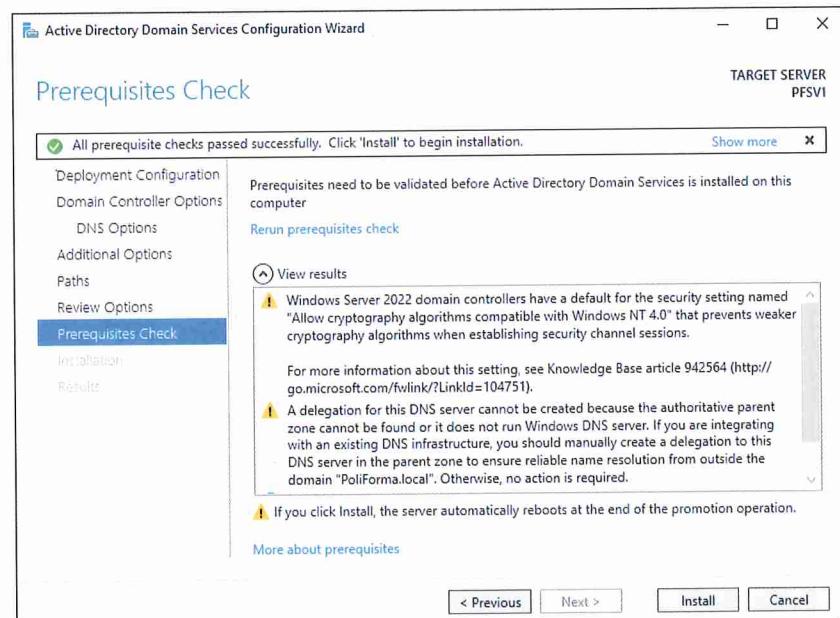
Afb. 2-26 De samenvatting

In de lijst in afbeelding 2-26 valt te lezen:

- Dat met de installatie van AD ook DNS zal worden geïnstalleerd. Zie ook afbeelding 2-22.
- Vervolgens dat in de IPv4-instellingen de machine zelf zal worden aangeduid als *Preferred DNS server*.
- Dat het nieuwe account van de domain *Administrator* hetzelfde password krijgt als de machine local *Administrator*.

21 Klik op de knop *Next >*.

Wacht tot het systeem klaar is met de *Prerequisites Check*. Er wordt gecontroleerd of uw instellingen in hun gehele samenstelling voldoen aan de voorwaarden (afbeelding 2-27).



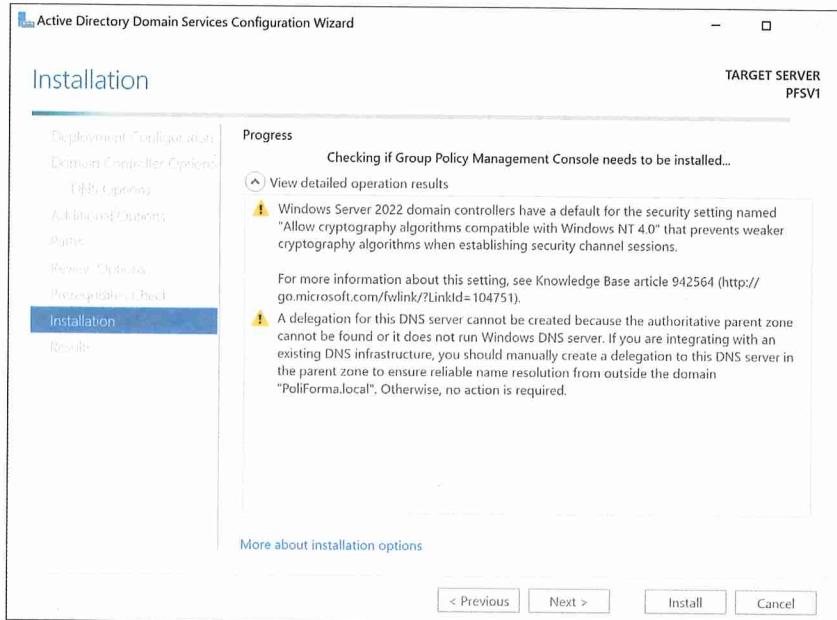
Afb. 2-27 Het resultaat na controle op de voorwaarden: twee waarschuwingen

Als de controle op de voorwaarden goed is verlopen zoals bovenin afbeelding 2-27 te zien is, kan er geïnstalleerd worden. Merk op dat na de configuratie van de AD DS de server automatisch herstart wordt.

! If you click Install, the server automatically reboots at the end of the promotion operation.

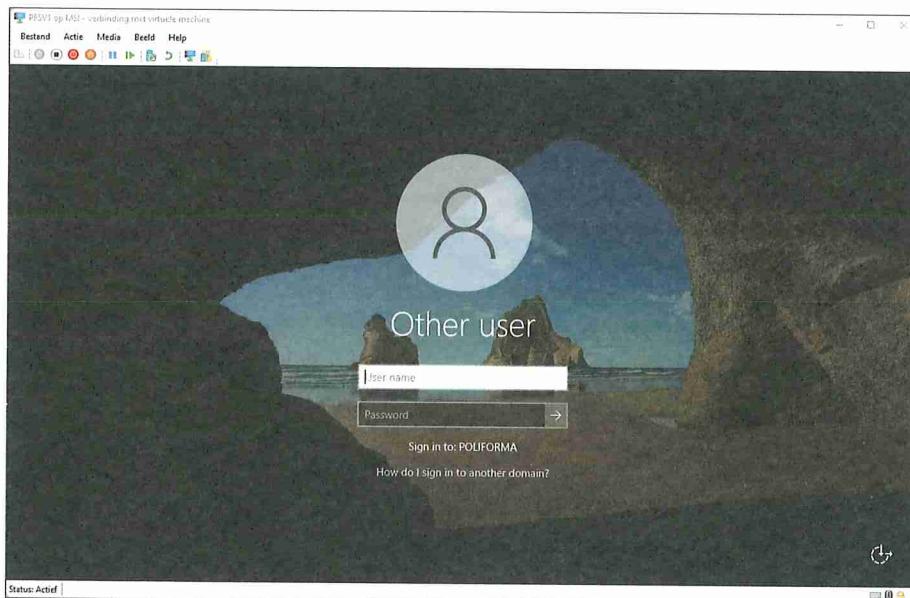
22 Klik op de knop *Install*.

De installatie van AD gaat vervolgens van start. Het verloop kunt u volgen (afbeelding 2-28).



Afb. 2-28 Het installeren van AD

Na afloop verschijnt er automatisch nog een waarschuwing en wordt server *PFSV1* automatisch herstart. Wacht tot het venster van afbeelding 2-29 voor u staat.



Afb. 2-29 Het herstarten gebeurt vanzelf

Het inlogschermscherm

De installatie van AD is nu voltooid. De eerste verandering is het inlogschermscherm (afbeelding 2-29). Vergelijk het inlogschermscherm met dat van afbeelding 1-20. Daar logde u in als **machine local Administrator** op een standalone server. Met het inlogschermscherm dat nu voor u staat, gaat u inloggen op het domain *POLIFORMA*. Dat is de NetBIOS-naam van het domain *PoliForma.local* (afbeelding 2-24). U gaat dus inloggen als de *Administrator* van het **domain**. Uit afbeelding 2-26 weet u dat het password van de domain *Administrator* is overgenomen uit het machine local user account *Administrator*. Daarom kunt u dus hetzelfde password gebruiken.

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

Log verder in met uw administrator password.

Sluit de virtuele server *PFSV1* op de normale manier af.

De *AD DS* is geconfigureerd in uw testnetwerk. AD is geïnstalleerd. Standalone server *PFSV1* is DC geworden in het domain *PoliForma.local*. Dat is het root domain van het nieuwe forest en tevens het root domain van de enige tree in dat forest.

2.2 De eerste Domain Controller in het domain

Uw virtuele server *PFSV1* is nu dus de eerste DC van uw client/server-testnetwerk bij de firma PoliForma BV. In deze paragraaf bestudeert u enkele belangrijke gevolgen van de installatie van AD op server *PFSV1*. DC's zijn echt anders dan stand-alone servers.

Practicum 2.2.1: Domain Controller

60 min.

In dit practicum:

- Leert u de gevolgen van de installatie van AD op server *PFSV1*.
- Leert u enkele beschikbare beheertools voor AD kennen.
- Past u enkele instellingen aan met behulp van die beheertools.

Voor dit practicum heeft u nodig:

- Uw virtuele DC *PFSV1* zoals geïnstalleerd in de vorige paragraaf.
- Het werkblad bij practicum 2.2.1 waarop u uw werkzaamheden vastlegt.
- Tijd: ± 60 minuten.

Korte practicum instructies

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

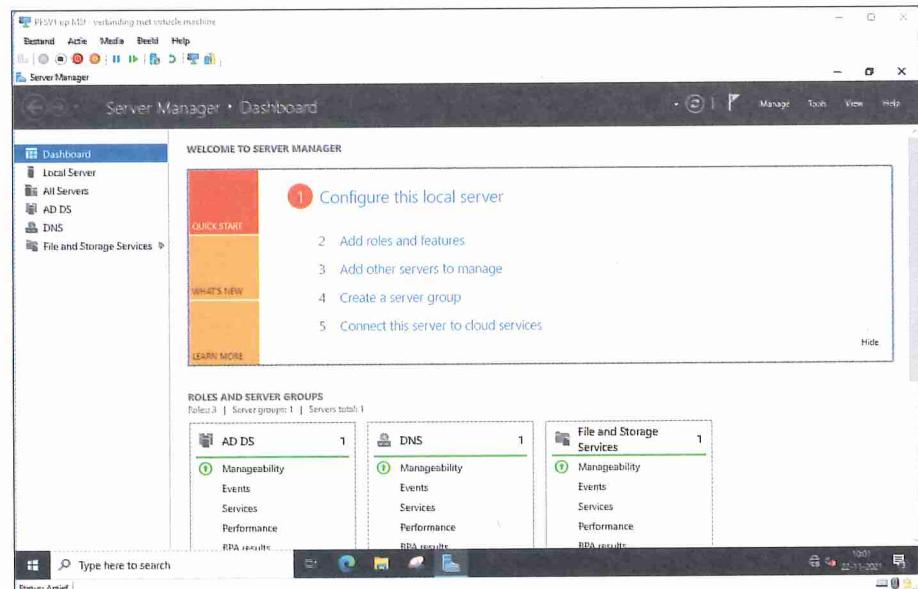
- a Welke server roles zijn er geïnstalleerd op DC *PFSV1*?
- b Controleer het overzichtsvenster van de server role *AD DS*.
- c Gebruik de MMC *Active Directory Users and Computers* voor het onderstaande:
 - Wat is de inhoud van de container *Computers*?
 - Wat is de inhoud van de OU *Domain Controllers*?
 - Bekijk, zoals u in hoofdstuk 1 ook heeft gedaan, de gebruikers en groepen met behulp van de MMC *Computer Management*. Wat constateert u?
 - Welke gebruikers en groepen komen in AD voor?
 - Controleer de eigenschappenvensters van de domain users *Administrator* en *Guest*.
 - Stel zo nodig voor de domain *Administrator* de eigenschap *Password never expires* in.
 - Vul de eigenschap *Description* van DC *PFSV1* met: *DC in het domain PoliForma.local*
 - Controleer of DC *PFSV1* een GCS is.
 - Vul het tekstvak *Description* van de *NTDS Settings* met: *AD van het domain PoliForma.local*
 - Welk besturingssysteem is er op DC *PFSV1* geïnstalleerd?
 - Van welke groep(en) is DC *PFSV1* lid?
- d Gebruik de MMC *Active Directory Sites and Services* voor het onderstaande:
 - Wijzig de sitenaam in: *PFBudel*
 - Vul voor de site *PFBudel* het tekstvak *Description* met: *Vestiging van PoliForma BV*
 - Vul voor de site *PFBudel* het tekstvak *Location* met: *Budel*
 - Koppel het IPv4-netwerk *192.168.101.0/24* aan de site *PFBudel*.
- e In welke map is AD op server *PFSV1* opgeslagen?
- f Bestudeer het overzichtsvenster van de server role *DNS Server*.
- g Welk IPv4-adres staat er ingevuld bij de *Preferred DNS server* van de NIC *LAN-Connectie*? Wat betekent dat?
- h Controleer of voor de NIC *InternetConnectie* het IPv4-adres van de DNS-server dat u van uw docent heeft gekregen nog steeds staat ingevuld. Herstel dat als dat niet zo is.

Gedetailleerde uitwerking van het practicum

- 1 Maak verbinding met uw virtuele server *PFSV1* en start deze.
 - 2 Vul het tekstvak *User name* van het inlogscherm met *POLIFORMA\Administrator* of *Administrator@PoliForma.local*.
- Log verder in met uw administrator password.

Server roles

In het vorige practicum heeft u de server role *AD DS* geïnstalleerd. Tijdens de installatie van AD heeft u gelijk ook DNS laten installeren (afbeelding 2-22). Dat is nu allemaal terug te vinden op het *Dashboard* van de *Server Manager* (afbeelding 2-30).



Afb. 2-30 De *AD DS* en *DNS* in de tree van de *Server Manager*

De server role Active Directory Domain Services

- 3 Klik in de tree van de *Server Manager* op de container *AD DS*.

U ziet de toestand waarin deze server role zich op dit moment bevindt (afbeelding 2-31).