Windows server

EMBRECHTS KENNY, ADAMS JENTE, EYCKERMAN REINOUT, PELLERIAUX JORIS

UNIVERSITEIT ANTWERPEN | Netwerken

Inhoudsopgave

1 Roles en features

In dit onderdeel worden alle verschillende roles en features uitgelegd die we hebben geïnstalleerd en ook waarom we ze hebben geïnstalleerd.

1.1 AD DS

Active Directory staat beheerders toe om alle rechten en instellingen in het netwerk van een volledig bedrijf te beheren (bepaalde rechten toekennen aan gebruikers, wat ze wel en niet mogen doen). Ook het automatisch installeren van software en patches behoort tot de mogelijkheden. Active Directory slaat instellingen in relatie tot een object centraal op in een database. Een AD-netwerk kan variëren van een netwerk van tientallen tot miljoenen objecten.

Een Active Directory bestaat uit:

- Forests
- Domains
- Sites
- Organisational units

1.1.1 Domain (boekingnow)

Aan de basis van AD staan domeinen. Een domein is een collectie van objecten. Deze objecten kunnen variëren van users naar computers of printers. Deze structuur wordt georganiseerd in een tree. Een groep van trees noemen we een forest.

1.1.2 Forests

Forests zijn het geheel van domeinen. Alle domeinen binnen een forest vertrouwen elkaar direct of indirect. Alle domeinen in een forest kunnen dezelfde soort objecten huisvesten (ze hebben hetzelfde schema). De namen van domeinen worden allemaal bepaald volgens het domain name system.

1.1.3 Organizational units

Een organizational unit (OU) is een manier om een bepaalde hiërarchie van digitale certificaten te maken. Via OU's is het heel makkelijk om bepaalde gebruikers in dezelfde OU te gaan zetten die dezelfde dingen moeten kunnen.

1.2 DHCP

Dynamic host configuration protocol (DHCP) is het protocol dat ervoor zorgt dat alle computers in het netwerk hun IP-instellingen dynamisch ontvangen. Op deze manier zal je nooit meer het IP-adres van een computer zelf moeten toewijzen (tenzij je een machines wilt configureren met een specifiek IP, en zelfs dan nog kan je dit via DHCP toewijzen).

1.3 DNS

Domain Name System is de service die IP-adressen vertaalt naar echte namen die voor mensen beter begrijpbaar zijn. I.p.v 'ping 192.168.0.50' kan je 'ping client1' gebruiken.

1.4 File and Storage Service

Dit is de service die ervoor zorgt, dat er in je netwerk 1 locatie komt waar je de bestanden zal opslaan. Deze files kan je dan ook delen met gebruikers op je netwerk.

1.5 Distributed File System

DFS is een onderdeel van windows server dat ervoor zorgt dat je shares kan maken die gedeeld worden met bepaalde gebruikers in het netwerk. Dit is de windows versie van een gedistribueerd bestandssysteem. Er zijn 2 onderdelen van DFS, namespace en replication.

1.5.1 Namespace

Dit is een manier om meerdere folders in 1 folder te bundelen, zelfs als de orginele folders op verschillende fysieke locaties te vinden zijn.

1.5.2 Replication

Replication is een manier om efficiënt folders (of gehele shares) te repliceren. Zelfs als deze shares over meerdere servers staan. DFS replication werkt met een algoritme dat DFS in staan stelt om in een gerepliceerde folder, in de originele folder, de aanpassingen te detecteren en enkel deze aanpassing te kopiëren

1.5.3 Shares

Bij DFS is het mogelijk om een bepaalde groep fileshares, verdeeld over meerdere servers of locaties via een logische naam als een (virtueel) geheel te zien. Voor de eindgebruiker lijkt de DFS-share een gewone lokale fileshare te zijn, maar de data kan in de praktijk verspreid zijn over diverse servers en locaties en vaak wordt er ook gebruikgemaakt van replicatie: de data is aanwezig op meerdere locaties en de gebruiker krijgt (automatisch) toegang tot de best toegankelijke dataset (bijvoorbeeld de data op zijn eigen locatie of krijgt verbinding met de site waarmee de beste verbindingen bestaan).

1.5.4 Roaming profiles

Roaming profiles zorgt ervoor, dat als een gebruiker inlogt op een computer, alle bestanden die worden gemaakt, gerepliceerd worden naar de server. Als de gebruiker nadien inlogt op een andere computer, zijn alle bestanden beschikbaar via de server. De documenten worden opgeslagen aan de server en de computer krijgt een link naar de locatie van de bestanden, zodat er toch nog mee gewerkt kan worden.

1.6 Remote Acces (Service)

Remote Acces wordt gebruikt voor de VPN verbinding naar de server. Dit staat gebruikers toe om door middel van deze VPN toch nog op het netwerk van het bedrijf te werken vanop een andere locatie.

1.6.1 Network Access Protection

Network access protection is een service die controleert of een computer ‘veilig’ genoeg is om op het netwerk toegelaten te worden.

1.7 Remote Desktop Service

Dit geeft users de mogelijkheid om toegang te krijgen tot sessies van virtuele machines, of tot applicaties die niet op hun eigen machines staan.

In ons geval wordt deze service gebruikt zodat de gebruikers toegang hebben tot het boekhoudprogramma.

1.8 Internet Information Services

IIS wordt gebruikt door windows om internetdiensten aan te kunnen bieden. De machine die deze service biedt kan worden aanzien als de webserver. IIS is zeer veelzijdig. Het is niet enkel een mogelijkheid om een website op te zetten, maar ook PHP en Perl en nog vele anderen dingen worden door IIS ondersteund.

1.9 WSUS

Windows Server Update Service is de service die ervoor zorgt dat een administrator alle laatste updates van Microsoft op een Windows besturingssysteem kan verspreiden. Via WSUS kan de systeemadmin bepalen welke updates wel of niet moeten geïnstalleerd worden op de computers in het netwerk.

1.10 WDS

Windows Deployment Service is een service die ervoor zorgt dat je bij het aansluiten van een nieuwe computer makkelijk een windows OS installatie kunt doen. Via WDS kan je heel makkelijk een Operating System deployen via het netwerk.

1.11 Printer server

Een printerserver verwijst naar een netwerk waar een gekoppelde printer kan bereikt worden door middel van het IP-adres. Het grootste voordeel is dat er geen 5 printers moeten aangekocht per lokaal maar dat alle computers in het netwerk kunnen afdrukken op 1 en dezelfde printer.

2 Onze instellingen

2.1 AD DS

2.1.1 Domain

Het domain van ons netwerk is boekingnow. Dit is het boekhoudkantoor waarvoor we deze server hebben geconfigureerd.

2.1.2 Forests

Aangezien er maar 1 domain is voor dit project, is er geen overkoepelende forest. Je hebt enkel een *forest* nodig om meerdere *trees* te omvatten qua configuratie. Ook *trees* hebben we dus niet

2.1.3 Organizational units

Deze worden later nog uitgelegd.

2.2 DHCP

Voor de DHCP settings is alles ingesteld op IPv4.

2.2.1 Address pool

Voor deze DHCP server wordt maar 1 address pool gebruikt. Deze gaat van 192.168.1.1 tot 192.168.1.254.

Voor de vaste servers zijn er momenteel IP-adressen *geexclude* uit deze pool. Van 192.168.1.1 tot 192.168.1.10 worden niet uitgedeeld aan gewone computers of hardwareapparaten.

Ook voor RAS (Remote Access Service/VPN) worden er addressen *geexclude*. Van 192.168.1.11 tot 192.168.1.20 worden niet uitgedeeld aan gewone computers of hardwareapparaten.

2.2.2 Leases

De DHCP leases duren momenteel 8 dagen. Dit is de standaard lease die DHCP instelt en hier hebben wij niets aan veranderd.

2.3 DNS

We hebben in onze DNS configuratie enkel een forward lookup zone. Voor een kleiner bedrijf was het niet nodig om een reverse lookup zone te maken.

2.3.1 Forward lookup zone

In onze forward lookup zone staan alle ip adressen die worden uitgedeeld in ons netwerk. Zowel de statische up adressen, de ip addressen van RAS en de ip adressen uitgedeeld door onze DHCP server.

De msdcs forward lookup zone is voor LDAP services. Deze gebruiken we zelf niet en hebben we ook niet geconfigureerd. Deze is er standaard bij gekomen bij de installatie van DNS.

2.4 File and Storage Service

2.5 Distributed File System

DFS is een systeem om file te delen via het netwerk(te vinden via tools). Wij hebben enkel namespace gebruikt.

2.5.1 Namespace

Er zijn 2 verschillende soorten namespace in DFS. Je hebt domain based namespace en stand alone namespace. Het grootste verschil is het verschil in de locatie waar de DFS configuratie wordt opgeslagen. Standalone names spaces doen dit in de host server zijn registry, terwijl domain based namespaces dit in de AD database doen. Ook kan een domain based namespace meerdere root targets hebben. Dit wil zeggen dat de namespace op meerdere servers zijn data kan gaan zoeken. Aangezien we rekening moesten houden met het misschien splitsen van de servers, hebben we ook voor een domain based namespace gekozen.

2.5.1.1Domain based namespace

Voor de instellingen van namespace, nemen we voor elke OU een aparte share. Bij het instellen van deze namespace, moeten we *'control'* geven aan een group die behoort tot de OU (full control, read, change).

Voor elke afzonderlijke OU is er een namespace gemaakt. Hierin worden hun *gemeenschappelijke* files in opgeslagen. Deze zijn ook beschikbaar via een VPN access.

2.5.1.2Stand-alone namespace

Dit hebben we niet gekozen omdat we met de mogelijkheid zitten van het splitsen van onze servers. Aangezien we zo goed als zeker dat zullen opslagen op beide servers, kunnen we met deze namespace geen share maken met files op de 2 of meerdere servers, omdat deze namespace geen meerdere root targets kan selecteren.

2.5.2 Shares

Een share is de benaming voor alle folders die *geshared* worden tussen specifieke personen. Dit is eigenlijk hetzelfde als DFS, maar onder een andere naam. We hebben een share voor secretariaat, boekhouders, zaakvoerders en het boekhoudprogramma.

2.5.3 Roaming profiles

Per user wordt er automatisch een roaming profile aangemaakt. Dit wordt gebruikt om alle settings, alle documents en zelfs achtergronden te 'importeren' telkens je je aanmeldt. Dit zorgt ervoor dat je elke keer als je je aanmeldt, zelfs op andere computers, het uitzicht en de instellingen elke keer exact hetzelfde zijn.

2.5.4 Shares vs DFS

Het grootste verschil tussen deze 2 is de moeilijkheidsgraad in gebruik. Voor shares heb je de fysieke locatie nodig. Het is dus moeilijk om voor grote bedrijven, tussen 2 fysieke locaties een share te maken, terwijl dit bij DFS makkelijker is.

2.6 Remote Access

Remote access hebben we gebruikt om VPN toegang te verkrijgen tot ons netwerk. De IP adressering, zoals hierboven uitgelegd, gebeurt van de adressen 192.168.1.11 tot 192.168.1.20. Remote access maakt gebruikt van pptp (point to point tunneling protocol).

2.6.1 Authenticatie

Dit gebeurt via het EAP MSChap V2 protocol. Hierdoor kunnen we inloggen d.m.v. de gebruikersnaam die beschikbaar is via het domein.

2.6.2 Network Access Protection

Via NAP moet je Health Policies instellen. Deze health policies zorgen ervoor dat onze gebruikers wel of niet toegang tot het netwerk. NAP is helaas niet compatibel met W10 computers (we konden het in elk geval niet instellen voor W10).

2.7 Remote Desktop Service

Deze service wordt gebruikt door onze gebruikers om toegang te krijgen tot het boekhoudprogramma. Er worden via deze certificaten uitgedeeld aan computers. Computers zonder certificaten kunnen dus geen toegang krijgen tot deze service. Omdat deze service via https werkt, kan je zonder certificaat geen toegang krijgen.

2.8 Internet Information Services

Dit wordt enkel en alleen gebruikt voor onze remote desktop service.

2.9 WSUS

De Windows Server Update Service wordt gebruikt om alle updates van windows op de computers te installeren. De instellingen worden per dag gecontroleerd. Dit is zodat de verplichte beveiligingsupdates toch zeker up to date blijven.

2.10 WDS

Windows Deployment Service wordt gebruikt om, als er nieuwe computers zijn, dat je makkelijk een OS op deze nieuwe computer kunt installeren. Dit is overigens het enige waarvoor we dit gebruiken.

Dit doe je door in de WDS service een boot image te selecteren (boot.wim) en dan ook een install image (install.wim). De makkelijkste manier is om in de virtuele machine je disc te mounten (in de virtuele CD lezer steken) en dan deze files selecteren via de 'wizard'.

2.11 Printer server

Dit spreekt voor zich. Zo heeft iedereen toegang tot de printers op het netwerk.

3 Organizational Units

Hieronder worden de organizational units uitgelegd. Waarom we ze hebben gemaakt en wie hierin zit.

3.1 Personeel

Dit is de overkoepelende OU voor alle werknemers van ons boekhoudkantoor, met een groep die is gelinkt aan het group policy object.

3.1.1 Zaakvoerders

Dit is de overkoepelende OU voor alle zaakvoerders van ons boekhoudkantoor, met een groep die is gelinkt aan het group policy object.

3.1.1.1 Gebruikers

Hierin zitten alle gebruikers die behoren aan de OU zaakvoerders.

3.1.1.2 Computers

Hierin zitten alle computers die behoren aan de gebruikers van de OU zaakvoerders.

3.1.2 Boekhouders

Dit is de overkoepelende OU voor alle boekhouders van ons boekhoudkantoor, met een groep die is gelinkt aan het group policy object.

3.1.2.1 Gebruikers

Hierin zitten alle gebruikers van de OU boekhouders.

3.1.2.2 Computers

Hierin zitten alle computers die behoren aan de gebruikers van de OU boekhouders.

3.1.3 Secretariaat

Dit is de overkoepelende OU voor alle secretariaatmedewerkers van ons boekhoudkantoor, met een groep die is gelinkt aan het group policy object.

3.1.3.1 Gebruikers

Hierin zitten alle gebruikers van de OU zaakvoerders.

3.1.3.2 Computers

Hierin zitten alle computers die behoren aan de gebruikers van het OU secretariaat.

4 Group policies

De group policies zijn alle restricties die we kunnen toedienen aan bepaalde OU's. Hieronder kan je lezen welke group policies we hebben gemaakt en waarom.

4.1 Personeel

4.1.1 User

4.1.2 Computer

In het register UseProfilePathsExtensionVersion toegevoegd om verschillende versies van de gebruikers hun homefolder te kunnen gebruiken (werkt beter met os upgrades)

Set roaming profilepathh for all users: voor roaming profielen

Configure automatic updates: spreekt voor zich

Turn on script execution: disabled zodat powershell scripts niet uitgevoerd worden

Drive map ingesteld om de DFS share personeel te automounten

Specify default connection url: zodat de gebruikers deze url zelf niet moeten ingeven als ze remote apps willen gebruiken.

4.1.3 Zaakvoerders

4.1.4 Boekhouders

4.1.5 Receptie

4.1.6 BoekhoudUsers

4.1.6.1 User

4.1.7 IedereenBuitenZaakvoerders

4.1.7.1 Computer

Deny log on locally voor secretariaat en boekhouders omdat deze niet mogen inloggen op de computer van de zaakvoerder