



MONOGRAFIE

Milan Vermeulen, Jonas Vermesen, Jarno Bollen, Jaime Saes

Opleiding: VDO Netwerkbeheer

Academiejaar 2019-2020

Docent: Eddy Debauve, Steven Reekmans; Luca Ruggiero

Voorwoord

Voor onze eindproef kregen we de opdracht om een netwerk te bouwen waarin we laten zien dat we alle vaardigheden die we doorheen het jaar hebben verworven onder de knie hebben. Het moest zeker een goede verdeling hebben van zowel Linux en Windows toestellen, er moesten ook zeker een paar dingen in verwerkt worden die niet gezien zijn doorheen het jaar.

Graag willen wij Steven Reekmans, Eddy Debauve en Luca Ruggiero bedanken voor het delen van hun kennis en ervaring.

Veel leesplezier

Groep B: Milan Vermeulen, Jonas Vermesen, Jarno Bollen, Jaime Saes

Inhoudsopgave

Het team	7
Milan Vermeulen	7
Contactgegevens	7
Profiel	7
Opleidingen	7
Ervaring	7
Talenkennis:	7
Jonas Vermesen	8
Contactgegevens	8
Profiel	8
Opleidingen	8
Ervaring	8
Talenkennis:	8
Jarno Bollen	9
Contactgegevens	9
Profiel	9
Opleidingen	9
Ervaring	9
Talenkennis:	9
Jaime Saes	10
Contactgegevens	10
Profiel	10
Opleidingen	10
Ervaring	10
Talenkennis:	10
De opdracht	11
Het netwerk	11
Taakverdeling	12
Milan Vermeulen	12
Jonas Vermesen	12
Jarno Bollen	12

Jaime Saes	12
Prijzen	13
TCO	13
Site 1 Hoofdkantoor	14
Firewall	14
Wat is een firewall?	14
Waarom PFsense?	14
Firewallrules	14
OpenVPN configuratie pfSense	15
OpenVPN Users toevoegen	17
Active Directory	20
Wat is een active directory?	20
Netwerk instellen	20
Installeren van Active Directory services	20
Opzetten van het domein	21
Reverse DNS Lookup zone	22
DHCP server installeren	23
Users en Groepen registreren.	24
Via een batch file de leden een snellere weg geven naar hun fileshares.	26
Mailserver	29
Wat is een mailserver?	29
Waarom Microsoft Exchange?	29
Send Connector	29
Gebruikers aanmaken	29
Postvak beheer	30
Exchange log files cleanup	31
PST files exporteren	31
Fileserver	34
Netwerk configureren.	34
Verbinding maken met de Active Directory	34
Aanmaken van resource pools	35
Rechten toekennen	36

Home folder	36
Public folder	37
Group folders	38
Back-up Server	40
Wat is een backup?	40
Waarom Veeam?	40
Back-up job	40
E-mail notificaties	41
Monitoring	42
Nagios core	42
Hosts toevoegen	43
Sharepoint	44
Wat is Sharepoint?	44
Sharepoint configuratie	44
Site 2	48
Firewall	49
WAN Gateway	49
LAN RULES	50
IPSEC	50
Read Only Domain Controller	53
Back-up PST-files	55
Monitoring	58
Exchange	58
FreeNAS	59
RODC	59
Webserver	62
Wat is een DMZ?	62
Webserver	62
Service Level Agreement	65
Version	65
Approval	65
Agreement Overview	65

Goals & Objectives	65
Stakeholders	66
Periodic Review	66
Service Agreement	66
Service Scope	66
The following Services are covered by this Agreement;	66
Customer Requirement	67
Service Provider Requirements	67
Service Assumptions	67
Service Management	67
Service Availability	67
Service Requests	67
Bronvermelding	67
Slot	69

Het team

Milan Vermeulen

Contactgegevens

Plaggenstraat 57 3600 genk

GSM: 0471106085

24 Januari 1996

Profiel

ik ben een sociaal persoon, mijn vrienden omschrijven me vaak als de rust zelve omdat ik niet snel opgejaagd geraak. Ik kan zowel in groep als alleen werken. Van nature ben ik ook heel Leergierig, sta dus ook altijd open om nieuwe dingen te leren.

In mijn vrije tijd doe ik aan Crossfit en Spinnen, en ben ook een heel actief lid Humanistische Jongen Leopoldsburg.

mijn vaardigheden zijn onder andere:

- stressbestendig
- leergierig
- sociaal
- Teamwerk

Opleidingen

- 2014 Secundair diploma Humane wetenschappen KA Leopoldsburg
- 2016-2017 Bacheloropleiding wijsbegeerte en moraalwetenschappen VUB
- 2017 2018 Bacheloropleiding Toegepaste Informatica Thomas More Geel
- 2019 -2020 Syntra netwerkbeheer

Ervaring

Studentenjobs:

- 2012 - 2015 Beenhouwerij Alex
- 2012- 2014 Accent Interieur
- 2012 - 2016 Pukkelpop

Talenkennis:

Nederlands: moedertaal

Engels: uitstekend

Jonas Vermesen

Contactgegevens

Tuilterstraat 14, 3510 Kermt

GSM: 0494 28 81 85

31 Maart 1999

Profiel

Ik ben een rustig persoon, dit is te merken in groepswerken. ik zal niet snel de leiding op mij nemen, maar zou er geen probleem mee hebben moest de leiding mij gegeven worden. Ik werk graag in groep omdat ik ook graag andere hun mening hoor over bepaalde onderwerpen.

In mijn vrije tijd ben ik veel bezig voor de KSA, ik behoor hier tot de Leidingsgroep. ook ben ik thuis graag bezig met kleine projectjes met bijvoorbeeld mijn Raspberry Pi.

Opleidingen

- 2017 Secundair diploma informaticabeheer KTA1 Hasselt
- 2018 toegepaste informatica PXL
- 2019 Marketing UCLL
- 2020 netwerkbeheer Syntra-Limburg

Ervaring

studentenjobs:

- 2016-2017 De spork
- 2018-2020 Carrefour
- 2019-2020 Deliveroo

Stage:

- 2017 ICT helpdesk Tractebel NV.

Talenkennis:

Nederlands: moedertaal

Engels: uitstekend

Jarno Bollen

Contactgegevens

Smeetsstraat 4 Lanaken

GSM: 0471 69 11 90

28 November 1994

Profiel

Ik ben een doelgericht persoon. Hoe meer tegenslagen er op mijn weg voorkomen, hoe gemotiveerder ik ben om het doel te bereiken. Mijn vrije tijd spender ik zowel achter de computer als in het bos. Ik werk graag in groepsverband maar heb er geen bezwaar bij om opdrachten alleen uit te werken. Opgeven staat niet in mijn woordenboek.

Opleidingen

- sociaal technische wetenschappen (middelbaar)
- verkoop (cvo)
- netwerkbeheer (cvo)

Ervaring

studentenjobs:

- hulpkok The Pigeon
- poetshulp ziekenhuis
- Productie Paas Food
- Afwashulp Dali

Stages:

- Rekkenvuller kruidvat

Talenkennis:

Nederlands: moedertaal

Engels: Uitstekend

Frans: Ok

Jaime Saes

Contactgegevens

Weg naar Ellikom 147 Oudsbergen

GSM: 0483 39 44 03

31 Juli 1997

Profiel

Ik ben een kalm, stressbestendig persoon die houdt van afwisseling. Hou mij het best bezig met veel verschillende projecten zodat ik alles met een frisse kijk in mijn handen kan nemen.

In mijn vrije tijd doe vind je me vaak in het bos, ga graag urenlang wandelen met de honden of joggen. Vind het leuk om te dansen en genieten van het leven.

Mijn vaardigheden zijn onder andere:

- Stressbestendig
- Geïnteresseerd
- Easy-going
- Gefocused

Opleidingen

- 2016 Secundair diploma Elektrotechnische installatietechnieken Tism Bree
- 2017-2018 3D-Artist Syntra Hasselt
- 2019 -2020 Netwerkbeheerder Syntra Genk

Ervaring

Studentenjobs:

- 2013-2014 Bakkerij
- 2014-2015 Skiverhuur Snowvalley Peer
- 2016 Technische dienst Nedlin Stein
- 2015-2020 Bar/Kelner Snowvalley Peer

Talenkennis:

Nederlands: moedertaal

Engels: uitstekend

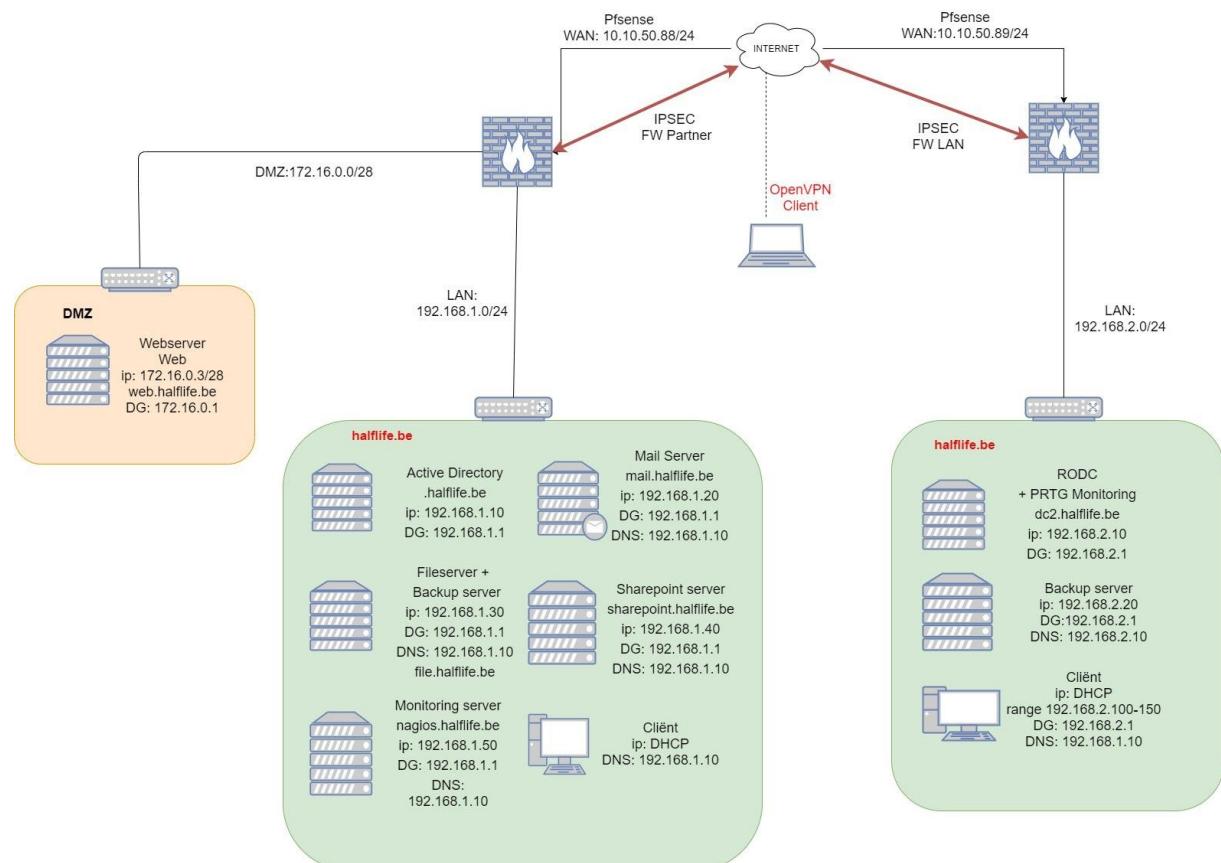
Frans: redelijk

De opdracht

Wij kregen de vraag om de IT-Infrastructuur te voorzien voor een fictief bedrijf genaamd Halflife waarin de werknemers moeten kunnen mailen, bestanden delen en van op afstand kunnen werken. Dit netwerk moet volledig gemonitord worden en moet een waterdichte back-up plan bevatten.

Het netwerk

Het netwerk van Halflife is opgedeeld in 2 sites, Site 1 is het hoofdkantoor waarvan de meeste mensen ook gaan werken. In de LAN bevindt zich de active directory waar de DNS en DHCP ook op draaien, onze mailserver vindt je hier ook hiervoor gebruiken we Microsoft Exchange. In de LAN vindt je ook onze File- en backup server , 1 van onze monitoring servers en een Sharepoint Server waar de teamsite op draait. Site 2 andere kantoor deze 2 kantoren zijn verbonden via een VPN verbinding tussen de 2 firewalls om op die manier één groot netwerk te maken. Om ons netwerk wat redundant te maken hebben we op de tweede site een Read Only Domain Controller geïnstalleerd en een tweede backup server. Er is ook een DMZ voorzien voor de Externe website, deze zetten we niet in ons eigen netwerk voor veiligheidsredenen. We zetten deze in de DMZ omdat deze beschikbaar is voor iedereen op het internet en moest deze dus gehacked worden kunnen ze nog altijd niet bij onze andere servers want deze zitten in onze LAN. We hebben ook een manier voorzien zodat de werknemers van thuis kunnen werken via een VPN connectie.



Taakverdeling

Milan Vermeulen

- Mail server
- Webserver
- Sharepoint Server
- backup mailboxes

Jonas Vermesen

- Firewall partner netwerk
- VPN
- Nagios en PRTG monitoring
- Cobian backup server

Jarno Bollen

- Active directory
- Read Only Domain Controller
- Fileserver

Jaime Saes

- Firewall hoofdkantoor
- Open Vpn
- Veeam Backup server

Prijzen

TCO

Netgate SG 1100	€197
Netgate SG 5100	€699
Dell poweredge t140 server standard	€796
Dell poweredge r540 server basic	€1433.3

VMware vSphere Essentials Kit	€695 x 2
Windows Server Standard 2019	€972 x2 (per jaar)
Client Access Licenses	€45 voor 24 users (per jaar)

Milan	€75 / uur	75 uur	€5625.00
Jonas	€75 / uur	75 uur	€5625.00
Jarno	€75 / uur	75 uur	€5625.00
Jaime	€75 / uur	75 uur	€5625.00

Totaal	€23 379.30
---------------	-------------------

Site 1 Hoofdkantoor

Firewall

Wat is een firewall?

Een firewall is een onderdeel van je netwerk dat ervoor zorgt dat de rest van je netwerk veilig is tegen misbruik van aan buitenaf. Deze doet dit ongewenst verkeer uit je netwerk te houden.

Waarom PFsense?

Dit is een open source firewall/router gebaseerd op FreeBSD, dat geïnstalleerd kan worden op een fysieke computer of virtuele machine. Configureerbaar door CLI of een web-based interface. Gratis gebruik en installeerbaar door ISO bestand of USB-stick.

PFSense is bovendien ook nog een licht programma en omdat we een beetje moesten oppassen met de resources die we tot beschikking hadden was dit dus ideaal.

Firewallrules

WAN interface:

OpenVPN: 1194 = OpenVPN

LAN interface:

ICMP (LAN net any rule)

Web Traffic (LAN netwerk): 53 = DNS (Domain Name System)
80 = HTTP (Hypertext Transfer Protocol)
443 = HTTPS (Hypertext Transfer Protocol over TLS/SSL)

Microsoft Active

Directory Server: 25 = SMTP (Simple Mail Transfer Protocol)
67 = Bootstrap Protocol (BOOTP) server,
DHCP
88 = Kerberos authentication system
123 = NTP (Network Time Protocol)
135 = Microsoft EPMP (End Point Mapper)
137 = Netbios Name Service
138 = Netbios Datagram Service
139 = Netbios Session Service
389 = LDAP (Lightweight Directory Access Protocol)
445 = MS-DS (Directory Services) AD,
Windows shares, SMB file sharing

464 = Kerberos Change/Set password
 636 = LDAPS (Lightweight Directory Access Protocol over TLS/SSL)
 2535 = MADCAP (Multicast Address Dynamic Client Allocation Protocol)
 3268 = MSFT-GC (Microsoft Global Catalog)
 3269 = MSFT-GC-SSL (Microsoft Global Catalog over SSL)
 5722 = MS RPC, DFSR (SYSVOL) Replication Service
 9389 = ADWS, MS AD DS Web Services, Powershell

Microsoft Exchange

Server:

25	= SMTP (Simple Mail Transfer Protocol)
110	= POP3 (Post Office Protocol V3)
143	= IMAP (Internet Message Protocol)
587	= Email Message Submission (SMTP)
993	= IMAPS (Internet Message Protocol over TLS/SSL)
995	= POP3S (Post Office Protocol V3 over TLS/SSL)

DMZ interface:

ICMP (DMZ net any rule)

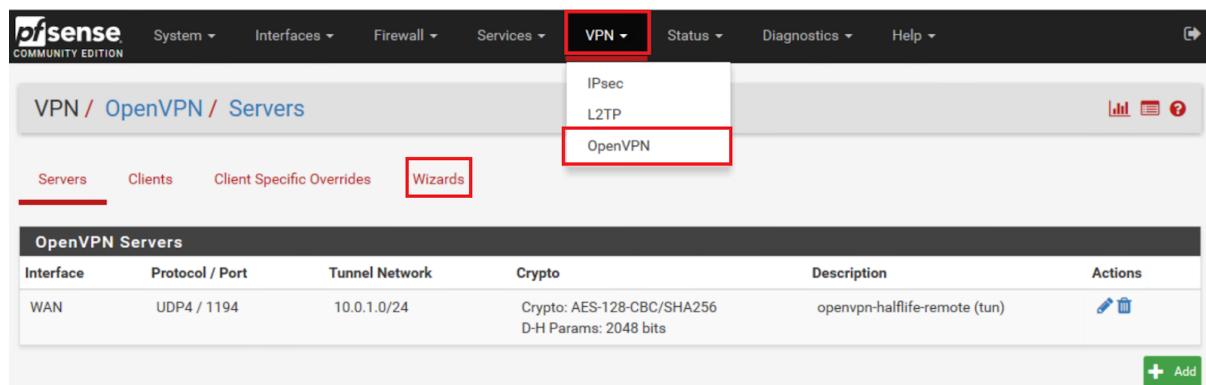
Web Traffic

(DMZ netwerk):

53	= DNS (Domain Name System)
80	= HTTP (Hypertext Transfer Protocol)
443	= HTTPS (Hypertext Transfer Protocol over TLS/SSL)

OpenVPN configuratie pfSense

Ga naar het tab VPN => OpenVPN => Wizards



The screenshot shows the pfSense web interface under the 'VPN' tab. In the 'Wizards' section, the 'OpenVPN' option is selected. Below it, the 'OpenVPN Servers' table is displayed, showing a single entry for 'WAN' with details: Protocol / Port: UDP4 / 1194, Tunnel Network: 10.0.1.0/24, Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits, Description: openvpn-halflife-remote (tun), and Actions: edit and delete buttons.

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	10.0.1.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	openvpn-halflife-remote (tun)	

Selecteer wat voor type authenticatie backend we gaan gebruiken:

- => Type of server: Local User Access
- => Next

Kies een naam voor de Certificate Authority:

- => Certificate Authority : OpenVPN Server
- => Next

Nu kun je de instellingen van je CA certificate gaan configureren.

- => Key length minimaal is 2048 bit, mocht je een sterkere beveiliging willen kies dan 4096 bit.
- => Country code: BE
- => State or Province: Limburg
- => City: Genk
- => Organization: halflife.be
- => E-mail: administrator@halflife.be
- => Next

Hierna stellen we General OpenVPN Server Information in.

- => Interface: WAN
- => Protocol: UDP (je kunt ook TCP kiezen voor een gegarandeerde packet delivery maar dan wordt de dataverwerking trager)
- => Local Port: 1194 (standaard OpenVPN port, mocht je een andere specifieke poort nodig hebben kun je die hier instellen)
- => Description: *Geef een logische en herkenbare descriptie*
- => Next

Nu komen de Cryptografische settings aan bod.

- => TLS Authentication: Aanvinken
- => Generate TLS Key: Aanvinken
- => DH Parameter Length: 2048 bit
- => Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)
- => Auth Digest Algorithm: SHA1 (160-bit)
- => Hardware Crypto: No Hardware Crypto Acceleration
- => Next

Tunnel settings instellen.

- => Tunnel Network: 10.0.0.0/24
- => Redirect Gateway: Aanvinken (Mocht je willen dat alle client data niet door de tunnel heen gaat vink dit dan uit)
- => Local Network: 192.168.1.0/24 (Ons LAN netwerk)
- => Concurrent Connections: Blanco (Mocht je willen limiteren hoeveel clients op 1 moment deze server kunnen gebruiken stel dit dan in)
- => Compression: Omit Preference (Use OpenVPN Default)

- => Type-of-Service: Uit laten staan
- => Inter-Client Communication: Uit laten staan
- => Duplicate Connections: Uit laten staan
- => Next

Kies nu de instellingen die de OpenVPN clients gaan gebruiken. Deze settings worden meestal verzorgd door servers op je netwerk maar je kunt er nog bij plaatsen.

- => Dynamic IP: Aanvinken
- => Topology: Subnet - One IP adres per client in a common subnet
- => DNS Default Domain: 192.168.1.10
- => DNS Server 1: 8.8.8.8
- => DNS Server 2: 8.8.4.4
- => NetBIOS Options: Aanvinken
- => Netbios Node Type: none
- => Next

Volgend screen kunnen we de OpenVPN wizard de firewall rule voor ons laten opbouwen.

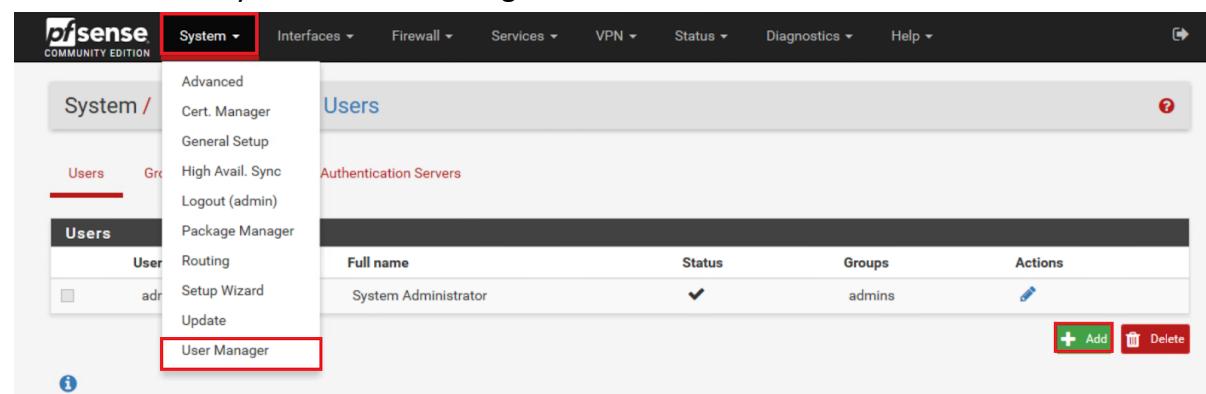
- => Firewall Rule: Aanvinken
- => OpenVPN rule: Aanvinken
- => Next

Nadat we al de vereiste settings hebben ingegeven, is de setup wizard klaar. Klik op finish om alle settings toe te passen tot pfSense.

- => Finish

OpenVPN Users toevoegen

Ga naar het tab System => User Manager => Add



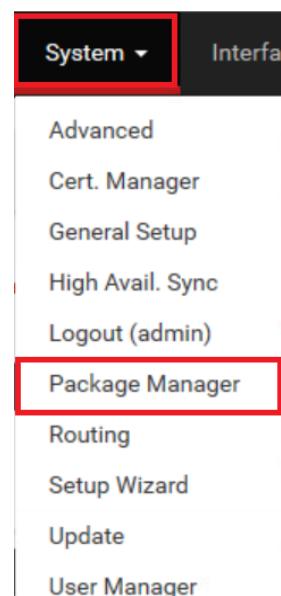
The screenshot shows the pfSense User Manager interface. The top navigation bar has tabs for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'System' tab is selected. On the left, there's a sidebar with 'System /' at the top, followed by 'Users' (which is selected and highlighted in red), 'Groups', 'Advanced', 'Cert. Manager', 'General Setup', 'High Avail. Sync', 'Logout (admin)', 'Package Manager', 'Routing', 'Setup Wizard', 'Update', and 'User Manager' (which is also highlighted in red). The main content area is titled 'Users' and contains a table with one row: 'Full name' (System Administrator), 'Status' (✓), 'Groups' (admins), and 'Actions' (with a pencil icon). At the bottom right of the table are two buttons: a green '+' labeled 'Add' and a red '-' labeled 'Delete'.

- => Username: VPNuser
- => Password: *****
- => Full name: Wordt enkel gebruikt voor administratieve informatie
- => Expiration Date: Je kunt deze user tijdelijk maken door een toekomstige datum in te stellen MM/DD/YYYY
- => Group Membership: We kunnen hier de user in de juiste groep plaatsen b.v. admins

- => Certificate: Aanvinken
- => Descriptive name: Certificate VPNUser
- => Certificate Authority: OpenVPN
- => Key Length: 2048 bits
- => Lifetime: 3650 of meer
- => Save

Nu moeten we nog een package downloaden om OpenVPN configuratie te exporteren zodat de client dit kan gebruiken.

Ga naar:



Zoek voor: 'openvpn' en install package 'openvpn-client-export'

Name	Version	Description
openvpn-client-export	1.4.23	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.

Na de installatie hebben we een nieuwe tab 'Client Export' bij OpenVPN

In de client export settings kun je verschillende instellingen doen aan client connectie gedrag.
Voor ons zijn de basic settings goed.

=> Save

Nu kun je onderaan de pagina de config of volledige OpenVPN client downloaden.

The screenshot shows the 'OpenVPN Clients' interface. On the left, under 'User', 'VPNUser' is selected. In the center, 'Certificate Name' is listed as 'Certificate VPNUser'. On the right, the 'Export' section is expanded. It includes sections for 'Inline Configurations' (with 'Most Clients', 'Android', and 'OpenVPN Connect (iOS/Android)' buttons), 'Bundled Configurations' (with 'Archive' and 'Config File Only' buttons, where 'Config File Only' is highlighted with a red box), and 'Current Windows Installer' (with '7/8/8.1/2012r2' and '10/2016/2019' buttons, where '10/2016/2019' is highlighted with a red box). Other sections like 'Old Windows Installers' and 'Viscosity' are also visible.

Config File Only:

- => Klik op download en save het bestand op je computer
- => Open het programma OpenVPN GUI op je computer
- => Rechtermuisknop beneden in het systeemvak op de taakbalk
- => Import File
- => Open de config file

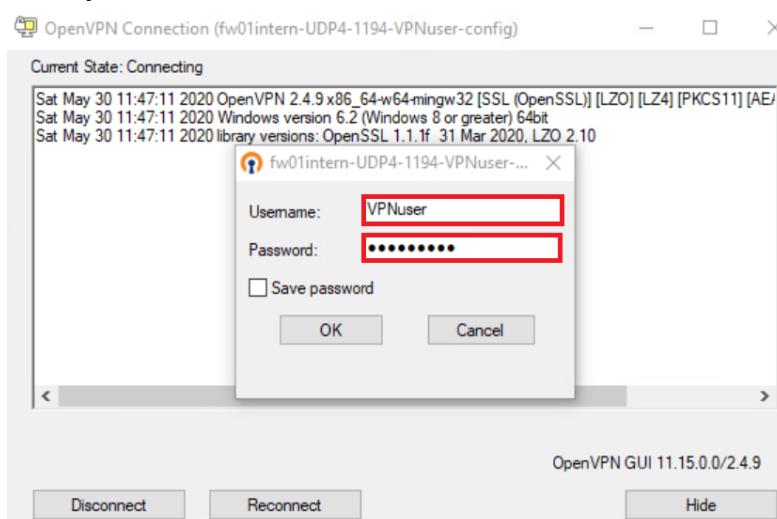
Current Windows Installer:

- => Klik op download en save het bestand op je computer
- => Run het bestand
- => Volg de installatiewizard

Nu installeert deze automatisch config files, certificate en key files.

Inloggen:

Gebruik de inloggegevens van de User die je voor de connectie hebt aangemaakt met het daarbij behorende wachtwoord.



Active Directory

Wat is een active directory?

Een active directory is een manier voor de beheerders om het netwerk en de users op een centrale plek te kunnen beheren. Hier kunnen ze bepaalde rechten toekennen aan bepaalde users/groepen. Het domein wordt gemaakt door de Active Directory.

Netwerk instellen

Voor we beginnen geven we onze active directory een static IP, dit doen we bij onze netwerkinstellingen onder ipv4.

IP address:	192 . 168 . 1 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

We kiezen een ip adres beschikbaar in de range van ons netwerk, samen met de subnetmask voor een /24 range. De default gateway is de LAN poort van de firewall.

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	. . .

Het DNS stellen we voorlopig in het publiek adres '8.8.8.8'. Bij het installeren van de active directory zal deze automatisch gewijzigd worden naar het loopback adres '127.0.0.1'

Installeren van Active Directory services

In de server manager kiezen we voor add roles and features

Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.

We duiden de server aan die we de rol willen toekennen.

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

Filter:		
Name	IP Address	Operating System
ActiveDirectory	169.254.45.239...	Microsoft Windows Server 2019 Standard

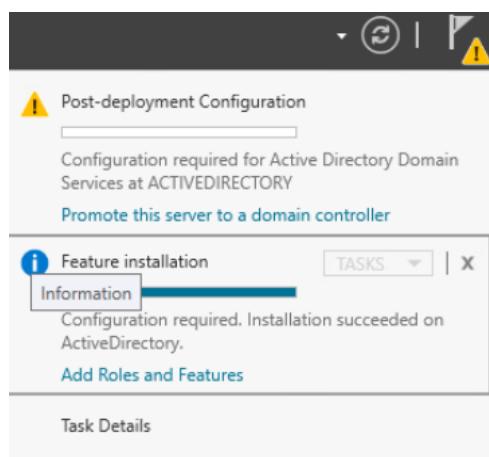
We zoeken in de lijst naar de rol die we deze server willen opleggen, in dit geval.

- Active Directory Domain Services

Add features. We moeten momenteel geen extra features installeren.

Opzetten van het domein

Na de installatie zou er een uitroepteken bij het vlagje bovenaan moeten staan. Klik op dit vlagje en vervolgens op ‘promote this server to a domain controller’



We willen een nieuwe forest creëren. Dit gaat ons domein worden ‘halflife.be’

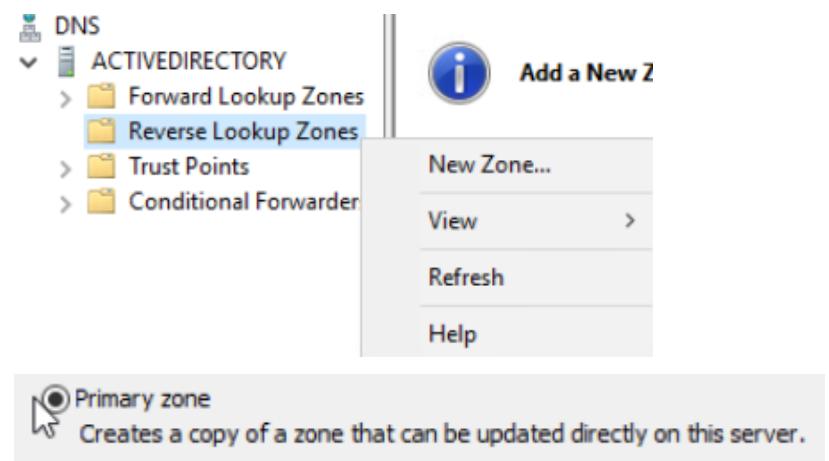
Select the deployment operation
<input type="radio"/> Add a domain controller to an existing domain
<input type="radio"/> Add a new domain to an existing forest
<input checked="" type="radio"/> Add a new forest
Specify the domain information for this operation
Root domain name: <input type="text" value="halflife.be"/>

Geef een 'Directory Services Restore Mode password' in voor deze server. Kies hiervoor een secure wachtwoord.

Het systeem zal nu een prerequisites check doen. We zien enkele warnings staan maar geen errors dus we lezen de warnings na en installeren het domein.

Reverse DNS Lookup zone

Vervolgens gaan we een reverse



next

To all DNS servers running on domain controllers in this domain: halflife.be

next

IPv4 Reverse Lookup Zone

next

We geven ons Netwerk id in, in ons geval is deze '192.168.1'.

To identify the reverse lookup zone, type the network ID or the name of the zone.

Network ID:

192 .168 .1| .

next

Uit veiligheid laten we enkel veilige dynamische updates toe in ons domein.

Allow only secure dynamic updates (recommended for Active Directory)

This option is available only for Active Directory-integrated zones.

next en vervolgens finish

We updaten het PTR-Record. Hiervoor gaan we naar Forward lookup zones en klikken we op 'domainname.be' wat in ons geval 'halflife.be' is.

Forward lookup zones => halflife.be => Active Directory (computername) A record =>

Update associated pointer (PTR) record

We herstarten het toestel en loggen in in het domein door in te loggen op HALFLIFE\Administrator.



DHCP server installeren

Manage => Add roles and features => next => **Role-based or feature-based installation** => next => **Select a server from the server pool**

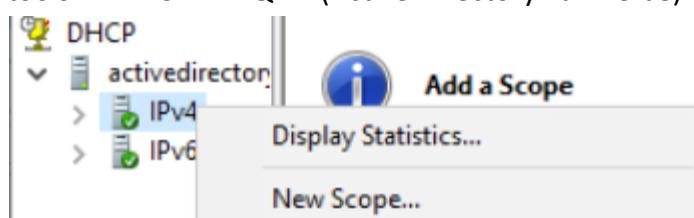
We duiden de server aan waarop we de service willen installeren.

=> next => **DHCP Server** => next => next => install

Na de installatie komt er een uitroep teken tevoorschijn bovenaan het vlagje. we klikken op het vlagje en klikken op ‘complete DHCP ‘configuration’ om de configuratie af te ronden. We laten de settings op default staan.

Voor de scope van onze DHCP in te stellen gaan we naar:

tools => DHCP => FQDN (Active Directory.halflife.be) => Ipv4 => New scope



=> next => Geef de scope een naam naar keuze => next =>
Geef de range in waaruit het DHCP adressen van mag uitdelen.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:	192 . 168 . 1 . 2
End IP address:	192 . 168 . 1 . 254

Configuration settings that propagate to DHCP Client

Length:	24
Subnet mask:	255 . 255 . 255 . 0

=> next

We krijgen de optie om ranges of enkele ip-adressen uit de scope te laten. Hier geef ik de ip-adressen in die al ingenomen zijn door servers om zo ip-conflicten te vermijden.

Start IP address:	End IP address:	Add
Excluded address range:		Remove
Address 192.168.1.10 Address 192.168.1.20 Address 192.168.1.30 Address 192.168.1.40 Address 192.168.1.50 Address 192.168.1.60		Subnet delay in milli second: 0

=> next => We laten de lease duration op default staan (8 dagen) => next =>

Yes, I want to configure these options now => next => We laten de router ip adres leeg => next => we geven aan dat we de DNS instellingen gebruiken van de parent domain.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:	halflife.be
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.	
Server name:	IP address:
	192.168.1.10
Resolve	Add Remove Up Down

=> next => next => Yes, I want to activate this scope now => next => finish

Nu zal elke Cliënt een ip-adres van de Active Directory moeten krijgen.

Users en Groepen registreren.

Server manager => tools => active directory users and computers

Onder de map 'halflife.be' gaan we naar users. we klikken op de map met onze rechtermuisknop en klikken op new => user

First name:	jeff	Initials:	
Last name:			
Full name:	jeff		
User logon name:	jeff	@halflife.be	▼
User logon name (pre-Windows 2000):	HALFLIFE	jeff	

=> next

We geven een tijdelijk wachtwoord in die naderhand aangepast moet worden door de user.

Password:	*****
Confirm password:	*****
<input checked="" type="checkbox"/> User must change password at next logon <input type="checkbox"/> User cannot change password <input type="checkbox"/> Password never expires <input type="checkbox"/> Account is disabled	

=> next => finish

Voor groepen aan te maken klikken we op het volgende icoontje in de toolbalk bovenaan.



We geven de naam in van de groep en laten de opties op default opties staan.

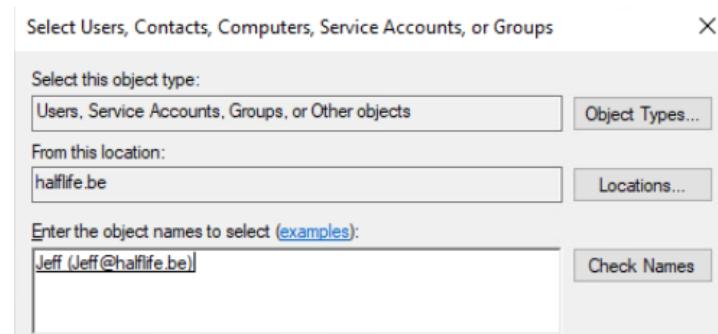
Group name:	boekhouding
Group name (pre-Windows 2000):	boekhouding
Group scope	<input type="radio"/> Domain local <input checked="" type="radio"/> Global <input type="radio"/> Universal
Group type	<input checked="" type="radio"/> Security <input type="radio"/> Distribution

=> ok

Nu zou de groep in de lijst moeten staan met de users. We klikken op de reeds aangemaakte groep om leden toe te kennen.

We gaan naar de sectie 'members' bovenaan en klikken op 'Add'.

Typ de naam van de gewenste user in en klik vervolgens op ‘check names’



=> ok

We doen hetzelfde voor de andere 2 groepen die we nodig hebben voor gerichte filesharing. Namelijk IT en directie.

Via een batch file de leden een schnellere weg geven naar hun fileshares.

Eerst maken we een batchfile. We openen een kladblad en typen het volgende commando in: net use x: \\192.168.1.30\boekhouding

We verwijzen hiermee naar het ip-adres van onze fileservice en de naam van de share.

Vervolgens slaan we dit op als een .bat file en slaan het voorlopig op op het bureaublad. We kunnen deze batch bij elk lid van de groep individueel instellen maar dat zou enorm tijds inefficiënt zijn. Daarom gaan we een group policy maken wat automatisch de file uitvoert bij elk lid van de groep.

We gaan naar windows server => tools => Group Policy Management

We klikken met de rechtermuisknop op de map ‘halfife.be’ en klikken op:

Create a GPO in this domain, and Link it here...

Geef de naam van de group policy in => ok

De GPO is aangemaakt. We moeten deze enkel nog editeren en de betrokken partijen aanduiden.

rechtermuisknop op de GPO => Edit

User configuration => policies => scripts => logon

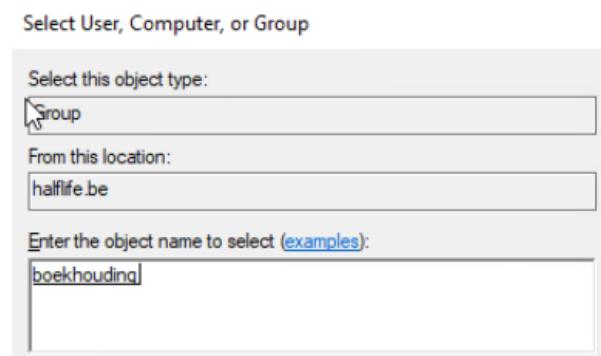
We komen uit op de properties. We klikken op ‘add’ voor een script toe te voegen aan deze GPO. We klikken op ‘browse’.

Nu zijn we uitgekomen in een lege map. We knippen en plakken de batchfile van het bureaublad naar uitdrukkelijk deze map. Een andere locatie voor de batch file gaat niet werken.

We klikken op 'ok'.

Nu rest ons nog enkel de betrokken partijen toe te voegen aan deze GPO.

We gaan naar onze reeds aangemaakte GPO en zien aan de rechterkant de sectie 'security filtering' verschijnen. Klik op 'add'.

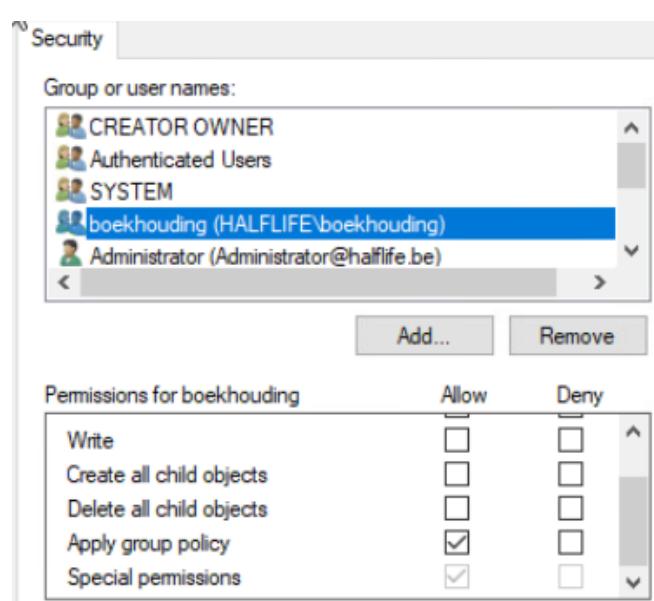


We geven hier de gewenste groep in.

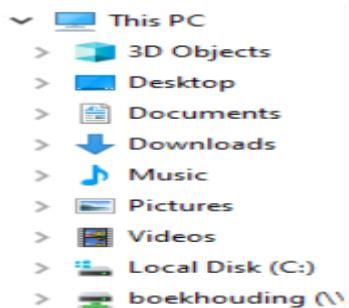
=> We gaan naar delegation



Klik enkel 1 keer op de groep 'boekhouding' en klik op 'advanced'. Hier kunnen we de rechten van de groep aanpassen op deze GPO. We vinken de volgende permissie aan.



Om te testen of dit gelukt is gaan we naar een account van een user die lid is van de groep 'boekhouding'



We zien onder 'This pc' de share 'boekhouding' staan. Dit wil zeggen dat de batch file succesvol is uitgevoerd. Indien dit niet het geval is kun je je begeven naar de cmd en het commando 'gpupdate /force' in te geven om handmatig de nieuwe configuraties door te voeren.

Mailserver

Wat is een mailserver?

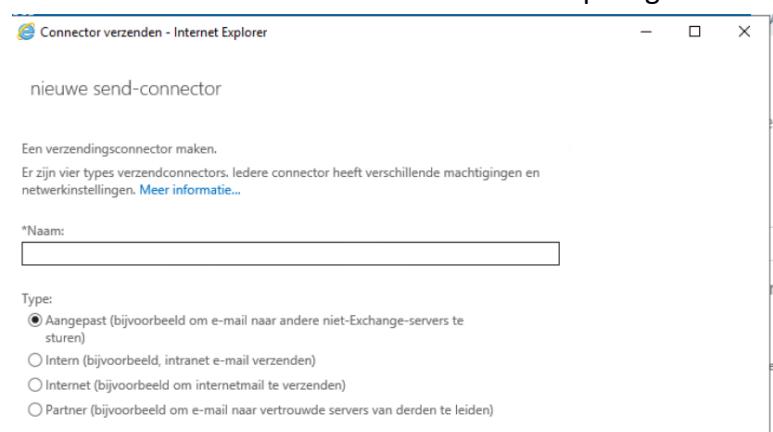
Een mailserver is een server die verantwoordelijk is voor het verwerken van e-mail. Een mailserver verzendt en ontvangt mails van andere mailservers

Waarom Microsoft Exchange?

Wij hebben gekozen voor Exchange omdat dit behalve een mailserver ook nog kan gebruikt worden om een agenda mee te beheren en om dat er ook een web applicatie voor is.

Send Connector

Open je exchange administration center en log je in. hierin gaan we een smart host aanmaken om emails te kunnen versturen. hiervoor gaan we naar de e-mailstroom tab, en in die tab klikken we op connectors verzenden en klikken op het plusje. we vullen hier een naam in en kiezen voor internet en klikken op volgende.



Vervolgens kiezen we voor e-mail routeren via smart host en maken er één aan. bij de smarthost vul je de FQDN (fully qualified domain name) bij ons is dit 'mail1.fluviusnet.be'. bij de volgende pagina kiezen we voor geen verificatie bij nieuwe connectors maak je een nieuwe aan en kies je voor smtp en bij de FQDN vul je een * in. vervolgens kies je voor de server die je gaat gebruiken als exchange server en klik je op voltooien.

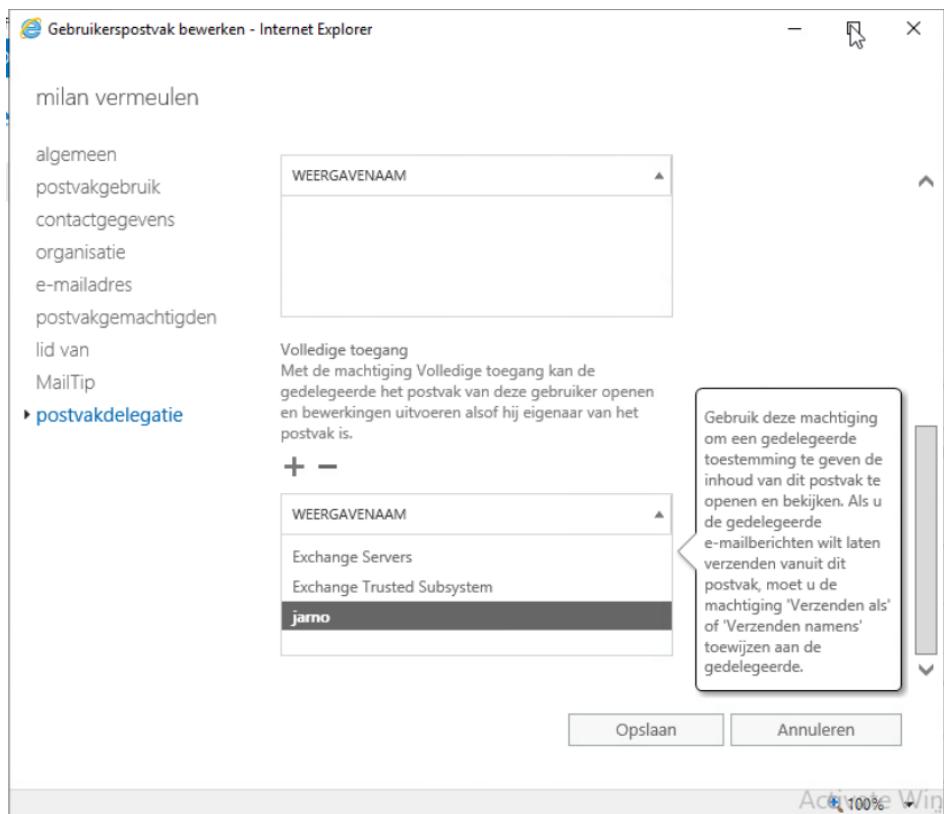
Gebruikers aanmaken

Bij geadresseerden bij postvakken op en het plusje klikken en kiezen voor gebruikers postvak hier kan je kiezen om een bestaande user te gebruiken en dan gaat de exchange kijken naar de gebruikers op de active directory of we kunnen een nieuwe maken. Moesten we kiezen voor een nieuwe gebruiker dan wordt deze ook automatisch aangemaakt op de active directory.



Postvak beheer

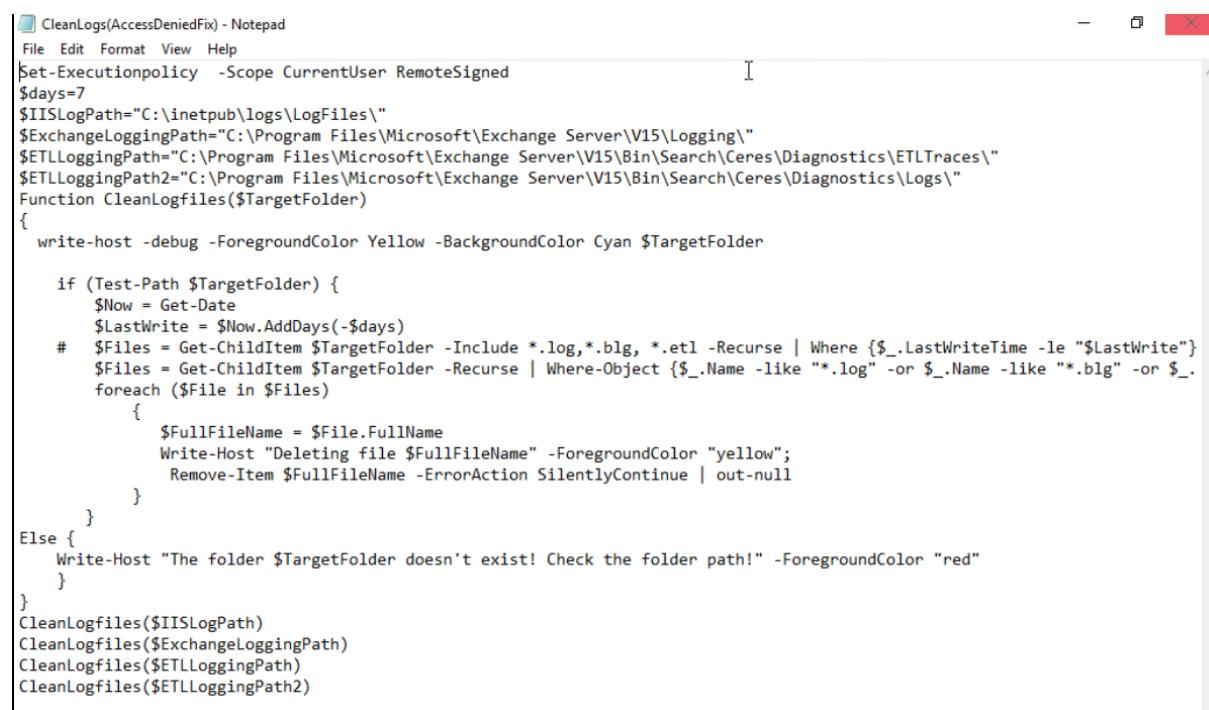
In Exchange kan je ook andere mensen toegang verlenen tot je mailbox of agenda dit is heel handig als je bijvoorbeeld een secretaresse zou hebben. Moest je druk bezig zijn kan je vragen of je secretaresse of medewerker om voor jouw je email te beantwoorden of iets in je agenda te zetten. Dit doe je door te dubbelklikken op de gebruiken en bij postvak delegatie.



Hierboven heb ik de gebruiker Jarno volledige toegang tot het postvak van Milan dit betekent dat hij mijn postvak volledig beheren alsof hij de gebruiker Milan zou zijn.

Exchange log files cleanup

Exchange 2016 heeft een gekend probleem dat deze heel veel logs bewaard en deze worden niet standaard gewist waardoor je hardeschijf heel snel vol raakt om dit te voorkomen heb ik een task gemaakt dat iedere zondag een script start of deze log files te wissen. Dit script is heb ik gehaald van technet.microsoft.com en heb ik aangepast zodat op onze server zou werken.



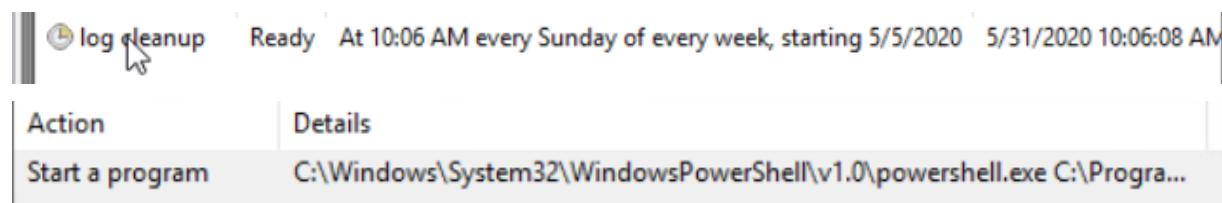
```

CleanLogs(AccessDeniedFix) - Notepad
File Edit Format View Help
$Set-ExecutionPolicy -Scope CurrentUser RemoteSigned
$days=7
$IISLogPath="C:\inetpub\logs\LogFiles\" 
$ExchangeLoggingPath="C:\Program Files\Microsoft\Exchange Server\V15\Logging\" 
$ETLLoggingPath="C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\Diagnostics\ETLTraces\" 
$ETLLoggingPath2="C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\Diagnostics\Logs\" 
Function CleanLogfiles($targetFolder)
{
    write-host -debug -ForegroundColor Yellow -BackgroundColor Cyan $targetFolder

    if (Test-Path $targetFolder) {
        $Now = Get-Date
        $LastWrite = $Now.AddDays(-$days)
        # $Files = Get-ChildItem $targetFolder -Include *.log,*.blg, *.etl -Recurse | Where {$_.LastWriteTime -le "$LastWrite"}
        $Files = Get-ChildItem $targetFolder -Recurse | Where-Object {$_.Name -like "*.log" -or $_.Name -like "*.blg" -or $_.Name -like "*.etl"} 
        foreach ($File in $Files)
        {
            $FullName = $File.FullName
            Write-Host "Deleting file $FullName" -ForegroundColor "yellow";
            Remove-Item $FullName -ErrorAction SilentlyContinue | Out-Null
        }
    }
    Else {
        Write-Host "The folder $targetFolder doesn't exist! Check the folder path!" -ForegroundColor "red"
    }
}
CleanLogfiles($IISLogPath)
CleanLogfiles($ExchangeLoggingPath)
CleanLogfiles($ETLLoggingPath)
CleanLogfiles($ETLLoggingPath2)

```

In mij task scheduler op mij Exchange server dat iedere zondag met powershell dit script start.



PST files exporteren

Eerst loggen we als administrator in op het Exchange administration center (EAC). Hierna klikken we rechts op machtigingen en kiezen we voor beheerrollen.
Onder beheerrollen dubbelklikken we op Recipient management.

geadresseerden

machtigingen

compliancebeheer

organisatie

beveiliging

e-mailstroom

mobiel

openbare mappen

servers

beheerrollen

- [+](#)
 - [edit](#)
 - [delete](#)
 - [list](#)
 - [search](#)
 - [refresh](#)
-
- NAAM
- Compliance Management
- Delegated Setup
- Discovery Management
- Help Desk
- Hygiene Management
- Organization Management
- Public Folder Management
- Recipient Management**
- Records Management

Recipient Management

*Naam:

Recipient Management

Beschrijving:

Leden van deze beheerrollengroep hebben machtigingen om Exchange-ontvangerobjecten aan te maken, te beheren en te verwijderen in de Exchange-organisatie.

Schrijfbereik:

Standaard

Organisatie-eenheid:

In het menu van Recipient management moeten we een rol toevoegen genaamd “Mailbox Import Export” dit doen we door op het plusje te klikken en dan de rol te selecteren en op apply te klikken.

toevoegen ->

Mailbox Import Export [verwijderen]:

Als gebeurt is heb mag je de EAC afsluiten en dan je Exchange Management Shell open doen. In de Management shell gaan we een regel aanmaken dat administrators content uit mailboxen kunnen importeren en exporteren. Dit gebeurt met het commando New-ManagementRoleAssignment -Role “Mailbox Import Export” -user Administrator

```
[PS] C:\Windows\system32>New-ManagementRoleAssignment -Role "Mailbox Import Export" -User Administrator
Name          Role      RoleAssigneeName  RoleAssigneeType AssignmentMethod EffectiveUserName
---          ---      ---              ---           ---           ---
Mailbox Import Export-Admin... Mailbox Import... Administrator        User             Direct
```

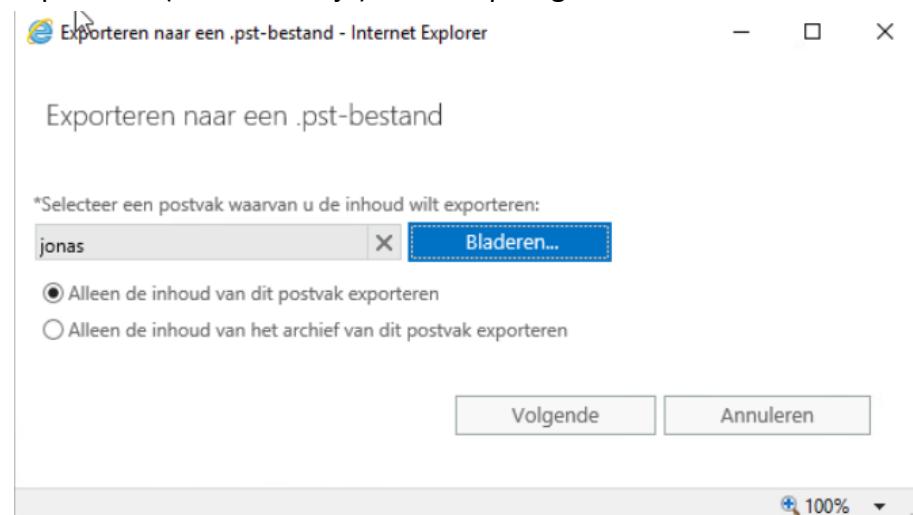
als dit gebeurt is mag je shell terug afsluiten terug naar je EAC gaan.

Links in het tabblad geadresseerden bij postvakken klik je op het postvak waarvan je een PST-bestand van wil maken en dan klikken we op de 3 bolletje voor meer opties.

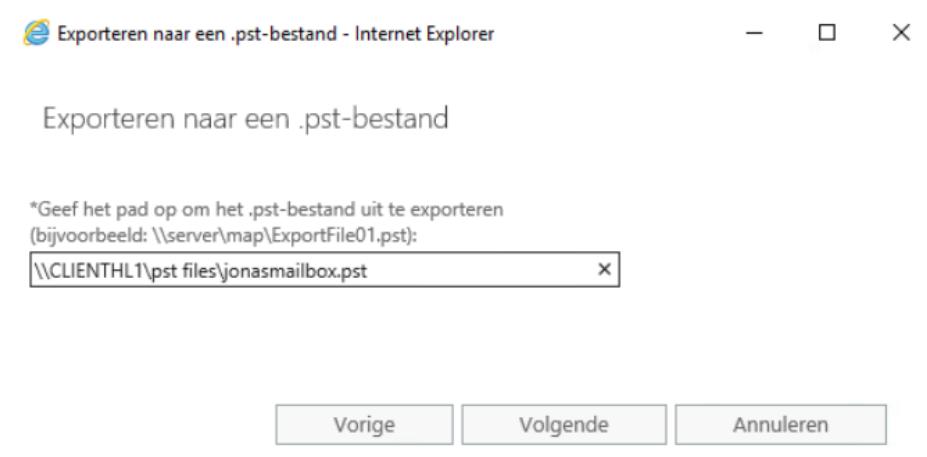
Eens je hierop hebt geklikt heb je nu een optie “exporteren naar een PST-bestand” klik daarop en hierna gaat er een wizard open om je PST-bestand te maken.

Op de eerste pagina van de wizard moet je de mailbox waarvan je de inhoud wilt exporteren aanduiden en in ons geval aanduiden dat we alleen de inhoud van het postvak willen

exporteren (eerste bolletje) en dan op volgende klikken.



Op de volgende pagina moeten we specificeren waar naartoe we dit bestand willen exporteren. (\\\CLIENTHL1\pst files\jonasmailbox.pst)



Vervolgens kunnen we kiezen of een email moet verzonden worden als het bestand geëxporteerd werd en specificeren naar welk postvak deze email moet verzonden worden.

Fileserver

Netwerk configureren.

Na de clean install van freeNAS krijgen we een beeld met een aantal opties. Voor het correct configureren van het netwerk kiezen we eerst voor optie 1:

1) Configure Network Interfaces

Kies de interface waarmee de server verbonden wordt met het LAN-netwerk. In ons geval is het het default interface ‘vmx0’

Configure interface for DHCP? (y/n)

We kiezen voor nee, Omdat een server een statisch ip-adres moet hebben om functioneel te zijn

Configure IPv4? (y/n)

Ja, hier stellen we het ip adres in wat we hebben gereserveerd voor deze server. In ons geval 192.168.1.30.

Configure IPv6? (y/n)

Nee, wij werken met IPv4 adressen.

We begeven ons naar de cliënt en loggen in op het ‘root’ account in de freeNAS gui. We begeven ons naar het adres '<https://192.168.1.30>'

Zodra we ingelogd zijn, begeven we ons naar de optie network -> global configuration.

Hier moeten we nog onze Default Gateway ingeven. In ons geval ‘192.168.1.1’

We passen ook de naam aan naar ‘nas’.

Verbinding maken met de Active Directory

Voor we starten moeten we toeziendat de ntp server van onze Active Directory de tijdsinstellingen van de freeNAS synchroniseert. We begeven ons via onze freeNAS gui naar: System -> NTP servers.

We geven het domeinnaam van de dc in voor het adres.

Address	activedirectory.halflife.be
---------	-----------------------------

De rest laten we op default staan. Zie ook toe dat Deze NTP server bovenaan staan zodat deze prioriteit krijgt.

Vervolgens gaan we verbinding maken met het domein. We begeven ons naar Directory services -> Active Directory.

Hier geven we de naam in van het domein dat we willen joinen. met de inloggegevens van de administrator. Vergeet het lege vakje ook niet aan te vinken.

<input checked="" type="checkbox"/>	Enable (requires password or Kerberos principal)	
-------------------------------------	--	---

Als de settings succesvol opgeslagen zijn, zit je in het domein. Om dit te kunnen dubbelchecken kunnen we ons naar de shell begeven en het volgende commando intypen: 'wbinfo -u'. We krijgen de users van de freeNAS te zien. Als freeNAS succesvol aan het domein is gekoppeld staan de users van het domein hier ook bij.

```
HALFLIFE\sm_66b30f3fdb9a4034b
HALFLIFE\sm_b00a4e16835444a08
HALFLIFE\sm_a6cda7dadf9a493bb
HALFLIFE\healthmailbox1d1e023
HALFLIFE\healthmailbox1584701
HALFLIFE\healthmailbox71e1e74
HALFLIFE\healthmailboxd4fb41b
HALFLIFE\healthmailbox437e3bc
HALFLIFE\healthmailboxab411e8
HALFLIFE\healthmailbox3471ef4
HALFLIFE\healthmailbox091f77a
HALFLIFE\healthmailbox8a67984
HALFLIFE\healthmailbox4dd4fc6
HALFLIFE\healthmailbox16calc9
HALFLIFE\milan
HALFLIFE\jonas
HALFLIFE\jarno
HALFLIFE\jaime
HALFLIFE\backup
root@nas[~]#
```

Output:

Aanmaken van resource pools

Voor onze datastore aan te maken begeven we ons naar storage -> pools en klikken we op 'add' rechts bovenaan.

We kiezen voor een nieuwe pool.



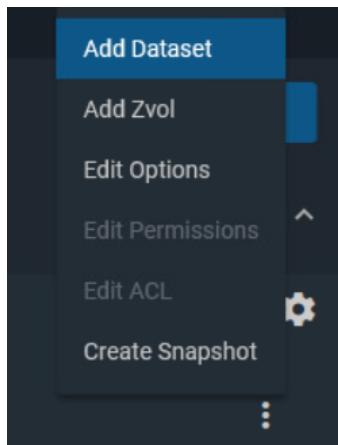
Hier moeten we de pool een naam geven en een harde schijf toekennen aan deze pool in ons geval hebben we de pool 'ourpool' genoemd. Daarna klikken we op 'create pool'.

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
> Ourpool	dataset	8.49 MiB	5.32 GiB	lz4	14.36x	false	off	

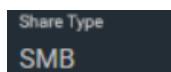
Nu moeten we de pool verdelen in verschillende datasets. Verschillende databases hebben verschillende rechten waardoor een onderdeling cruciaal is.

We kiezen voor: Home, Backup, Public en Groups.

We klikken op de 3 puntjes rechts van pool en klikken op 'Add dataset'



We moeten onze dataset hier vernoemen. De opties moeten op default blijven buiten de share type. Die moeten we op SMB zetten (Windows shares).



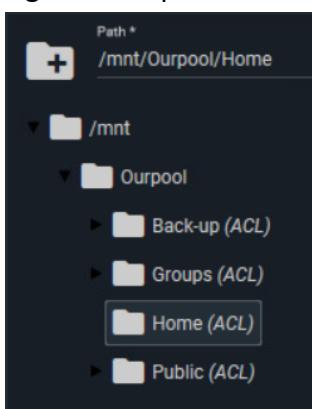
Dit doen we voor al onze benodigde datasets.

Rechten toekennen

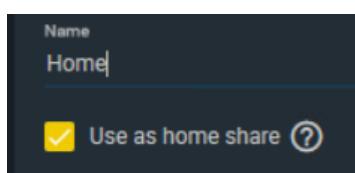
Om rechten toe te kennen aan de datasets moeten ons begeven naar sharing -> Windows shares. Hier moeten we de rechten aanmaken en aanduiden voor welke datasets deze rechten gelden. We beginnen met de home folder.

Home folder

We geven het pad in naar de dataset die we gereserveerd hebben voor de home shares.



Omdat dit de home folder gaat zijn moeten we de optie 'use as home share' aanvinken



De rest laten we op default staan.

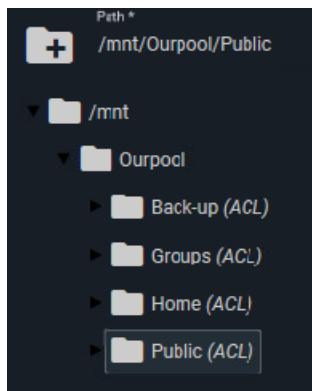
Vervolgens klikken we op de 3 puntjes rechts van de share en klikken we op 'edit ACL' voor de rechten in te stellen. De rechten van een homefolder moeten er als volgt uitzien.

File Information <hr/> Path /mnt/Ourpool/Home/HALFLIFE	Who * owner@ <hr/> ACL Type * Allow <hr/> Permissions Type * Basic <hr/> Permissions * Full Control <hr/> Flags Type * Basic <hr/> Flags * Inherit
--	--

Door deze rechten toe te kennen zorg je ervoor dat zowel de administrator als de domein users volledige controle hebben op hun home share.

Public folder

We geven het pad in voor de public folder.



De rest van de opties laten we staan op default.

Vervolgens klikken we op de 3 puntjes rechts van de share en klikken we op 'edit ACL' voor de rechten in te stellen. De rechten van een public folder moet er als volgt uitzien.

Path <code>/mnt/Ourpool/Public</code>	Who * <code>owner@</code>	Who * <code>group@</code>
User <code>HALFLIFE\administrator</code>	ACL Type * <code>Allow</code>	ACL Type * <code>Allow</code>
Group <code>HALFLIFE\domain users</code>	Permissions Type * <code>Basic</code>	Permissions Type * <code>Basic</code>
	Permissions * <code>Full Control</code>	Permissions * <code>Full Control</code>
	Flags Type * <code>Basic</code>	Flags Type * <code>Basic</code>
	Flags * <code>Inherit</code>	Flags * <code>Inherit</code>

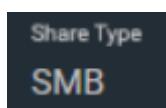
door het toekennen van deze rechten geef je de administrator en de domein users volledige controle over de public folder.

Group folders

Er zijn 3 verschillende groepen aangemaakt in de Active Directory. Namelijk: Directie, IT en boekhouding. Deze groepen moeten individueel een eigen map hebben waar ze werkgerelateerde files kunnen delen. We moeten datasets toevoegen onder de dataset 'groups' om deze rechten toe te kennen.

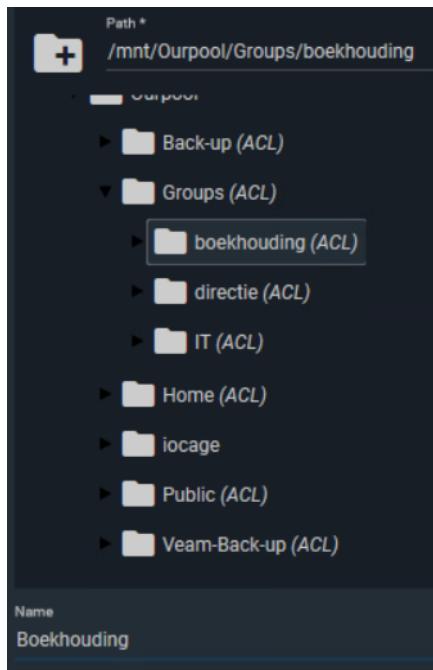
We gaan naar de opties van de datapool groups en klikken op 'add dataset'.

Geef de naam in van de dataset en verander de sharing type naar SMB. De rest blijft op default.



Dit doen we voor alle groepen.

Dan gaan we weer over naar sharing -> windows shares en voegen we een share toe op de gereserveerde datasets.



We laten shadow copies aanstaan.
Dit doen we ook met de andere 2 groepen.

Vervolgens klikken we op de 3 puntjes rechts van de share en klikken we op 'edit ACL' voor de rechten in te stellen. De rechten van een group folder moet er als volgt uitzien.

<p>Path <i>/mnt/Ourpool/Groups/boekhouding</i></p> <hr/> <p>User <i>HALFLIFE\administrator</i></p> <hr/> <p>Group <i>HALFLIFE\boekhouding</i></p> <hr/> <p>Default ACL Options</p>	<p>Who * <i>owner@</i></p> <hr/> <p>ACL Type * <i>Allow</i></p> <hr/> <p>Permissions Type * <i>Basic</i></p> <hr/> <p>Permissions * <i>Full Control</i></p> <hr/> <p>Flags Type * <i>Basic</i></p> <hr/> <p>Flags * <i>Inherit</i></p>	<p>Who * <i>group@</i></p> <hr/> <p>ACL Type * <i>Allow</i></p> <hr/> <p>Permissions Type * <i>Basic</i></p> <hr/> <p>Permissions * <i>Full Control</i></p> <hr/> <p>Flags Type * <i>Basic</i></p> <hr/> <p>Flags * <i>Inherit</i></p>
---	--	--

Door het toekennen van deze rechten zorg je ervoor dat zowel de administrator als de leden van de groep 'boekhouding' toegang hebben tot de mappen.

Back-up Server

Wat is een backup?

Een back-up is een kopie van gegevens dat je opslaat op een externe opslagplaats voor eventuele recovery van deze bestanden. Dit kan gebeuren als de schijf kapot gaat, diefstal, natuurverschijnselen (brand, overstroming, ...), verwijdering van bestanden door de gebruiker of ransomware zoals een cryptolocker. Bij het opzetten van een back-up strategie moet je al deze mogelijke opties overwegen. Het is zeker verstandig om meerdere back-ups te bewaren over een langere periode.

Waarom Veeam?

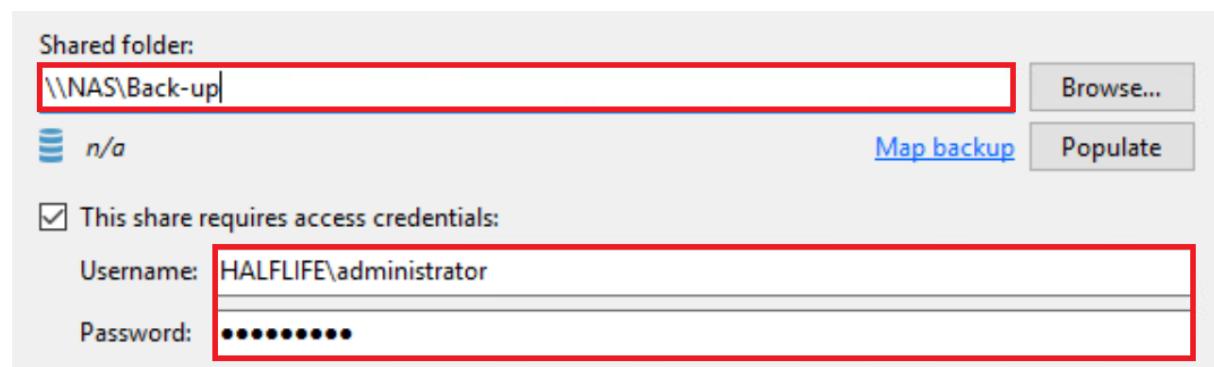
Dit is gratis te gebruiken software waarmee je 1 back-up ‘job’ mee kunt opstellen per apparaat. Je kunt hiermee gemakkelijk verschillende back-up methodes instellen, volledig, incrementeel of progressief.

Back-up job

Na Veeam agent te installeren op de server starten we een nieuwe back-up job.



Voor onze setup kiezen we een volledige backup die wordt weggeschreven naar onze fileserver netwerk share genaamd ‘back-up’.



We kiezen ervoor om deze back-ups voor 7 dagen te bewaren. Zondagnacht zal de job starten en de server volledig back-uppen en de server zal blijven runnen.

E-mail notificaties

Veeam biedt de optie om een automatische e-mail te verzenden wanneer de job voltooid is naar een mailadres naar keuze.

We stellen in om een mail te verzenden naar het account backup@halflife.be. Wanneer de job klaar is zal deze een mail sturen met de volgende informatie:

- Success of failure
- Warning als er te weinig opslagruimte is of begint te zijn
- Server
- Job
- Hoe lang het proces duurde

Email settings:

backup@halflife.be

[%JobResult%] %ComputerName% - %JobName% - %CompletionTi



Notify on:

Success Warning Error

[Show SMTP server settings](#)

[Test Message](#)

Click to test the specified SMTP server settings

Settings van de verzending:

SMTP server settings:

mail.halflife.be

587

backup

Use secure connection (SSL/TLS)

Monitoring

Nagios core

We hebben besloten om nagios te installeren op een ubuntu server 18.04 LTS, omdat het open source is, en is gemakkelijk te gebruiken eens deze is opgezet. Deze linux server staat in ons intern netwerk en heeft het ipv4 adres : **192.168.1.50** en hostname : **nagios.halflife.be** we hebben voor deze setup de installatiestappen van de nagios support pagina gebruikt, we zullen deze stappen hier even herhalen.

Eerst voeren we systeem updates uit:

```
>sudo apt update  
>sudo apt upgrade -y
```

Nu moeten we bepaalde pakketjes binnen halen op de service op te zetten:

```
>sudo apt install -y autoconf gcc libc6 make wget unzip apache2 php  
libapache2-mod-php7.2 libgd-dev
```

We nigeren naar /tmp om daar onze download op te slaan.

```
>cd /tmp
```

Het downloaden van de data:

```
>wget -O nagioscore.tar.gz  
https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.5.tar.gz
```

Het uitpakken van de data:

```
>tar xzf nagioscore.tar.gz  
>cd /tmp/nagioscore-nagios-4.4.5/
```

De data uitvoeren:

```
>sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled  
>sudo make all
```

Aanmaken van gebruiker en groep:

```
>sudo make install-groups-users  
>sudo usermod -a -G nagios www-data
```

Installeren van de benodigdheden:

```
>sudo make install  
>sudo make install-daemoninit  
>sudo make install-commandmode  
>sudo make install-config
```

Het installeren van de web server:

```
>sudo make install-webconf  
>sudo a2enmod rewrite  
>sudo a2enmod cgi
```

De firewall open zetten voor poort 80:

```
>sudo ufw allow Apache  
>sudo ufw reload
```

Het creëren van het web admin account en een paswoord:

```
>sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Herstarten van de webserver:

```
>sudo systemctl restart apache2.service
```

Nagios starten:

```
>sudo systemctl start nagios.service
```

Nu hebben we de nagios service running en kunnen we inloggen op de webinterface van nagios door <http://192.168.1.50/nagios> hier log je dan in met de user "nagiosadmin" en jezelf gekozen paswoord. Momenteel kan je nog geen trafic zien met nagios, We moeten nog eerst hosts toevoegen, en config files aanpassen. volg onderstaande stappen.

Hosts toevoegen

We nigeren naar onderstaande locatie:

```
>cd /usr/local/nagios/etc/objects
```

Hier maken we een nieuwe map aan, nu genaamd "intern"

```
>sudo mkdir intern
```

We openen even de main config file van nagios om te tonen in welke map we onze host configuratie bestand gaan zetten:

```
>sudo nano /usr/local/nagios/etc/nagios.cfg
```

en we voegen onderstaande wijziging toe aan het nagios.cfg bestand

```
#monitoring voor intern netwerk  
cfg_dir=/usr/local/nagios/etc/objects/intern
```

we gaan nu naar onze aangemaakte map "intern":

```
>cd /usr/local/nagios/etc/objects/intern
```

Hier maken we onze host file aan "hosts.cfg":

```
>sudo nano hosts.cfg
```

In deze file hebben we voor elke server een nieuwe host gedefinieerd. zoals op onderstaande foto

```
define host{  
    use                  intern-hosts  
    host_name            activedirectory.halflife.be  
    alias                Active-Directory  
    address              192.168.1.10  
}
```

'use' : geeft de map weer voor de host templates.

'host_name' : geef de hostname van de server op.

'alias' : geef een gekozen naam voor de server.

'address' : geef het ipv4 adres van de server op.

Nu gaan we een settings file maken voor de hosts die we gedefinieerd hebben.

```
>sudo nano /usr/local/nagios/etc/objects/intern/hosts-service-template.cfg
```

de onderstaande settings zijn voor alle aangemaakte hosts

```
#Host template definition
define host{
    name                           intern-hosts
    check_command                  check-host-alive
    check_interval                 5
    max_check_attempts             2
}
```

we zullen even de settings overlopen:

check_command : host-alive : we kijken hier of al de hosts online zijn.

check_interval: 5, nagios gaat om de 5 minuten checken of de hosts online zijn

max check attempts : nagios gaat maximum nog 2 keer proberen een connectie te zoeken als het geen OK state terug krijgt.

Nu moeten we nog de plugins installeren op de server

>sudo apt install nagios-plugins

>sudo systemctl restart nagios

>sudo cp /usr/lib/nagios/plugins/check_* /usr/local/nagios/libexec/

De nagios server is klaar voor gebruik en nu kan je van elk toestel in het netwerk kijken of dat de servers online zijn.

Sharepoint

Wat is Sharepoint?

Sharepoint is een web based Content Management System (CMS), Dit is een vorm van software die het makkelijk maakt om documenten te delen over het internet.

Wij hebben gekozen voor sharepoint omdat we met 2 kantoren zitten die soms ook samen moeten kunnen werken en met onze teamsite kunnen we makkelijk samen aan bepaalde documenten werken en hebben we ook altijd toegang tot onze documenten op één centrale plaats.

Sharepoint configuratie

Wij hebben onze Sharepoint server op een Microsoft server 2019 geïnstalleerd op deze server draait ook SQL server 2017 omdat sharepoint ook een database nodig heeft.

In de installatie image van Sharepoint zit een Microsoft SharePoint Products and Technologies Preparation Tool die voor ons alle requirements gaat installeren voor ons. deze gaat een paar service configureren en updates doen zodat onze Microsoft server klaar is voor de sharepoint. Dit zijn de services en updates.

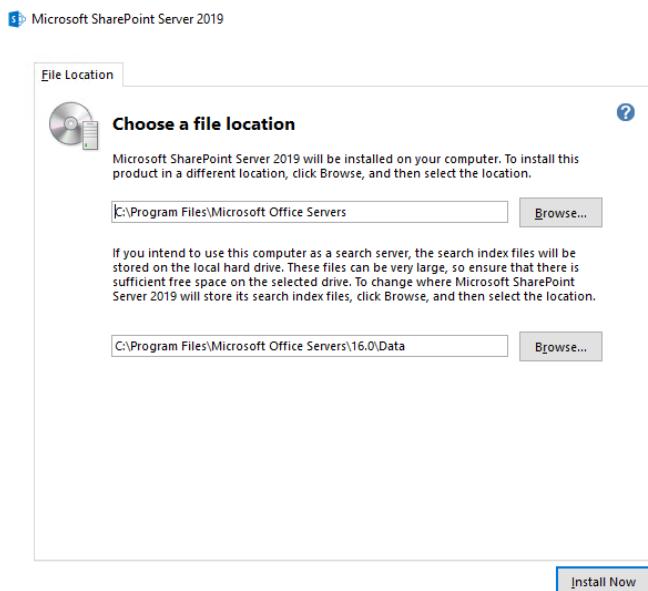
- Web Server (IIS) role

- Windows Process Activation Service feature
- Microsoft .NET Framework version 3.5
- Microsoft .NET Framework version 4.7.2
- Microsoft SQL Server 2012 Service Pack 4 Native Client
- Microsoft WCF Data Services 5.6
- Microsoft Identity Extensions
- Microsoft Information Protection and Control Client 2.1 (MSIPC)
- Microsoft Sync Framework Runtime v1.0 SP1 (x64)
- Windows Server AppFabric 1.1
- Cumulative Update Package 7 for Microsoft AppFabric 1.1 for Windows Server (KB 3092423)
- Visual C++ Redistributable Package for Visual Studio 2012
- Visual C++ Redistributable Package for Visual Studio 2017

Als dit gebeurt is herstart je je server en start je de setup van de Sharepoint server. Je kiest voor install en hierna geef je je product key in. Moest je nog geen key, op de microsoft website kan je een trial key verkrijgen via

<https://www.microsoft.com/en-us/download/details.aspx?id=57462> hier kan je standaard of enterprise key verkrijgen. Lees en accepteer de voorwaarden.

Vervolgens kies je waar je deze wilt opslaan. Klik op install now en dan wachten tot het klaar is en close.



Als de installatie gedaan is open je de SharePoint Products Configuration Wizard, nu gaan we de configuratie beginnen. Hierin gaan we de Sharepoint server met de SQL server verbinden en zeggen in welke database deze moet worden opgeslagen. omdat wij nog geen database

hebben aangemaakt gaan de configuration wizard dit voor ons doen. hier moeten we ook zeggen met welk account de sharepoint kan verbinden met de SQL server. Hier kiezen we voor create a new server farm en dan op next. op de volgende pagina moet je je database server en database name in geven als je nog geen database hebt gaat die hier ook één voor u aanmaken. onze database server is SHAREPOINT\SHAREPOINTSQL, en de database naam is SharePoint_config_sharepoint. en geven we ook de naam van de gebruiker die onze databases gaan beheren in ons geval is dit Halflife\administrator. Vervolgens vragen ze om een passphrase te kiezen om je database configuraties te beveiligen. nu kies je welke rol je deze wil geven wij kiezen voor de single server farm omdat dit onze enigste sharepoint server is in ons netwerk. op de volgende pagina kies je via welke poort je naar de central administration webpage je wil gaan en hoe je op deze wil inloggen. wij kiezen voor NTLM hierdoor kunnen mensen die in onze database kunnen en die in ons domein zitten inloggen op onze Sharepoint. Op de volgende pagina zie je al je gekozen configuraties kijk even na of dit allemaal klopt en klik dan op next dan gaat die alles configureren. Als dit gebeurt klik op finish en dan gaat de central administration web page open. Voor een teamsite te maken zoals wij gebruiken ga je naar application management → manage web applications linksboven klik je op new, er gaat een venster open gaan hier kies je via welke poort je de website wil gaan bezoeken we laten dit even op 80 staan later veranderen we dit omdat we deze site https gaan maken hiervoor gaan we zometeen op de IIS een self signed certificate maken. We kiezen yes bij use SSL en we veranderen de naam van de database die wordt aangemaakt voor onze site anders wordt het onoverzichtelijk als we later meer websites zouden maken op deze sharepoint. De rest laten we staan zoals het staat.

Use an existing IIS web site
 Create a new IIS web site

Name: SharePoint - 80

Port: 80

Host Header:

Path: C:\inetpub\wwwroot\wss\VirtualDirector

Allow Anonymous

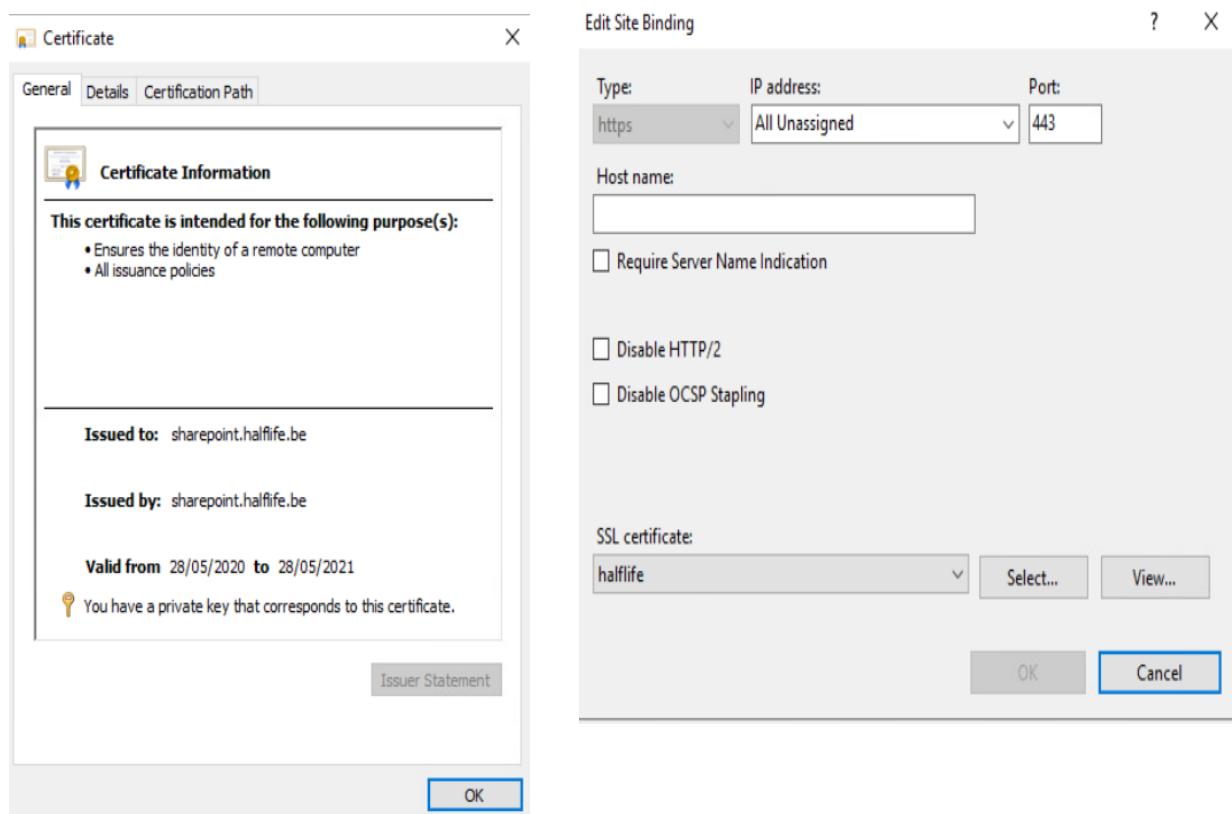
- Yes
 No

Use Secure Sockets Layer (SSL)

- Yes

vervolgens kies je de naam van de site bij ons is dit 'halflife' voor de template kiezen we voor teamsite en de URL is <http://sharepoint/sites/halflife>. Maar http is niet veilig dus we gaan deze https maken. Hiervoor moeten we een certificaat hebben dit gaan we maken op de IIS.

Op de server manager ga je naar Manage → Internet Information Service links klik je op onze server genaamd Sharepoint en vervolgens op server certificates → new self signed certificate. Nu klikken we onze Sharepoint 80 website open en klikken recht op bindings → add.



Ten laatste gaan we terug naar de Manage web applications pagina op de Sharepoint → configure alternate access mappings → edit public URL → selecteer je webapplicatie

Alternate Access Mapping Collection: [SharePoint - 80](#) ▾

Default

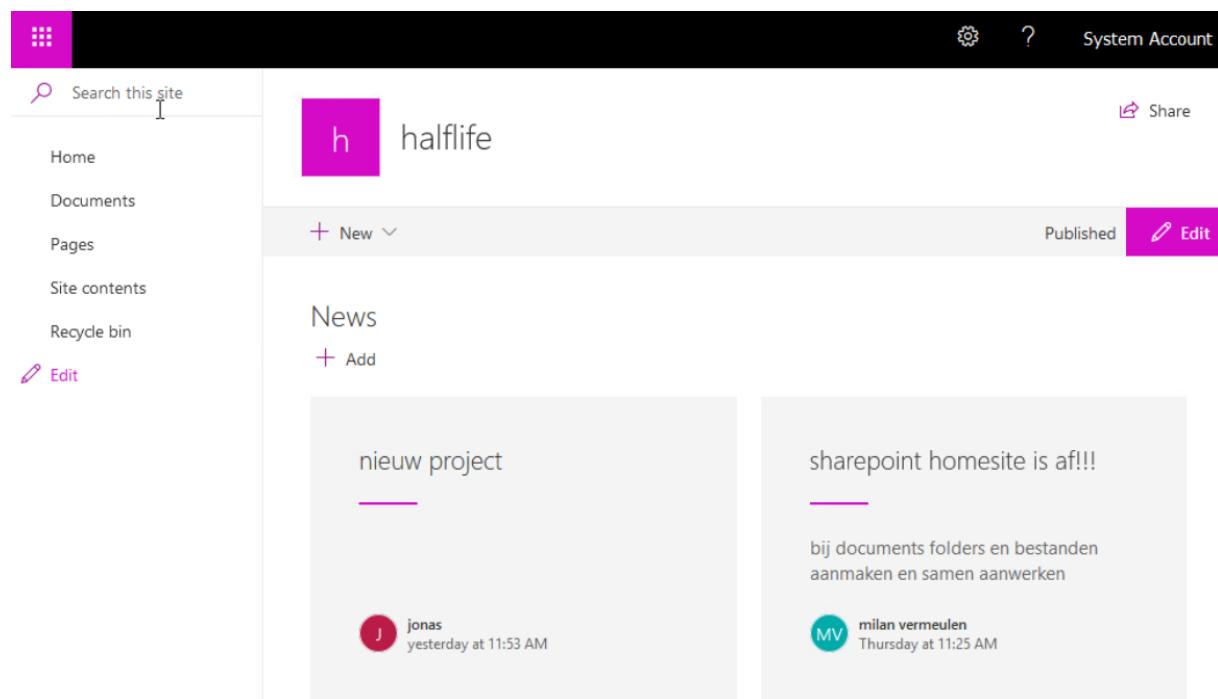
Intranet

Internet

Custom

Extranet

Als je nu surft naar <https://sharepoint/sites/halflife> dan kom je op onze teamsite.



The screenshot shows a SharePoint site titled "halflife". The top navigation bar includes a search bar, a gear icon, a question mark icon, and a "System Account" link. The left sidebar has links for "Home", "Documents", "Pages", "Site contents", "Recycle bin", and an "Edit" button. The main content area displays a "News" section with two items:

- nieuw project** by **jonas** yesterday at 11:53 AM
- sharepoint homesite is af!!!** by **milan vermeulen** Thursday at 11:25 AM

Below the news section, there is a note: "bij documents folders en bestanden aanmaken en samen aanwerken".

Op deze pagina kan je onder het tabblad 'Documents' folders maken of files uploaden , je kan er een status aan toevoegen je kan ze hier ook altijd downloaden. Je kan news delen, samen aan documenten werken.

Site 2

Firewall

Waarom PFsense?

PFsense is open source dus gratis te gebruiken en er komen regelmatig updates voor. PFsense is bovendien ook nog een licht programma en omdat we een beetje moesten oppassen met de resources die we tot beschikking hadden was dit dus ideaal.

Static WAN: 10.10.50.89/24

Static LAN : 192.168.2.1/24

WAN Gateway

We hebben een pfsense firewall opgezet met een WAN en een LAN kant voor het partner netwerk en die hebben we geconfigureerd volgens onderstaande stappen.

Login met je Admin account op de webGUI.

Eerst hebben we ons WAN IP static gemaakt omdat we niet met een echt WAN ip werken maar met een private ip adres. zo kan ons ip adres niet meer veranderen.

navigeer naar : “Interfaces” en klik dan op “WAN”

Kies bij ‘IPv4 configuration type’ static ipv4. bij IPv6 configuratie type kiezen we voor none. omdat we nu niet met ipv6 adressen gaan werken.

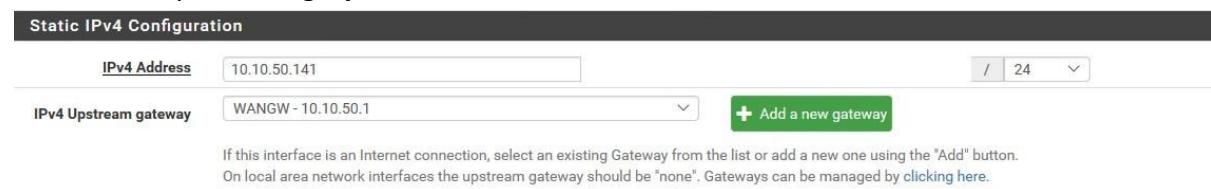


IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None

Scrol door naar Static IPv4 Configuration

Hier gaan we ons ip zetten.

Bij Ipv4 hebben we gekozen voor 10.10.50.89 omdat die niet in gebruik was. we zetten ook het subnet op /24 dat gelijk staat aan 255.255.255.0



IPv4 Address	10.10.50.141	/ 24
IPv4 Upstream gateway	WANGW - 10.10.50.1	+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

voor de upstream gateway klik je op add new gateway. (de groene kader)
dan krijgen we volgende popup.

New IPv4 Gateway

<input checked="" type="checkbox"/> Default	<input checked="" type="checkbox"/> Default gateway
Gateway name	<input type="text" value="WANGW"/>
Gateway IPv4	<input type="text"/>
Description	<input type="text"/>
<input type="button" value="+ Add"/> <input type="button" value="Cancel"/>	

Geef de gateway voor het wan adres een naam '**WANGW**' en geef het ip adres van de gateway. in ons geval is dat **10.10.50.1** klik op add.

En zorg ervoor dat onderstaande vinkjes zijn uitgevinkt.

Block private networks and loopback addresses	<input type="checkbox"/>
	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/>
	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Klik dan op Save.

LAN RULES

Nu stellen we de firewall regels in voor op het LAN netwerk. navigeer hiervoor naar 'Firewall' en klik dan op 'Rules' en dan kies je in de lijst 'LAN'

We hebben 3 Nieuwe regels aangemaakt.

- ICMP met any rules zodat we vanuit het 'LAN net' naar alles kunnen pingen voor te troubleshooten.
- TCP met source LAN net en met any destination en AD protocols zodat de RODC gemakkelijk verbinding kan maken met de Active directory
- TCP/UDP met source het LAN net en destination any en met het alias web. waaronder de poorten, HTTP, HTTPS & DNS zitten zodat iedereen in het LAN net verbinding kan maken met het internet

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	5 /482.26 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 3 /170.13 MiB	IPv4 ICMP any	LAN net	*	*	*	*	none		PING	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 31 /5.51 GiB	IPv4 TCP	LAN net	*	*	RODC	*	none		RODC	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1 /4 KiB	IPv4 TCP/UDP	LAN net	*	*	web	*	none		Internet acces	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 8 /9 KiB	IPv4 TCP/UDP	*	*	*	161 (SNMP)	*	none			Go to Setting

IPSEC

Nu dat we het LAN netwerk geconfigureerd hebben gaan we de IPSEC tunnel opzetten naar het interne netwerk. Navigeer naar ‘VPN’ en klik op ‘IPSEC’ dan klik je op tunnels en klik je op ‘Add p1’

The screenshot shows the 'IPsec Tunnels' configuration page. At the top, there are tabs for 'Tunnels', 'Mobile Clients', 'Pre-Shared Keys', and 'Advanced Settings'. The 'Tunnels' tab is selected. Below the tabs is a table titled 'IPsec Tunnels' with columns: IKE, Remote Gateway, Mode, P1 Protocol, P1 Transforms, P1 DH-Group, P1 Description, and Actions. One row is listed: IKE is V1, Remote Gateway is WAN (10.10.50.56), Mode is main, P1 Protocol is AES (128 bits), P1 Transforms is SHA256, P1 DH-Group is 14 (2048 bit), P1 Description is 'wan addr van pf 1', and Actions includes edit, copy, and delete icons. Below the table is a button labeled '+ Show Phase 2 Entries (1)'. At the bottom right of the page is a red box highlighting the green '+ Add P1' button.

kijk even na of je ipv4 gebruikt en de interface op WAN staat wat normaal default zou zijn dan bij remote gateway geef je het WAN ip adres van de interne firewall waar je de verbinding mee wilt maken. in ons geval is dit **10.10.50.88**. Geef een discription aan de IPSEC zodat je weet waarvoor deze regel dient.

scroll door naar de pre-shared key en laat alles daar boven op default staan. klik dan op ‘Generate ne pre-shared key’ deze sleutel ga je identiek moeten overnemen op de INTERNE firewall.

The screenshot shows the 'Pre-Shared Key' configuration page. It has a text input field containing '78c8d477fc41356dbd67ea02f9a1cf62faa4e4af5b8777c8e51ba27'. Below the input field is a note: 'Enter the Pre-Shared Key string. This key must match on both peers.' and 'This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.' At the bottom is a red box highlighting the orange 'Generate new Pre-Shared Key' button.

Laat voor de rest alles op default staan en klik op save.

Klik dan op show phase 2 en daarna op Add p2.

Kies bij local network voor het lan netwerk van deze firewall : 192.168.2.0/24

Bij remote netwerk kies je voor het Lan netwerk van de andere firewall. in ons geval 192.168.1.0/24

The screenshot shows the 'Phase 2 entry' configuration page for a new tunnel. It has several sections: 'Disabled' (checkbox), 'Mode' (Tunnel IPv4), 'Local Network' (Network type, address 192.168.2.0/24), 'NAT/BINAT translation' (None, address 0), 'Remote Network' (Network type, address 192.168.1.0/24), and 'Description' (connectie naar remote lan net). A red box highlights the 'Address' field for the Local Network section.

geef ook hier een beschrijving bij.

Scroll door naar onder naar automatically ping host en daar geef je het lan ip adres van de interne firewall. 192.168.1.1 en klik dan op save.

nu gaan we naar de interne firewall op ip 192.168.1.1

navigeer naar de IPSEC pagina klik op Add1

Kijk ook hier even na of we ipv4 gebruiken en op het WAN interface aan het configureren zijn. nu geven we bij de remote gateway het WAN adres van de externe firewall in dit geval is dat 10.10.50.89. geef ook hier weer een beschrijving op van wat je doet. scroll door naar de pre-shared key. deze moet exact hetzelfde zijn als op de externe firewall.

Pre-Shared Key	78c8d477fc41356dbd67ea02f9a1cf62faa4e4af5b8777c8e51ba27
Enter the Pre-Shared Key string. This key must match on both peers.	
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.	
Generate new Pre-Shared Key	

laat voor de rest alles op default staan en klik op save.

Kies nu voor show phase 2 en dan voor Add p2.

Typ nu hier bij het local network het ip adres van het LAN net van de interne Firewall : 192.168.1.0/24 en bij het remote netwerk voor het LAN net van de externe Firewall : 192.168.2.0/24. geef ook hier opnieuw een beschrijving van wat je doet.

Scroll door naar beneden naar Automatically ping host en geef hier het local ip adres van de externe firewall. Hier 192.168.2.1 en klik dan op save. Nu keren we terug naar de Externe firewall want hier gaan we nog even de rules instellen voor de ipsec.

navigeer naar Firewall en klik dan op 'Rules'

Maak een nieuw regel aan op de WAN interface.

Kies protocol Any, source 'Single host or Alias' en zet het WAN IP van de interne firewall : 10.10.50.88. en destination Any. en klik op save.

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 4.22 MiB	IPv4 *	10.10.50.56	*	*	*	*	none			 

Open nu de IPSEC tab onder de rules. Nu maken we hier nog een nieuwe rule aan. Kies protocol any, source => network => 192.168.1.0/24 en dan nog destination any en klik op Save! klik op save changes! en nu is de ipsec klaar voor gebruik.

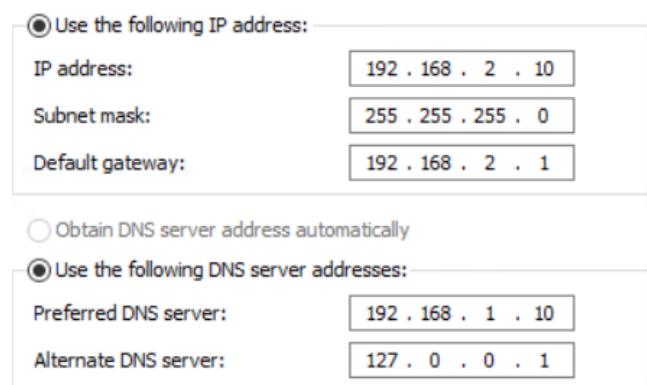
Read Only Domain Controller

Het opzetten van een RODC verschilt niet veel met het opzetten van een gewone Active Directory. We moeten enkel een configuratie aanpassen. Deze RODC gaat dienen als Active Directory van ons extern netwerk en vangnet voor het hele netwerk.

Network => Open network and internet settings => Network and sharing center =>
 Connections: Ethernet() => Properties => internet protocol version 4 (TCP/Ipv4) => properties

Hier stellen we onze netwerkgegevens in.

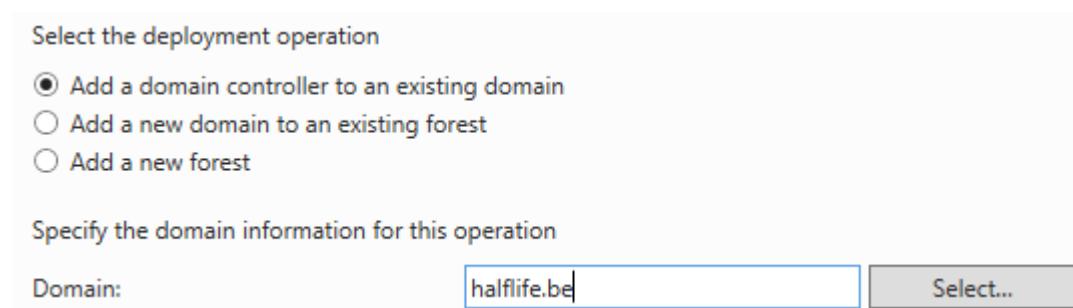
De DNS-server moet verwijzen naar de hoofd active directory van het netwerk.



The screenshot shows the 'Network and Sharing Center' interface. Under 'Connections', it lists 'Ethernet'. Clicking on 'Ethernet' leads to the 'Properties' screen. In the 'Internet Protocol Version 4 (TCP/IPv4)' properties window, the 'Use the following IP address' and 'Use the following DNS server addresses' options are selected. The IP address is set to 192.168.2.10, the subnet mask to 255.255.255.0, and the default gateway to 192.168.2.1. The preferred DNS server is set to 192.168.1.10, and the alternate DNS server is set to 127.0.0.1.

Na de installatie van 'Active Directory domain services' moeten we een domein toekennen aan de RODC. we klikken op 'promote this server to a domain controller'.

Bij de configuratie moeten we aanduiden dat we een controller willen toevoegen aan een bestaand domein. Daaronder moeten we de naam van het domein ingeven waar we ons aan willen aansluiten. Daaronder moeten we onze credentials aanpassen. We geven de naam en het wachtwoord in van de administrator en drukken op 'next'.



The screenshot shows the first step of the 'Promote This Server to a Domain Controller' wizard. It asks to 'Select the deployment operation'. The 'Add a domain controller to an existing domain' option is selected. Below it, there are two other options: 'Add a new domain to an existing forest' and 'Add a new forest'. The next section, 'Specify the domain information for this operation', shows the 'Domain:' field containing 'halflife.be' and a 'Select...' button.

Bij de domain controller options kun je het vakje aanduiden om deze controller enkel te laten dienen als een read-only account.

Read only domain controller (RODC)

Daarna geven we een secure wachtwoord op voor de restore modus.

We komen op een venster uit waar we de groepen moeten ingeven die toegang hebben en die geen toegang hebben op het repliceren van een wachtwoord naar de RODC.

Accounts that are allowed to replicate passwords to the RODC

HALFLIFE\Allowed RODC Password Replication Group

Enkel de leden van deze groep zullen die rechten krijgen.

Bij de additional options geven we in dat we willen repliceren van 'any domain controller'. We moeten nog het pad invullen waar de bestanden gaan worden opgeslagen, controleren de requisites op warnings & errors en installeren de RODC als er hier geen complicaties zijn.

Back-up PST-files

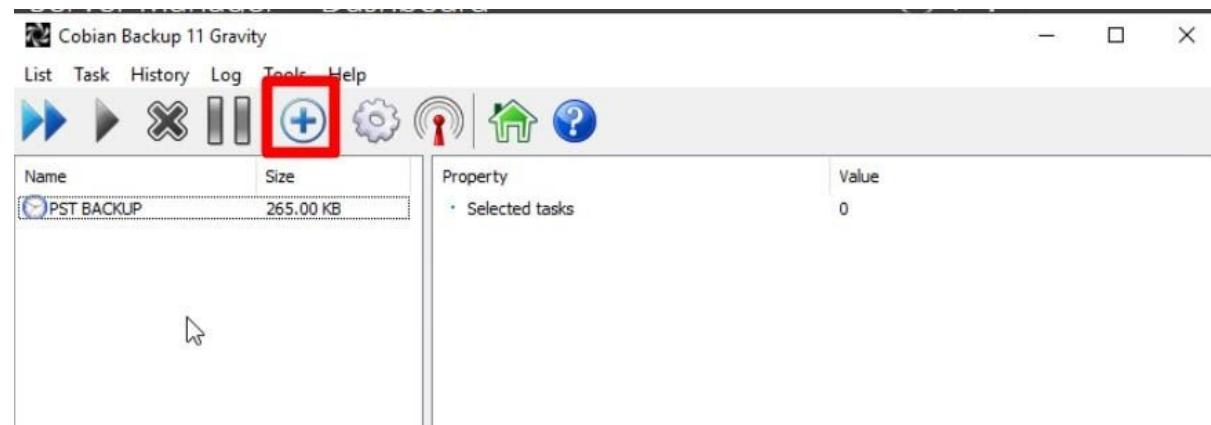
we hebben een windows server geïnstalleerd met daar het programma ‘Cobian backup 11’. We hebben voor deze software gekozen omdat deze gratis te gebruiken is, en omdat we vertrouwd zijn met het programma omdat we hier doorheen het jaar mee gewerkt hebben. we hebben op de active Directory een map onder de ‘C schijf’ staan waar we de pst files in opslaan en we connecteren naar deze map met het commando net use. zodat we deze bestanden zien staan over het netwerk

```
Administrator: Command Prompt
C:\Users\Administrator.HALFLIFE>net use p: "\\\ACTIVE DIRECTORY\pst files"
The command completed successfully.

C:\Users\Administrator.HALFLIFE>
```

dan openen we Cobian backup.

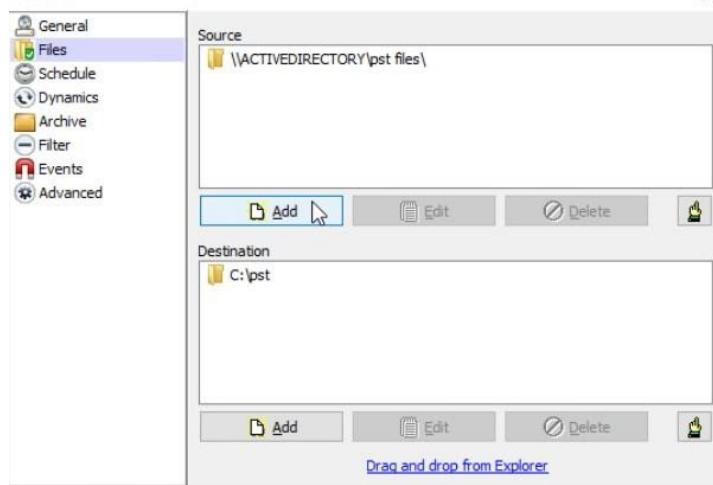
we klikken op het + teken voor het maken van een nieuwe backup task.



dan geef je de naam van de task op. onze heet PST BACKUP.

we klikken links op de tab ‘Files’ en klikken bij source op add. dan kiezen we onze shared netwerkmap ‘PST Files’ en klik op ok

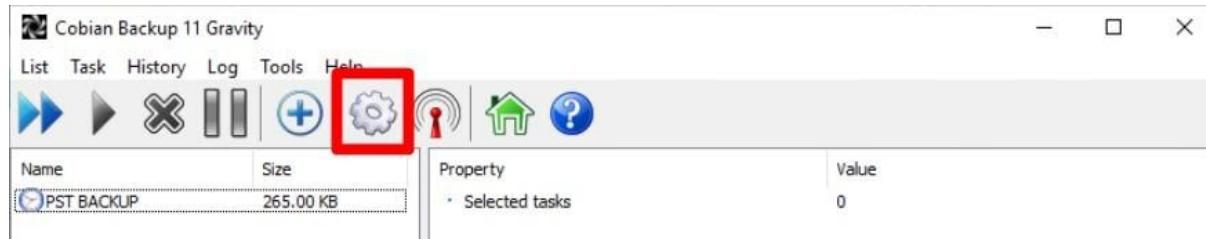
dan bij destination kies je een lokale map waar je de backup wilt opslaan. en klik op Ok.



vervolgens klik je op de tab 'schedule' en zet het op weekly en we hebben gekozen om elke zondagnacht om 2u een backup te maken klik op Ok.

Kies dan nog tab Dynamics en zet 'Full copies to keep' op 10.

Nu gaan we nog de mail instellen dat we voor elke keer als er een backup wordt gemaakt dat we een mail krijgen. ga hiervoor dus naar de instellingen.



Klik op de tab 'Log' en vink 'Mail log files' aan.

Ga nu naar de tab 'Mail'.

geeft de smtp server op. in ons geval is dit onze exchange server (192.168.1.20)

kies een email adres voor de verzender en voor de ontvanger.

en vink authentication aan voor de mail verzender.

Check "Mail log file" in the Log tab to use the mail function

Sender's name	Sender's address	
Cobian Backup 11 Gravity	backup@halfife.be	
SMTP server	Port	
192.168.1.20	25	
Subject		
Cobian Backup 11 (%COMPUTERNAME) Backup pst files		
Recipients		
<input type="checkbox"/> Administrator@halfife.be		
<input type="button" value="Add"/>		
<input type="button" value="Edit"/>		
<input type="button" value="Delete"/>		
<input checked="" type="checkbox"/> Authentication		
User name	Password	
backup	*****	
<input type="button" value="Proxy..."/>	<input type="button" value="SSL..."/>	<input type="button" value="Test..."/>

Klik op Ok.

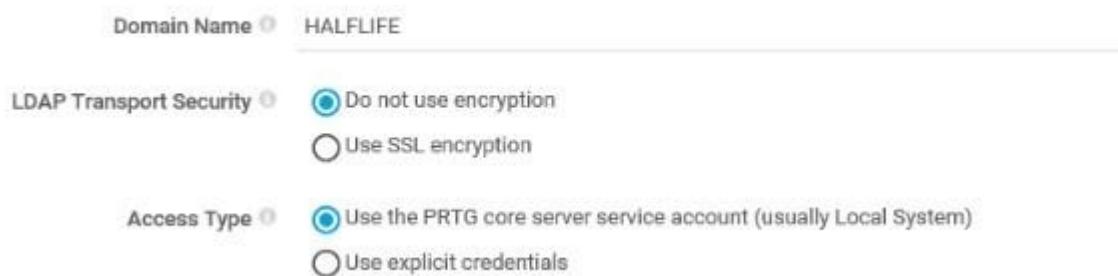
Monitoring

PRTG is een monitoring software en deze is gratis te gebruiken tot 100 sensors.

Omdat we met een beperkt aantal werkgeheugen zitten hebben we besloten om deze software te installeren op onze Read-only domain controller. Hier vind je de download [link](#) voor de software.

Na het installatieproces is er een nieuwe desktop icon beschikbaar “PRTG Network Monitor” deze open je. nu wordt er gevraagd om in te loggen. de default login is : ‘prtgadmin’ voor gebruikersnaam & wachtwoord. dit wachtwoord verander je best achteraf.

We beginnen met het koppelen met de software aan de Active directory. dit doen we door naar ‘setup’ te gaan , dan ‘core & probes’ en dan scrol je naar active directory integration. en geef hier je domeinnaam in



nu gaan we onze meldingen instellen. we gaan weer naar ‘setup’, dan naar ‘Notification delivery’.

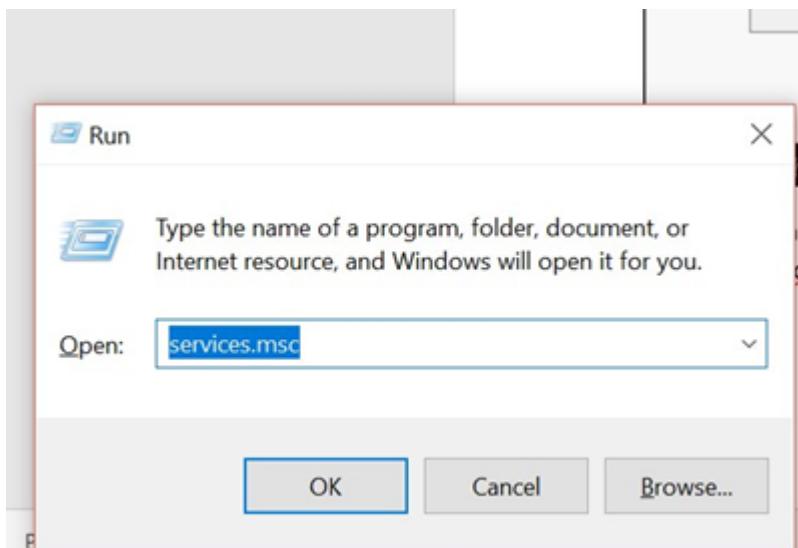
dan kies je ‘Use SMTP relay server’ want we gaan onze eigen mailserver hiervoor gebruiken. geef een mailadres op voor prtg om een mail mee te verzenden. en zet bij smtp relay server de hostname van de exchange server. in ons geval is dit **mail.halflife.be** sla deze instellingen op door op save te klikken.

We willen graag op de hoogte gehouden worden van hoeveel opslag er nog beschikbaar is op de exchange en op de fileserver. daarom gaan we nu **SNMP** aanzetten op de exchange en op de fileserver.

Exchange

open manage’, ‘Add roles and features’

Klik dan 4 x op ‘Next” en selecteer dan in de lange lijst **SNMP Service** en installeer deze tool. Open dan de services



en zoek 'SNMP service'. Ga naar de 'security' tab

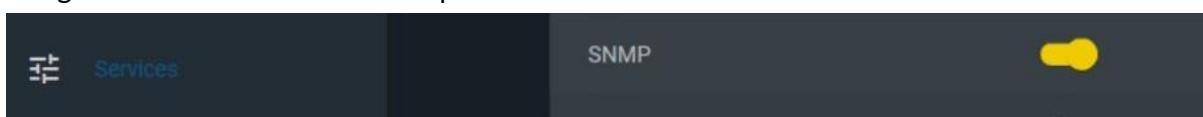
Bij accepted community names, klik op add en typ 'public' in de tekstbalk en klik op add. klik dan op Accept SNMP packets from these hosts, en voeg het ip adres van de RODC toe

192.168.2.1

FreeNAS

Login op de gui van FreeNas op **192.168.1.30**

navigeer naar services en zet snmp aan.



RODC

Nu kunnen we op PRTG al de netwerk toestellen toevoegen. volg onderstaande stappen om een toestel toe te voegen.

- >Klik op de device tab.
- >Rechtermuisknop op servers
- >Add device

Geef dan een naam op voor de server, het IPV4 adres, kies een icoon en selecteer 'standard auto-discovery' en klik op OK.

Connect using IPv4

 Connect using IPv6

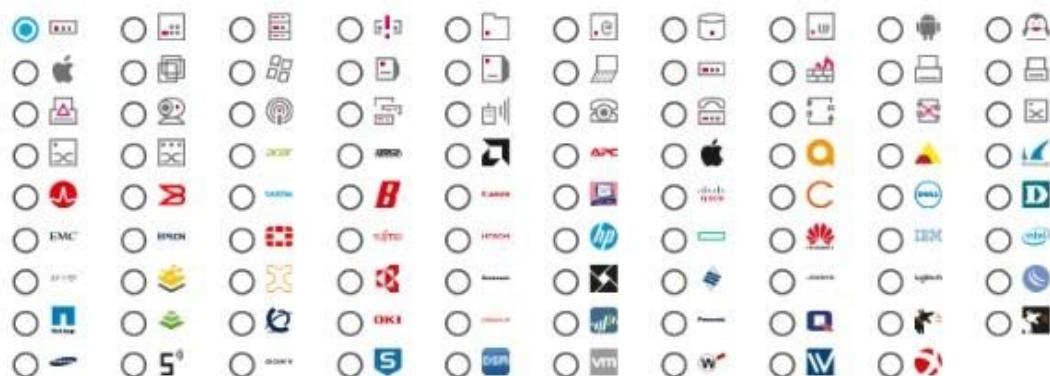
IPv4 Address/DNS Name *

This field is required.

Tags *



Device Icon *



Device Identification and Auto-Discovery

Auto-Discovery Level *

- No auto-discovery
- Standard auto-discovery (recommended)
- Detailed auto-discovery
- Auto-discovery with specific device templates

Schedule *

[Cancel](#)

[OK](#)

eens al de servers zijn toegevoegd gaan we naar exchange server en klikken op settings. kijk tussen de instellingen of 'Credentials for SNMP devices' is uitgevinkt en zorg ervoor dat de community string dezelfde waarde heeft als eerder opgegeven in services van de exchange server.

Credentials for SNMP Devices

inherit from [Servers \(SNMP Version: V2, SNMP Port: 161, SNMP Timeout: ...\)](#)

SNMP Version *

v1

v2c (recommended)

v3

Community String * public

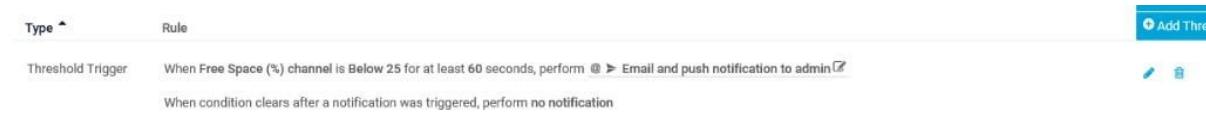
SNMP Port * 161

SNMP Timeout (Sec.) * 5

als je dit gedaan het voeg je een sensor toe op de exchange server.
dan zet je de sensor 'SNMP disk free' op de exchange server en op de fileserver.

Nu gaan we nog een melding trigger toevoegen voor als de schijf vol begint te geraken.
selecteer je sensor en klik ok 'notification triggers'.

Klik op Add Threshold trigger.
en geef een melding als de schijf minder dan 25% schijfruimte over heeft.



The screenshot shows a table with two columns: 'Type' and 'Rule'. There is one row listed:

Type	Rule
Threshold Trigger	When Free Space (%) channel is Below 25 for at least 60 seconds, perform @ > Email and push notification to admin When condition clears after a notification was triggered, perform no notification

At the top right of the interface, there is a blue button labeled 'Add Threshold'.

Doe dit voor elke schijf die je wilt monitoren.

Webserver

Wat is een DMZ?

Een DMZ is een Demilitarized zone dit is een apart netwerk segment dat wordt gebruikt om toestellen in te zetten die ook veel verkeer gaan hebben van mensen buiten ons eigen netwerk. Dus omdat iedereen toegang heeft tot die toestellen will we deze gescheiden houden van ons LAN netwerk voor veiligheidsredenen.

Webserver

Voor onze webserver heb ik gekozen voor een LAMP-stack. LAMP staat voor Linux dit is het operating systeem voor onze heb ik voor Ubuntu 18.04 server gekozen, Apache dit is de webserver; MySQL dit is de database waar de data van de website is opgeslagen en PHP is een scripting-taal die onze dynamische webpagina's te maken.

als eerste gaan we onze netwerkinstellingen aanpassen met het commando.

'Sudo nano /etc/netplan/50-cloud-init.yaml'

```
network:
  ethernets:
    ens160:
      addresses: [172.16.0.3/28]
      gateway4: 172.16.0.1
      dhcp4: no
      nameservers:
        addresses: [172.16.0.1]
      optional: true
  version: 2
```

' sudo netplan apply' om de netwerkinstellingen toe te passen.

Voordat we beginnen kijken we of er updates zijn en downloaden deze moesten ze er zijn.

'sudo apt update' 'sudo apt upgrade'

nu gaan we de Apache webserver installeren 'sudo apt install apache2' vervolgens duwen op Y en enter en dan begint de installatie.

Vervolgens gaan we onze firewall aanpassen om http en https trafiek door te laten

'sudo ufw allow in "Apache full"

Als dit afgerond is is we Apache webserver klaar en gaan we MySQL installeren

'sudo apt install mysql-server'. als de installatie klaar is gaan we een script starten zodat we ons wachtwoord voor onze MySQL root user kunnen instellen.

'sudo mysql_secure_installation'

als eerste wordt er gevraagd of we de Validate password plugin willen configureren ik heb Y gekozen om dit te configureren dit is goed zo kan je ervoor dat dat wacht woorden aan bepaalde criteria moeten voldoen ik heb gekozen voor 1 medium hierdoor moeten alle wachtwoorden tenminste 8 karakters lang zijn cijfers, kleine- hoofdletters en speciale karakters bevatten om goedgekeurd te worden. Hierna moeten we een wachtwoord voor onze MySQL root user instellen (kies hier voor een sterk wachtwoord). als je je wachtwoord gekozen hebt kies je nog 3 keer voor een anonieme user en een test database te verwijderen

en ervoor te zorgen dat je niet met de root user kan inloggen als je niet op de webserver zelf zit.

nu gaan we ervoor zorgen dat we ons wachtwoord moeten ingeven als we als root inloggen op MySQL

'sudo mysql'

ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password'; ← hier vul je je eigen wachtwoord in.

daarna updaten we onze tabel met 'FLUSH PRIVILEGES'

nu gaan we kijken of onze root user echt met een wachtwoord moet inloggen

'SELECT user,authentication_string,plugin,host FROM mysql.user;

```
mysql> SELECT user,authentication_string,plugin,host FROM mysql.user;
+-----+-----+-----+-----+
| user | authentication_string | plugin | host |
+-----+-----+-----+-----+
| root | *B823F5235EF7FFD5F7801DF86BEF783B99EBBA0F | mysql_native_password | localhost |
| mysql.session | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE | mysql_native_password | localhost |
| mysql.sys | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE | mysql_native_password | localhost |
| debian-sys-maint | *33CEDE75BC24D751E8D2879BFC7FB61E7617BE73 | mysql_native_password | localhost |
+-----+-----+-----+-----+
4 rows in set (0.00 sec)
```

Om de MySQL shell te verlaten typ je gewoon exit

Nu gaan we PHP installeren

'sudo apt install php libapache2-mod-php php-mysql'

bij een standaard apache installatie gaat Apache als een directory wordt opgevraagd in een file genaamd index.html wij gaan er voor zorgen dat deze eerst in de index.php file gaat kijken. Dit doen we door deze op de eerste plaats te zetten in de dir.conf file

'sudo nano /etc/apache2/mods-enabled/dir.conf'

```
<IfModule mod_dir.c>
  DirectoryIndex index.php index.html index.cgi index.pl index.xhtml index.htm
</IfModule>
```

Nu herstarten en Apache webserver met 'sudo systemctl restart apache2'.

Als dit gebeurt is zullen we een virtual host aanmaken. Eerst maken we een directory aan met halflife als naam.'sudo mkdir /var/www/halflife'. Vervolgens veranderen we de ownership 'sudo chown -R \$USER:\$USER /var/www/halflife'.

En passen we de rechten aan 'sudo chmod -R 755 /var/www/halflife'.

In deze directory maken we een nieuwe file aan 'index.html'

```
GNU nano 2.9.3                               /var/www/halflife/index.html

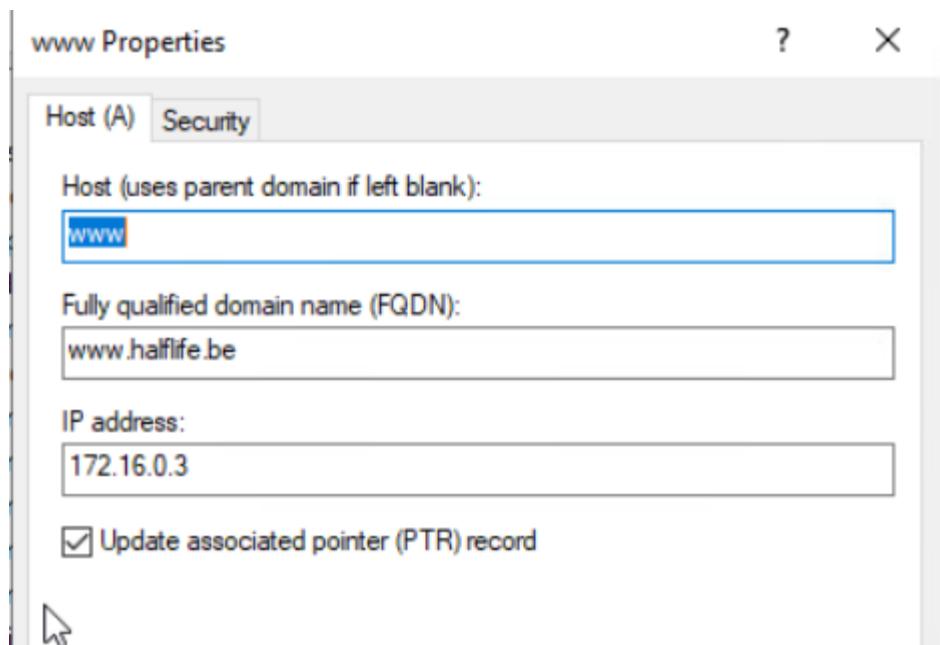
<html>
  <head>
    <title>Welkom op halflife.be</title>
  </head>
  <body>
    <h1>Eindproef groep B 2019-2020</h1>
  </body>
</html>
```

Als dit gebeurt is save and close en gaan we een virtual host file aanmaken
 'sudo nano /etc/apache2/sites-available/halflife/halflife.conf'

```
GNU nano 2.9.3           /etc/apache2/sites-available/halflife.conf

<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  ServerName halflife.be
  ServerAlias www.halflife.be
  DocumentRoot /var/www/halflife
  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/acces.log combined
</VirtualHost>
```

'sudo a2ensite halflife.conf' om de website aan te zetten, en 'sudo a2dissite 000-default.conf' om de default website te uit te zetten. nu herstarten we Apache om de verandering door te voeren ' sudo systemctl restart apache2'. omdat onze website nog niet gelinkt is aan het IP van onze server gaan we een A record in onze DNS server moeten aanmaken om dit bekend te maken op ons domein. Op je DNS server bij forward lookup zones klik je op je domeinnaam en kies je voor 'new host (A or AAA)



vergeet niet het vinkje 'update associated pointer record' aan te duiden en dan ben je klaar. als je nu surft naar <http://halflife/be> surft binnen ons netwerk kom je om deze Lamp server uit.

Service Level Agreement

Service Level Agreement (SLA)

for Customer

by Groep B

Effective Date: 29/05/2020

Document Owner:	Groep B
------------------------	----------------

Version

Version	Date	Description	Author
1	29/05/2020	Service Level Agreement	Jonas Vermesen

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this Agreement.)

Approvers	Role	Signed	Approval Date
Groep B	Service Provider		29/05/2020
Halflife	Customer		29/05/2020

Agreement Overview

This Service-Level Agreement, effective as of 29/05/2020, is made between Halflife and Groep B for providing information and service exchange necessary to support and maintain the product or service.

This Agreement remains valid until mutually endorsed by the stakeholders.

Goals & Objectives

The goal of this Agreement is to obtain mutual agreement between the Service Provider(s) and Customer(s).

The objectives of this Agreement are to:

- a. Provide a thorough understanding of service ownership and the roles and responsibilities.
- b. This Agreement represents a concise description of the services provided by the Service Provider.
- c. Match perceptions of expected service provision with actual service support & delivery.

Stakeholders

The following Service Provider(s) and Customer(s) will be used as the basis of the Agreement and represent the primary stakeholders associated with this SLA:

Service Provider(s): Groep B (“Provider”)

Customer(s): Halflife (“Customer”)

Periodic Review

The terms stated in the Agreement shall be valid from the Effective Date. The revisions to this agreement shall be carried out every fiscal year, however, during the revision, the current Agreement shall be considered valid.

Business Relationship Manager: Groep B

Review Period: 12 months

Previous Review Date: 29/05/2020

Next Review Date : 29/05/2021

Service Agreement

The following are the responsibility of the Service Provider in the ongoing support of this Agreement.

Service Scope

The following Services are covered by this Agreement;

- Binnen 12 uur remote ondersteuning bij problemen van onze diensten.

- Binnen de 3 dagen onsite ondersteuning bij grote problemen van onze diensten.

Customer Requirement

Customer responsibilities and/or requirements in support of this Agreement include:

- Payment for all support costs at the agreed interval.

Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Adhering to appropriate response times associated with service-related incidents.
- Advance notification to the Customer for all maintenance.

Service Assumptions

Assumptions related to in-scope services and/or components include:

- Changes to services will be communicated and documented to all stakeholders.

Service Management

For maintaining adequate customer-support levels, this Agreement lists the available scope of services provided by the Service Provider. This lists details regarding availability, monitoring, and other relevant factors.

Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- Telephone support: 0494 28 81 85
- Email support: jonas@groepb.be

Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service-related incidents and/or requests submitted by the Customer within the following time frames:

- 0-8 hours (during business hours) for issues classified as High priority.
- Within 48 hours for issues classified as Medium priority.
- Within 5 working days for issues classified as Low priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

Bronvermelding

Cursussen van syntra netwerkbeheer doorheen het jaar 2019 - 2020

<https://support.nagios.com/>

<https://www.paessler.com/>

<https://docs.netgate.com/pfsense/>

<https://www.microsoft.com/>

<https://www.ixsystems.com/documentation/freenas/>

<https://forum.cobiansoft.com/>

<https://ubuntu.com/>

<https://www.veeam.com/>

<https://tracktime24.com/>

<https://www.starwindsoftware.com/blog/installing-sharepoint-2019>

<https://nl.wikipedia.org/wiki/Hoofdpagina>

<https://docs.microsoft.com/en-us/sharepoint/>

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-ubuntu-18-04>

<https://www.linuxbabe.com/ubuntu/install-lamp-stack-ubuntu-18-04-server-desktop>

https://community.spiceworks.com/how_to/153965-clear-exchange-2013-2016-log-files

<https://support.microsoft.com/nl-be/help/287070/how-to-manage-pst-files-in-microsoft-outlook>

Slot

Dit is het einde van ons eindwerk. Heel graag zouden we Eddy Debauve, Steven Reekmans en Luca Ruggiero willen bedanken voor dit geweldig jaar en voor het delen van hun kennis dat gaat ons in onze komende jaren enorm helpen in een verdere carrière als netwerkbeheerders en wij wensen hun nog het beste in de volgende jaren.