

Portfolio Windows Server II: Victor Dewitte

Inleiding

In de opstelling wordt er gebruik gemaakt van 4 virtuele machine's dit elk met een versie van windows server 2019. De DC server is de enige server met een grafische interface. De andere server's hebben geen grafische interface. De DC server is de enige server die gebruikt wordt voor het beheer van de andere server's.

IP-Adressen	
DC	192.168.22.1
IIS	192.168.22.2
SQL	192.168.22.3
Exchange	192.168.22.4
Client	DHCP

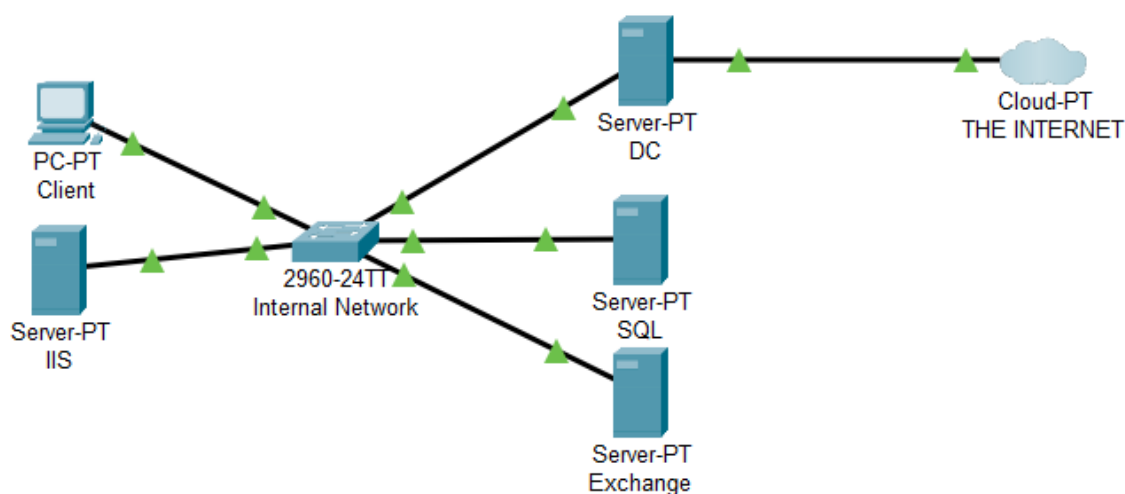


Fig.1 - Grafische weergave van de opstelling van de servers

DomeinController-Server

Op de domeincontroller server met een gui zullen volgende services draaien:

- AD DS
- DNS
- DHCP
- CA
- Router role met NAT

De server zal beschikken over 2 cores met 4gb ram en de windows server 2019 64 bit operating systeem zal er op geïnstalleerd zijn met de desktop experience (dus met een grafische interface). De server zal ook

beschikken over een 35gb virtuele harde schijf bevatten. Deze is dynamisch gealloceerd zodat hij enkel de nodige ruimte inneemt op je host machine. De complete domeinnaam van deze server zal **dc.ws2-2223-victor.hogent** zijn. De server heeft ook 2 network interface's:

- 1 voor het interne netwerk, die een statisch ip adres heeft in de range van het interne netwerk : 192.168.22.1
- 1 voor de NAT verbinding die heel de omgeving zal voorzien van een verbinding met het internet. Deze interface heeft een dynamisch ip adres die hij krijgt van de DHCP server van Virtualbox.

De Active Directory Domain Services (AD DS) zal geïnstalleerd zijn op de DomeinController. Deze zal de domeinnaam "**WS2-2223-Victor.hogent**" hebben. Na de installatie zal in de post deployment volgende stappen uitgevoerd worden: - We checken de de config van de server met ADprep /forestprep en ADprep /domainprep zodat de server klaar is om een domein te hosten. - Na dit wordt het forest en domain functioneel level ingesteld op windows server 2016. Ook worden de capabilities van de AD DS geselecteerd. Deze zijn GC (Global Catalog) en DNS (Domain Name System). Ook wordt er een DSRM (Directory Services Restore Mode) password ingesteld. Er kan een DNS Delegation gemaakt worden op de DNS server, dit wordt in dit geval niet gedaan.

De NetBIOS naam wordt ingesteld op **WS2-2223-VICTOR**. NetBIOS-naam is een naam van 16 bytes voor een netwerkservice of -functie op een computer met Microsoft Windows Server. NetBIOS-namen zijn een gebruiksvriendelijkere manier om computers in een netwerk te identificeren dan netwerknnummers en worden gebruikt door NetBIOS-compatibele services en toepassingen.

Er is ook een directory pad nodig voor de AD DS database, log files en de SYSVOL. Die wordt op de standaard paden van **C:\Windows\NTDS** en **C:\Windows\SYSVOL** ingesteld. De database folder heeft een paar belangrijke bestanden. De database gebruikt de ESE(Extensible Storage Engine), dit is een database engine die gebruikt wordt door de AD DS database.

De SYSVOL is een gedeelde map waarin de serverkopie van de openbare bestanden van het domein wordt opgeslagen die moeten worden gedeeld voor algemene toegang en replicatie in een domein.









 SystemResources	15/09/2018 9:19	File
 SYSVOL	23/10/2022 14:22	File
 SysWOW64	23/10/2022 15:13	File
 TAPI	15/09/2018 9:19	File
 Tasks	23/10/2022 14:05	File
 Temp	29/10/2022 14:55	File
 TextInput	15/09/2018 9:19	File
 tracing	15/09/2018 9:19	File

Fig.2 - C:\Windows\ folder met de SYSVOL folder in

Er is binnen de Active Directory 2 admin accounts voorzien met volle rechten voor alles te doen binnen het AD. Ze kunnen alles op elke pc/server binnen het domein aanpassen. Er is het standaard Administrator account en een account voor mezelf.

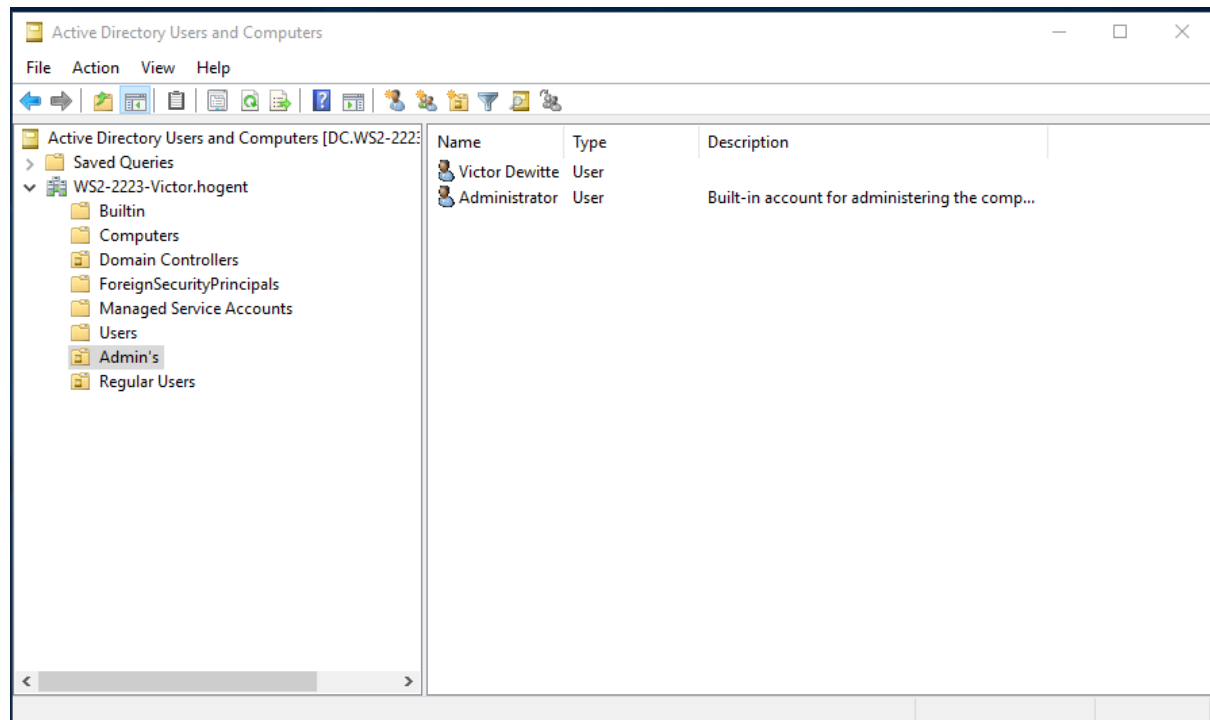


Fig.3 - Admin Accounts voorzien in de AD

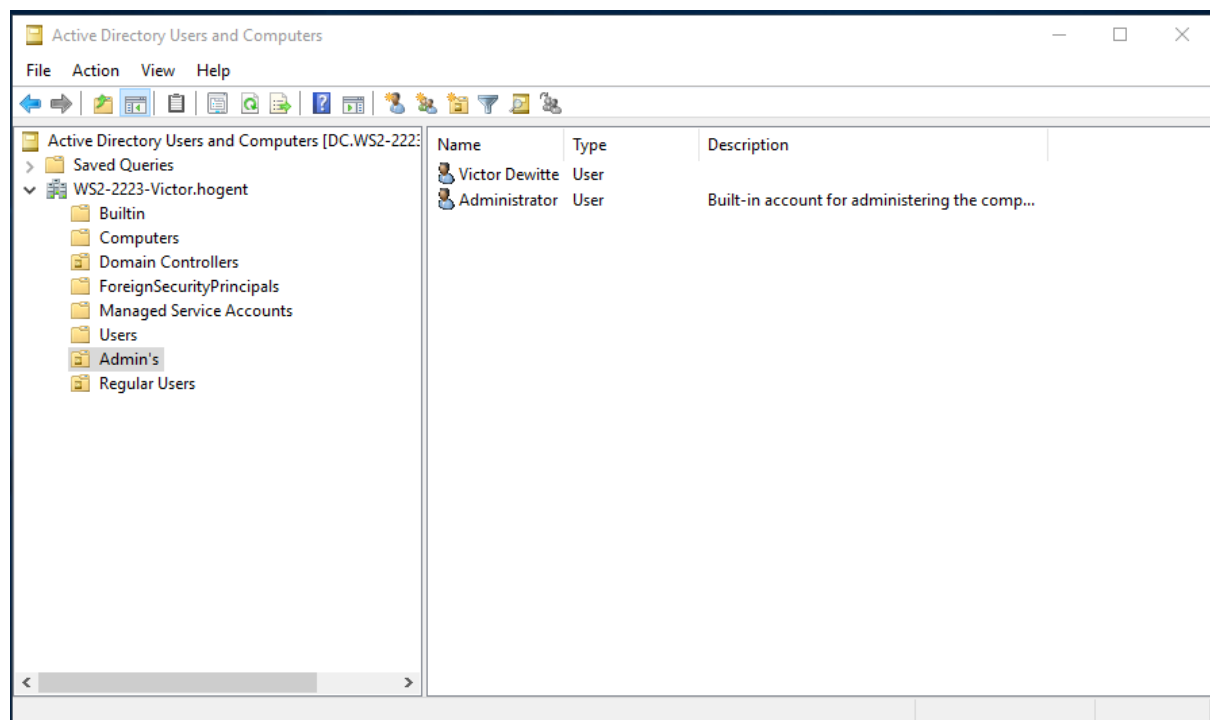


Fig.4 - De rechten van het "Victor Dewitte" account

Daarnaast zijn er de gewone gebruikers. Die toegang hebben tot het gebruiken van de gewone host computers. Ze kunnen daar de basis taken op uitvoeren. Ze hebben geen toegang tot het inloggen in de servers.

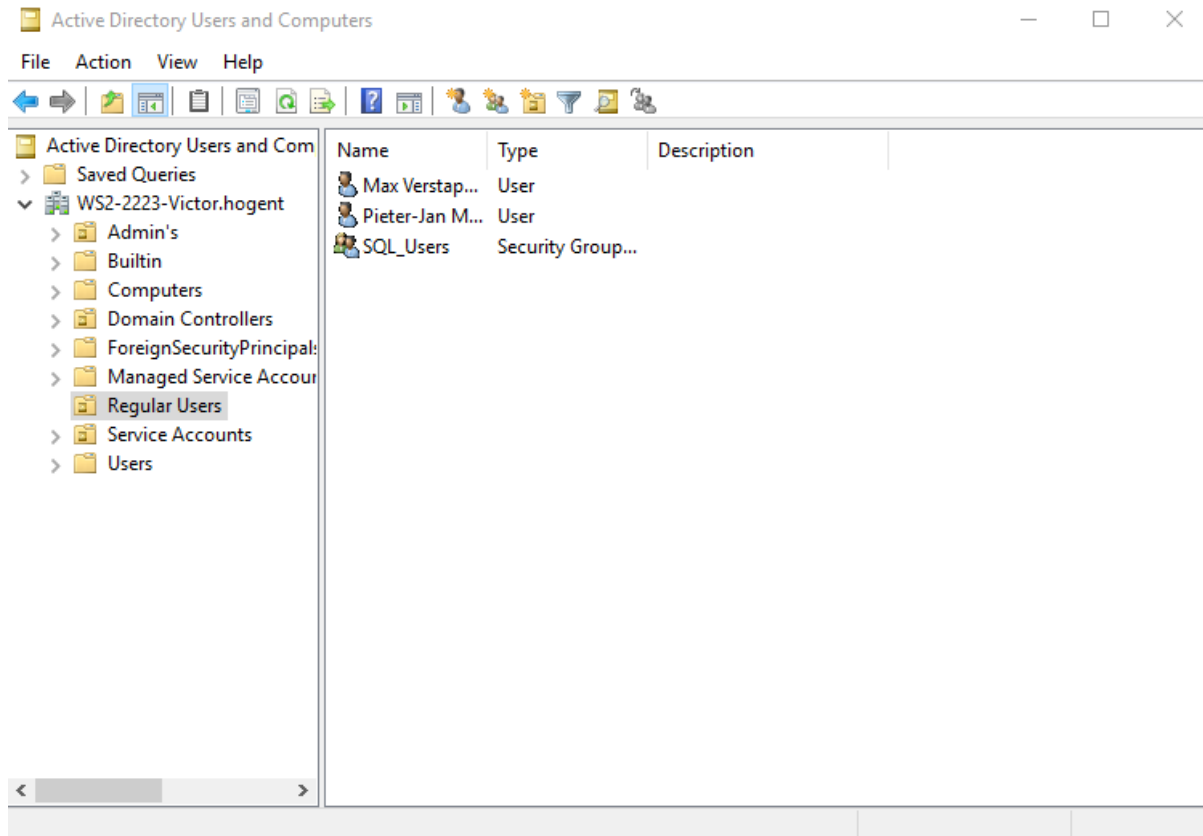


Fig.5 - Users in de AD

Sommige user's zullen extra rechten hebben om toegang te hebben tot de SQL Server. Deze zullen lid zijn van de SQL_Users groep. Deze groep zal ook de rechten hebben om de SQL Server te gebruiken maar niet beheren.

De Active Directory zal een apart service account voorzien voor elke applicatie die op de server's draait. Dit zal gedaan worden aan de hand van groepen die in de AD die toegevoegd worden tot de Admin users van de machine van wie ze admin rechten nodig hebben. De groepen zullen de naam van de applicatie hebben. Binnen de groepen kunnen er dan gemakkelijk gebruikers toegevoegd worden en verwijderd worden naar gelang er mensen komen en gaan die de rechten nodig hebben op die machines.

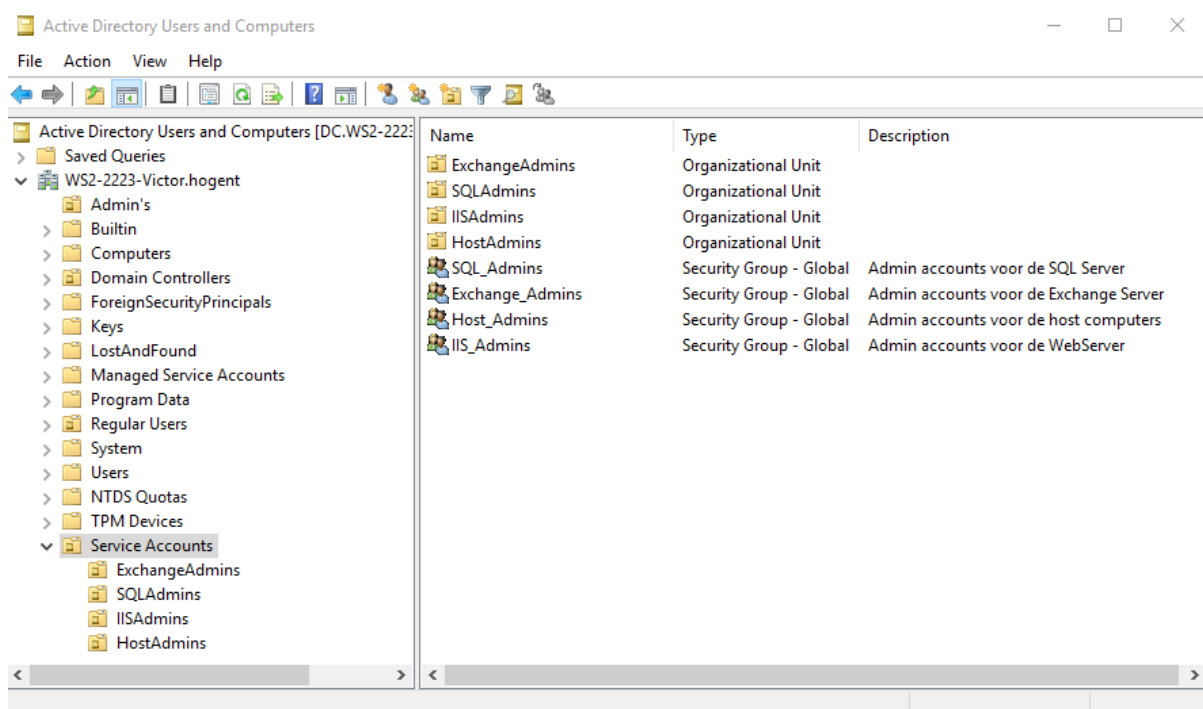


Fig.6 - Service Accounts OU

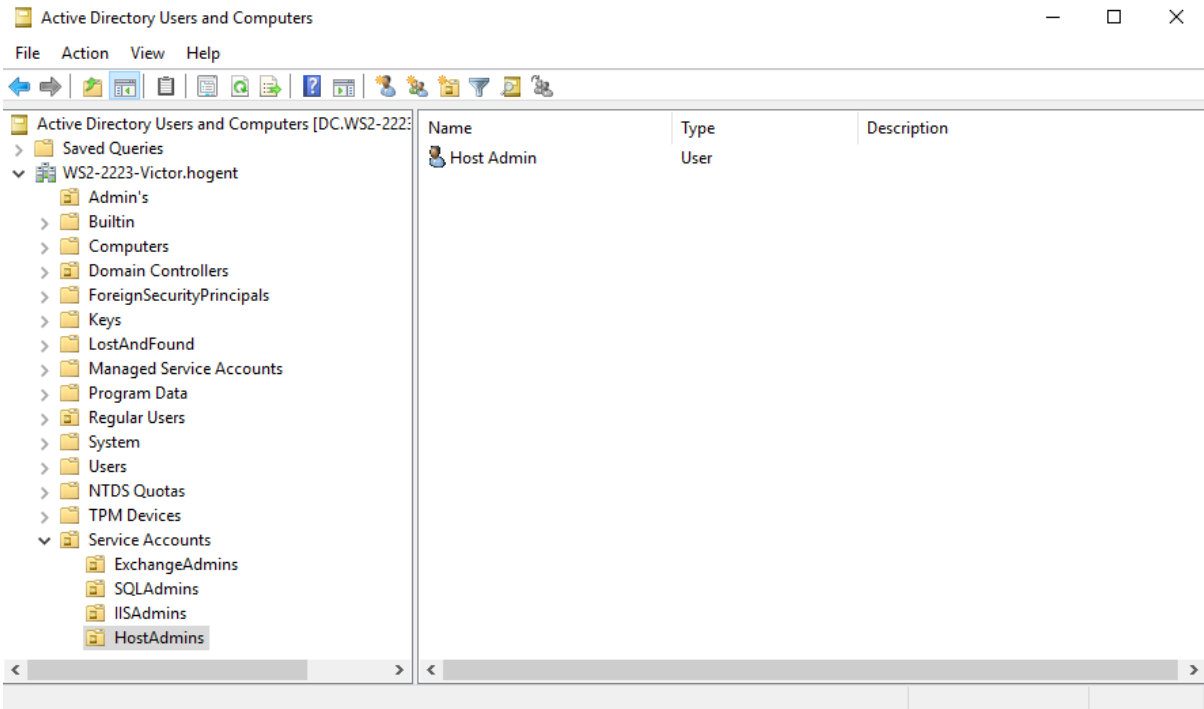


Fig.7 - Groep van de Host Admins

De DNS Server zal automatisch geconfigureerd worden door de AD DS, de nodige ldap records zullen dus automatisch gegenereerd worden. De DNS server zal ook de nodige forward lookup zones voorzien. Samen met de nodige AD DS records zullen er ook wat A records in de forward lookup zone zitten naar de servers, samen met een paar CNAME records en een MX record voor de Mail Server.

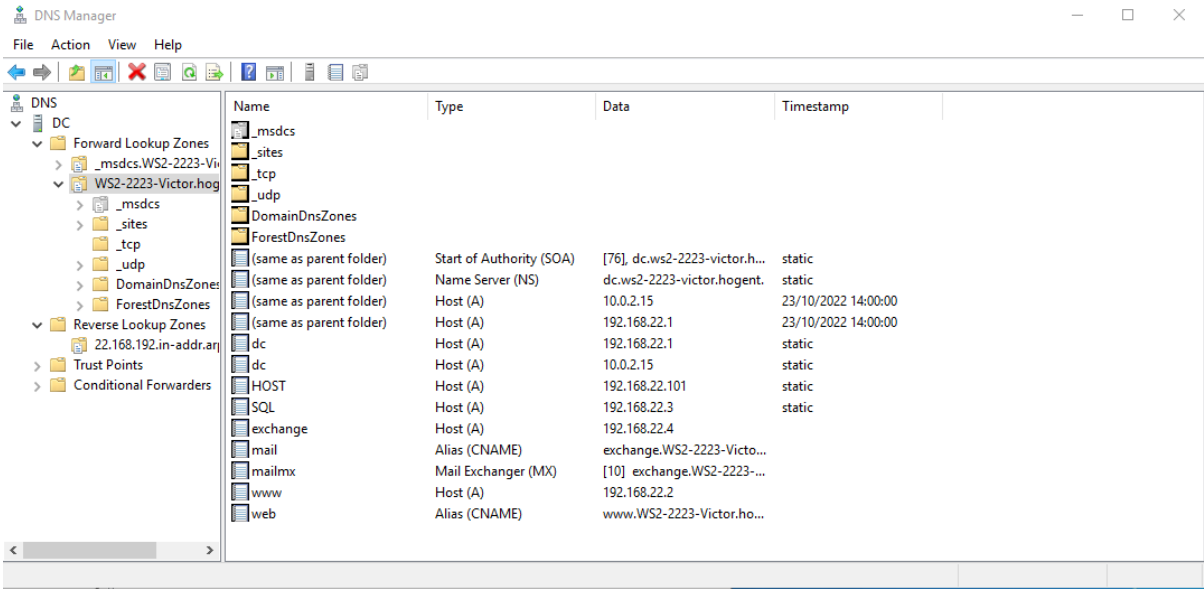


Fig.8 - DNS Server forward lookup zone

De DNS server zal ook de nodige reverse lookup records voorzien die automatisch kunnen gegenereerd worden door het aanmaken van de A records.

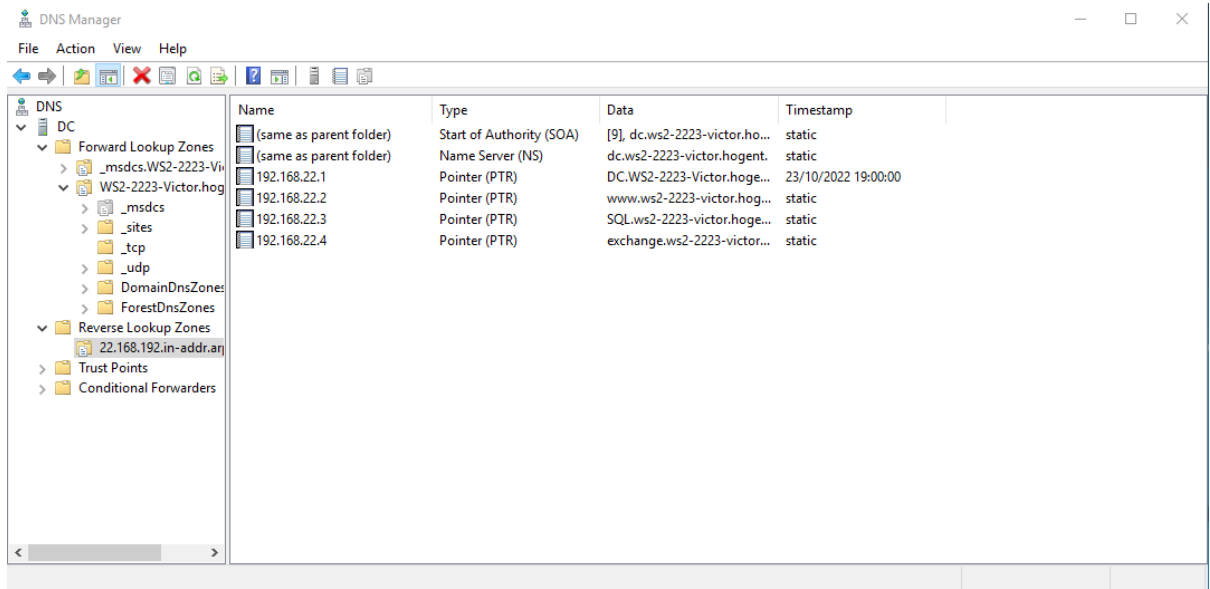


Fig.9 - DNS Server PTR records

De forwarders van de DNS server zullen ingesteld worden op die van op een hele hoop forwarders. Dit indien er een van de DNS servers niet bereikbaar is, zal de DNS server automatisch een andere forwarder gebruiken. Onder andere gebruik ik de forwarders van Google en Cloudflare. Ook worden er aan de hand van testen om het uur de configuratie van de DNS server getest.

Forwarders

Monitoring

IP Address	Server FQDN
208.67.222.222	dns.opendns.com
208.67.220.220	dns.opendns.com
208.67.222.220	resolver3.opendns.com
8.8.8.8	dns.google
8.8.4.4	dns.google
1.1.1.1	one.one.one.one

Fig.10 - DNS Server Forwarders

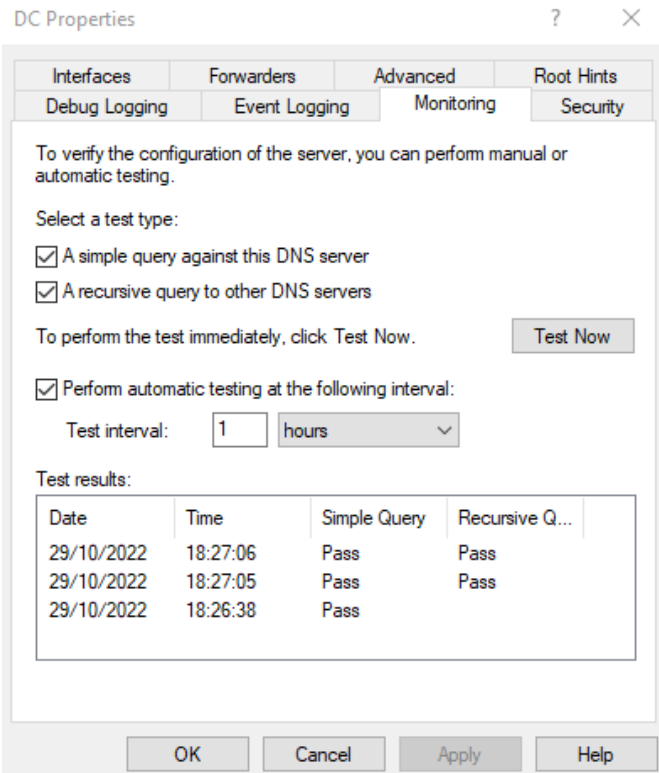


Fig.11 - DNS Server Monitoring

DHCP

De DHCP role zal ook op deze server staan. Deze zal ip adressen uitdelen aan alle clients in de opstelling. De servers krijgen allemaal een statisch adres. Er is dus maar 1 DHCP scope nodig. In dit geval is dit dus de UserScope.

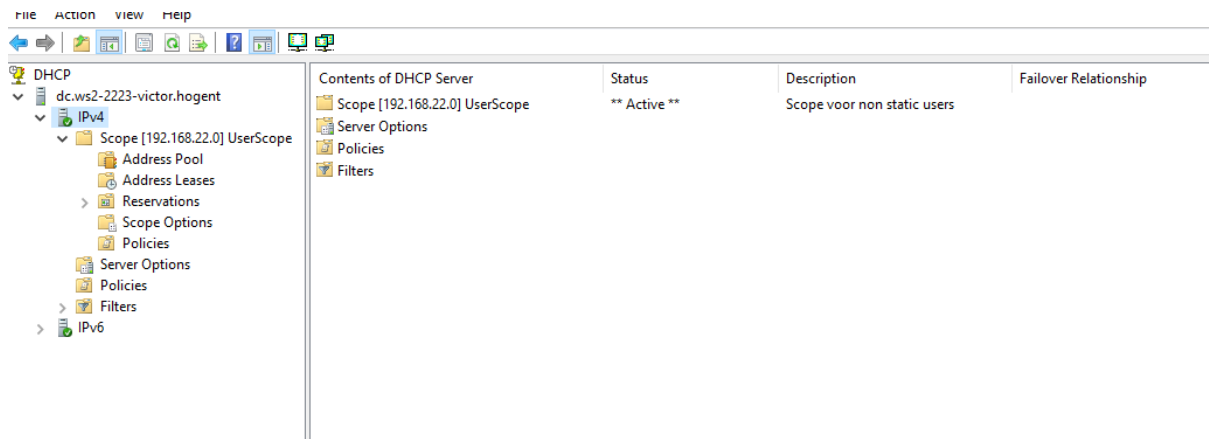


Fig.12 - UserScope in de DHCP Server

De clients binnen het netwerk krijgen een dynamisch address in de range van 192.168.22.101-150/24. De Users krijgen enkel een IPv4 adres toegewezen.

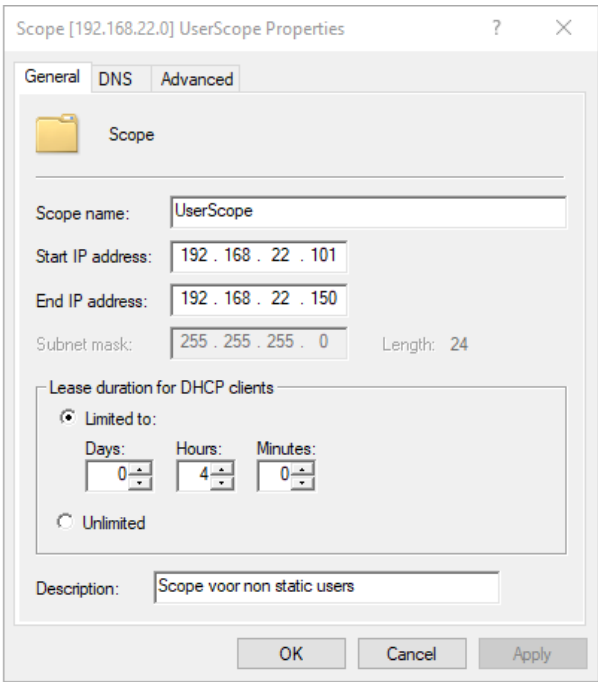


Fig.13 - UserScope's IP range

De DHCP server zal ook de nodige dns servers en default gateways meegeven aan de clients.

Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.22.1	None
006 DNS Servers	Standard	192.168.22.1, 192.168.22.3	None
015 DNS Domain Name	Standard	WS2-2223-Victor.hogent	None

Fig.14 - DNS Server en Default gateway in Scope Options

Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access Protection	Probation Expiration	Filter Profile	Policy
192.168.22.102	Host:WS2-2223-Vic...	2/11/2022 16:01:08	DHCP	080027a71...		Full Access	N/A	None	

Fig.15 - Host die een lease heeft bij de DHCP server

De Certification Authority (CA) zal digitale certificaten geven aan alle devices. Deze gaan helpen bij het veilig communiceren tussen de verschillende devices. De CA zal ook een certificaat geven aan de DC server zodat deze kan communiceren met de andere server's, ook zal de CA een certificaat geven aan de IIS server om de website te kunnen hosten met HTTPS.

Via de Certificate Authority webclient kunnen er certificaten aan de CA aangevraagd worden om gegenereerd te worden door de Server.

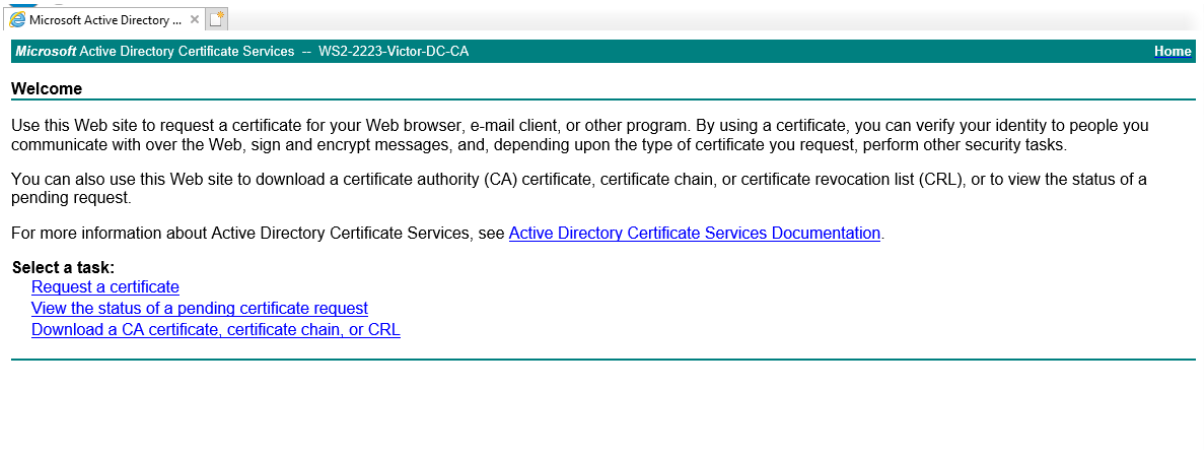


Fig.16 - Certificate Authority WebClient

Routing

De Routing and remote access role zal ook geïnstalleerd zijn op deze server. Deze zal de internet voorzien voor de hele omgeving. Het zal van de NAT adapter die aan de DC hangt network address translation doen met het internal network. Zo zullen alle server's die enkel een internal network adapter hebben ook voorzien zijn van een veilige verbinding met het internet. Er wordt aan Network address translation gedaan tussen de 2 interfaces.

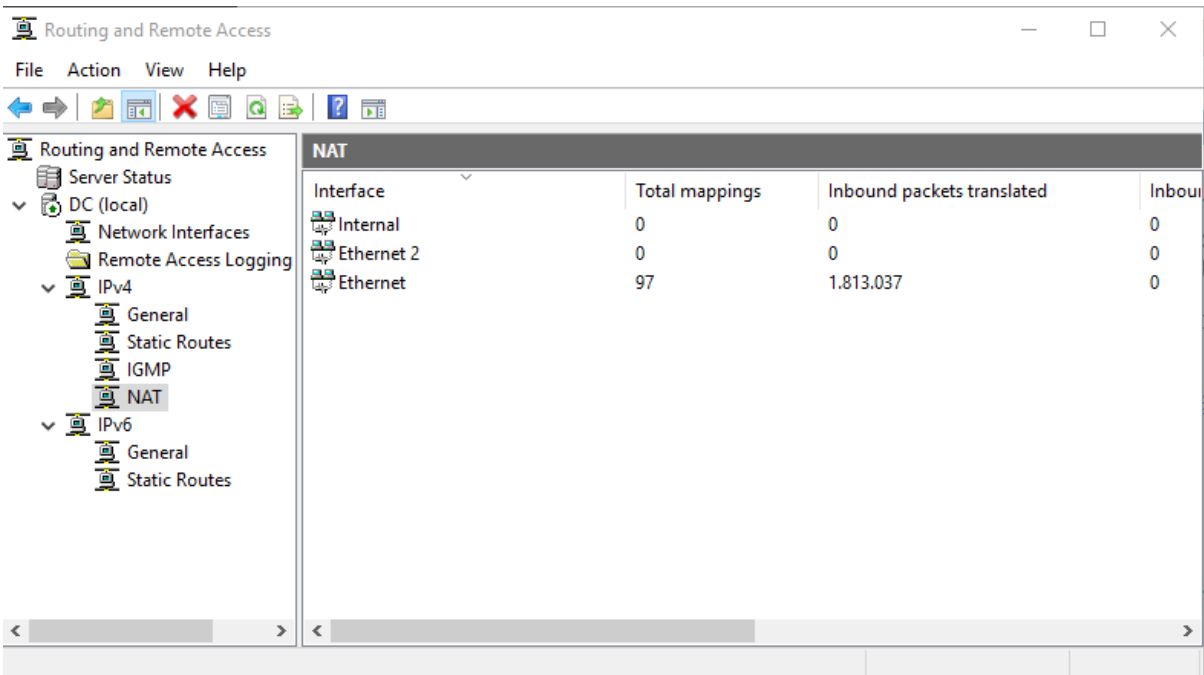


Fig.16 - Certificate Authority WebClient

SQL-Server

De SQL-Server zal enkel een command line interface hebben. Deze zal beschikken over 1 cores met 4gb ram en de windows server 2019 64 bit operating systeem zal er op geïnstalleerd zijn. De server zal ook beschikken over een 15gb virtuele harde schijf bevatten. Deze is dynamisch gealloceerd zodat hij enkel de nodige ruimte inneemt op je host machine. De complete domeinnaam van deze server zal **SQL.ws2-2223-victor.hogent** zijn.

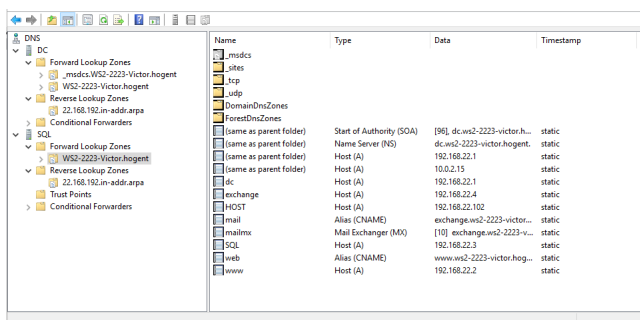
Op deze server zal enkel de SQL server draaien. De installatie is te vinden op de Website van Microsoft. Deze wordt gescheiden van andere roles zodat mensen met toegang tot deze server enkel deze server kunnen beheren zonder impact te hebben op andere services.

Er zal een database aangemaakt worden met de naam **WS2-2223-Victor**. Deze zal een aparte service account hebben. Deze service account zal enkel de nodige rechten hebben om de database te kunnen beheren. De database zal ook een aparte gebruiker hebben die enkel de nodige rechten heeft om de database te kunnen gebruiken.

De secundaire DNS zal op deze server komen om te functioneren als redundante DNS. Deze zal dus ook de nodige forward en reverse lookup zones voorzien. Secundaire servers kunnen ook worden gebruikt om DNS-queryverkeer te ontlasten in delen van het netwerk waar een zone zwaar wordt bevraagd. Als een primaire server niet beschikbaar is, kan een secundaire server bovendien dezelfde naamomzettingsservice bieden voor de gehoste zone terwijl de primaire server beschikbaar is.

De secundaire DNS bevat een secundaire zone voor de forward lookup zone en ook een secundaire zone voor de reverse lookup zone. Deze zal dus ook de nodige forward en reverse records kopiëren vanaf de primary DNS via een zone transfer voorzien.

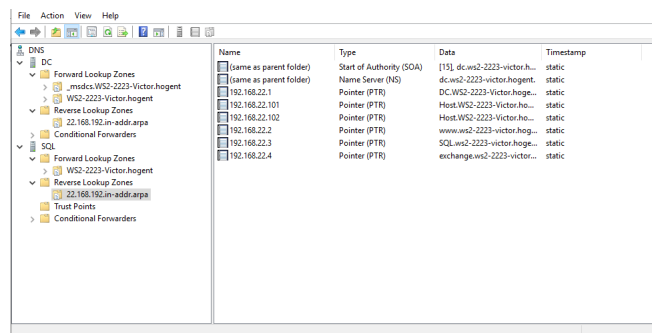
Forward lookup zone



Name	Type	Data	Timestamp
DC			
Forward Lookup Zones			
_msdcs.WS2-2223-Victor.hogent			
WS2-2223-Victor.hogent			
Reverse Lookup Zones			
22.168.192.in-addr.arpa			
Conditional Forwarders			
SQL			
Forward Lookup Zones			
WS2-2223-Victor.hogent			
Reverse Lookup Zones			
22.168.192.in-addr.arpa			
Trust Points			
Conditional Forwarders			
_start of authority (SOA)	static	[96] dc.ws2-2223-victor.h...	
_name server (NS)	static	dc.ws2-2223-victor.hogent.	
Host (A)	static	192.168.22.1	
Host (A)	static	10.0.2.15	
Host (A)	static	192.168.22.1	
Host (A)	static	192.168.22.4	
Host (A)	static	192.168.22.102	
Alias (CNAME)	static	exchange.ws2-2223-victor...	
Mail Exchanger (MX)	static	[10] exchange.ws2-2223-v...	
Host (A)	static	192.168.22.3	
Alias (CNAME)	static	www.ws2-2223-victor.hog...	
Host (A)	static	192.168.22.2	

Fig.10 - Secondary DNS Server Forward Lookup zone

Reverse lookup zone



Name	Type	Data	Timestamp
DC			
Forward Lookup Zones			
_msdcs.WS2-2223-Victor.hogent			
WS2-2223-Victor.hogent			
Reverse Lookup Zones			
22.168.192.in-addr.arpa			
Conditional Forwarders			
SQL			
Forward Lookup Zones			
WS2-2223-Victor.hogent			
Reverse Lookup Zones			
22.168.192.in-addr.arpa			
Trust Points			
Conditional Forwarders			
_start of authority (SOA)	static	[15] dc.ws2-2223-victor.h...	
_name server (NS)	static	dc.ws2-2223-victor.hogent.	
Pointer (PTR)	static	DC.WS2-2223-Victor.hoge...	
Pointer (PTR)	static	Host.WS2-2223-Victor.ho...	
Pointer (PTR)	static	Host.WS2-2223-Victor.ho...	
Pointer (PTR)	static	www.ws2-2223-victor.hog...	
Pointer (PTR)	static	SQL.ws2-2223-victor.hog...	
Pointer (PTR)	static	exchange.ws2-2223-victor...	

Fig.11 - Secondary DNS Server reverse Lookup zone

Als u een secundaire server toevoegt, is een ontwerpoptie om de server zo dicht mogelijk bij clients te plaatsen die veel behoefte hebben aan hostnaamomzetting. U kunt ook overwegen om secundaire servers op externe subnetten te plaatsen die zijn verbonden via langzamere of onbetrouwbare WAN-koppelingen.

Exchange-Server

De Exchange-Server zal enkel een command line interface hebben. Deze zal beschikken over 4 cores met 10gb ram en de windows server 2019 64 bit operating systeem zal er op geïnstalleerd zijn. De server zal ook beschikken over een 45gb virtuele harde schijf bevatten. Deze is dynamisch gealloceerd zodat hij enkel de nodige ruimte inneemt op je host machine. De complete domeinnaam van deze server zal **exchange.ws2-2223-victor.hogent** zijn.

Aan de hand van de verkregen ISO van exchange zal de mailserver geïnstalleerd worden. Deze zal een aparte service account hebben. Deze service account zal enkel de nodige rechten hebben om de mailserver te kunnen beheren. De mailserver zal ook een aparte gebruiker hebben die enkel de nodige rechten heeft om de mailserver te kunnen gebruiken.

Het zou moeten mogelijk zijn om de management webpagina van de mailserver te kunnen bezoeken via de browser op de domeincontroller die wel beschikt over een gui. De webpagina zal enkel toegankelijk zijn voor de gebruikers die toegang hebben tot de mailserver.

IIS-Server

De IIS Server met andere woorden de webserver van de organisatie zal enkel een command line interface hebben. Deze zal beschikken over 1 cores met 2gb ram. De server zal ook beschikken over een 15gb virtuele harde schijf bevatten. Deze is dynamisch gealloceerd zodat hij enkel de nodige ruimte inneemt op je host machine. De complete domeinnaam van deze server zal `web.ws2-2223-victor.hogent`, `www.ws2-2223-victor.hogent` of gwn `ws2-2223-victor.hogent` zijn. Mijn portfolio wordt afgebeeld op de site als demo.

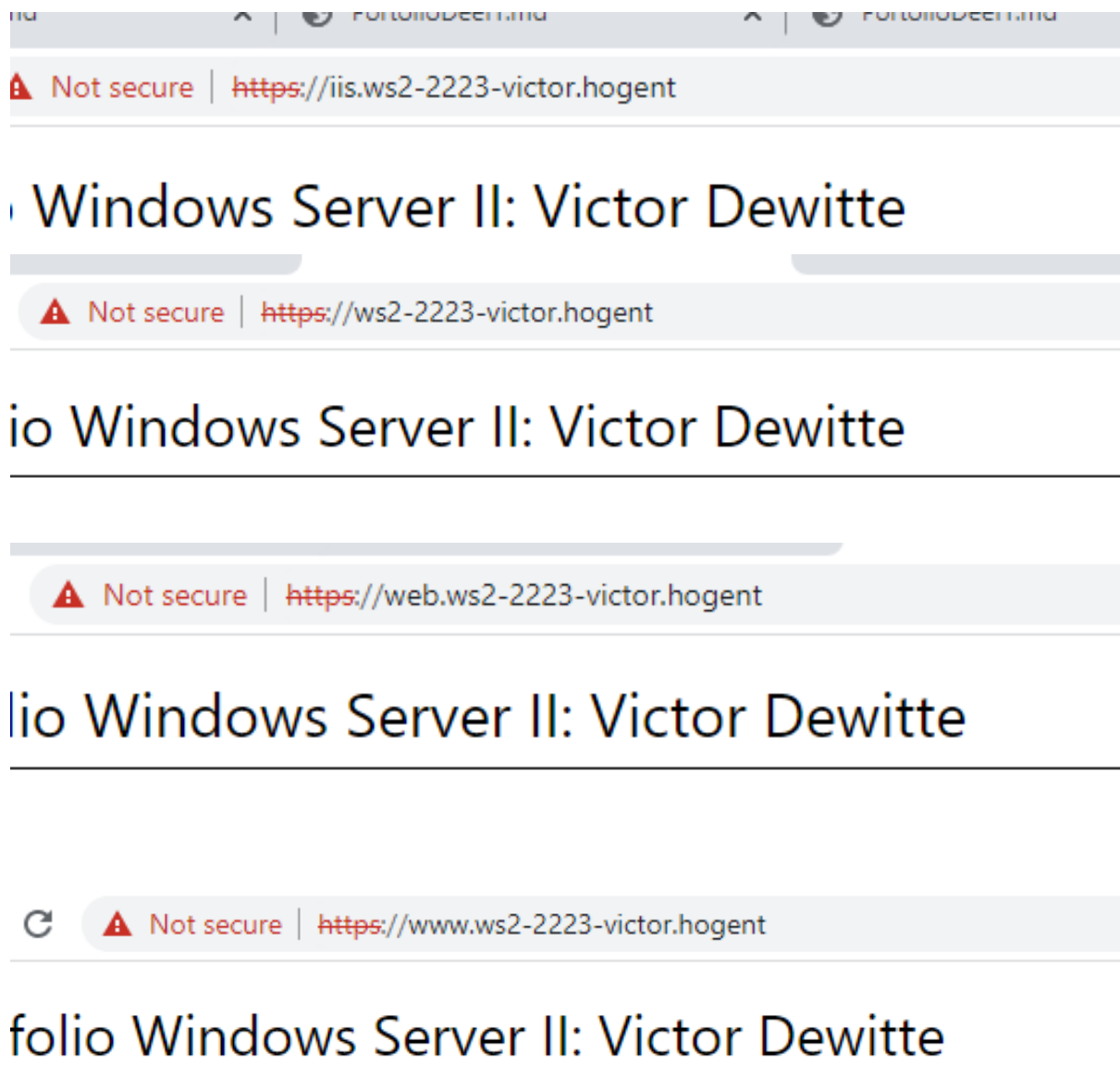


Fig. - Website is bereikbaar via deze links

Certificaat moet nog in orde gebracht worden met de CA Server...

De website van het domein zal bereikbaar zijn over heel het internal network maar enkel met https. De IIS role staat op een aparte server omdat alle users kunnen verbinden met deze server. Om het risico's op problemen door aanvallen of inbraak op de website te verminderen zal de IIS service op een aparte server geïnstalleerd staan.

Client

De client zal een gewone installatie van windows 10 zijn die een user heeft in het domein waarmee hij kan inloggen. De client zal ook een virtuele harde schijf hebben van 45gb. Deze is dynamisch gealloceerd zodat hij enkel de nodige ruimte inneemt op je host machine. De Client krijgt een ip address van de DHCP server.

Google chrome en SQL server management studio worden geïnstalleerd op de server. Deze zijn nodig om de website te kunnen bezoeken en de database te kunnen beheren. Ook is er een browser nodig om mails te versturen met de online mail client.

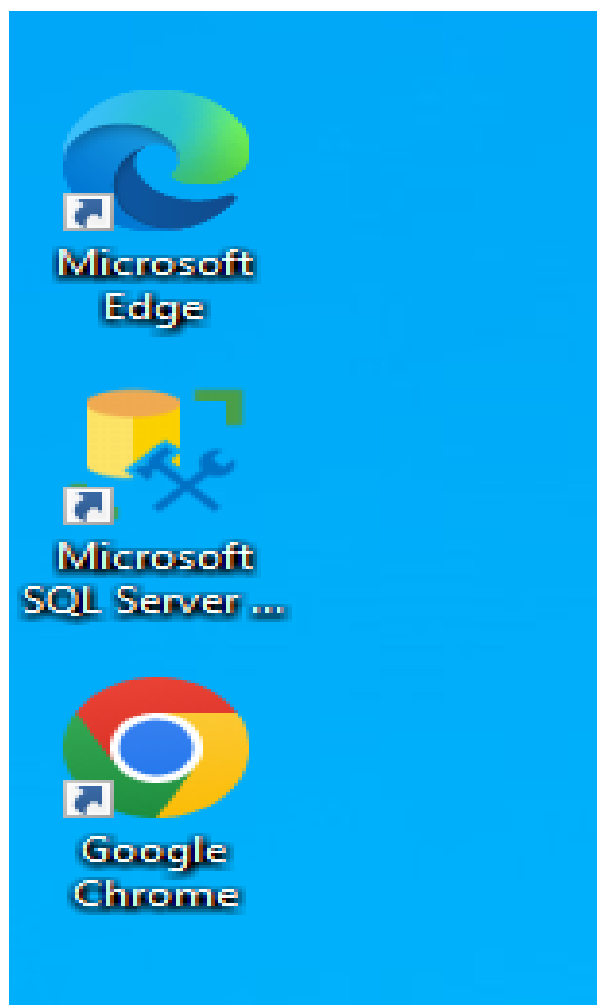


Fig. - Apps op de host device