PROFIELWERKSTUK

“PROFESSIONELE COMPUTER INFRASTRUCTUUR”

Gemaakt door: *Pieter Steenbergh*
Klas: *6 VWO*
Vak en begeleider: *Wiskunde A, de heer Schoon*
Inleverdatum: *31 augustus 2020*

INHOUDSOPGAVE

1 ONDERZOEKSOPZET

1.1 INTRODUCTIE

Ik heb als hobby bezig zijn met computers. Ik hou ervan projectjes uit te denken en uit te werken rond allerlei verschillende computervraagstukken. Ik zoek net zolang informatie op het internet op totdat ik weet hoe ik bepaalde zaken moet oplossen, zoals een plex mediaserver maken, gameservers maken, een eigen webserver hosten, websites schrijven door middel van html en CSS, software installeren en het zelf bouwen van een server. Die projectjes leidden tot steeds grotere projecten die je thuis kan uitdenken en uitwerken.

Toen ik ging nadenken over het onderwerp voor mijn profielwerkstuk, wilde ik graag aansluiten bij een onderwerp dat echt mijn interesse heeft. Dat zijn dus technische computer gerelateerde onderwerpen. Zo ben ik mij in de loop van de tijd steeds verder gaan oriënteren en verdiepen in het onderwerp “computerinfrastructuur”. Mijn motivatie was om meer te leren van computerinfrastructuur zoals die in een grote organisatie wordt gebruikt. Mijn bestaande kennis kon ik hiervoor gebruiken. Ik wilde mij verder verdiepen in de technische vaardigheden die nodig zijn om een netwerk te kunnen (na)bouwen.

Het bleek voor mij mogelijk om via de schoolcomputer toegang te krijgen tot bepaalde openbare informatie, zoals de lokale IP structuur, de domeinstructuur, remote management programma’s etc. Aan de hand hiervan ben ik zelf een netwerk thuis gaan bouwen.

1.2 ONDERZOEKSVRAAG EN DEELVRAGEN

Hoofdvraag: Hoe bouw je een infrastructuur zoals op school wordt gebruikt, thuis na?

Om hierop een antwoord te kunnen vinden heb ik verschillende stappen moeten doorlopen. Ik moet de volgende deelvragen gaan onderzoeken en beantwoorden:

1. Welke technische onderwerpen en begrippen moet ik begrijpen voordat ik in staat ben een infrastructuurnetwerk thuis na te bouwen?
2. Hoe ziet het netwerk van het RLW (Rijnlands lyceum Wassenaar) er uit? Hiervoor moet ik het netwerk van school bekijken en onderzoeken hoe dit is opgezet.
3. Is het mogelijk een handleiding/demo te bouwen zodat anderen mijn resultaat kunnen nabouwen?

Ik hoop – na het doorlopen en beantwoorden van de deelvragen – zodanig veel kennis opgebouwd te hebben dat het mij lukt thuis een computer infrastructuur na te bouwen gelijkend op die van het RLW.

1.3 WERKWIJZE

Doordat er zo veel informatie is over computers op het internet, moet ik keuzes gaan maken wat ik wel en niet nader ga uitzoeken en uitleggen in dit profielwerkstuk. Ik moet alleen die informatie gaan opschrijven die nodig is om een computernetwerk thuis na te kunnen bouwen.

Verder moet het lezen van het profielwerkstuk voor de lezer te begrijpen zijn en de lezer moet kunnen volgen wat ik doe. Ik probeer daarom in de eerste hoofdstukken eerst zoveel mogelijk uit te leggen wat alle technische begrippen inhouden. Hierdoor hoop ik dat bij de uiteindelijke demo(handleiding)[1] die ik ga maken, de lezer begrijpt wat ik heb gedaan.

Ik ga er daarbij wel vanuit dat de lezer een bepaalde technische basiskennis van computers en netwerken heeft, omdat ik anders te veel moet uitleggen en toelichten. De bedoeling is uiteindelijk dat degene die de demo (handleiding) bekijkt/leest, zelf in staat is om mijn thuis geïmiteerde schoolsysteem zelf op zijn eigen thuis netwerk na te bouwen.

1.4 TE REALISEREN DOELEN EN ONDERDELEN

Er zijn tijdens mijn onderzoek een aantal doelen die ik wil bereiken. In dit profielwerkstuk ga ik onderzoeken of het mij lukt de volgende zaken te realiseren:

- De instellingen en documenten van de gebruikers moeten op één server worden gesynchroniseerd, zodat - wanneer zij inloggen via een andere computer -, zij hun documenten en instellingen automatisch meenemen, waarbij instellingen van Chrome ook mee moeten worden ge-synchroniseert;
- Ik wil dat Windows makkelijk kan worden geïnstalleerd via een netwerkboot. Hierdoor kunnen bepaalde programma's en applicaties (zoals printers, permissies, register aanpassingen, taal, group policy etc) worden versoepeld.
- Een gebruiker moet kunnen inloggen via de browser zodat die een desktop sessie krijgt toegewezen zoals Citrix;
- Ik moet spellen kunnen blokkeren en zien wat wordt gedaan op het netwerk (zoals welke websites worden bezocht).

Om deze doelen te bereiken zijn er een aantal onderdelen die ik tenminste moet maken. De volgende onderwerpen zal ik nader gaan uitwerken:

- Router systeem: Alles wat komt kijken bij het opzetten van een "netwerk" (hoofdstuk 2);
- Hypervisor: Van één computer/server meerdere computers maken (virtual machines). Dit wordt uitgewerkt in hoofdstuk 3;
- Cloud desktop: Een gebruiker kan via de browser inloggen op een Desktop sessie (website/filmpje);
- Lokale login: Instellingen moeten worden ingeladen bij het inloggen van een ander werkstation. Dit wordt uitgewerkt in hoofdstuk 4.

Aan het eind van mijn profielwerkstuk heb ik een begrippenlijst opgenomen. Om deze reden hanteer ik afkortingen in mijn tekst.

1.5 GRENZEN AAN MIJN ONDERZOEK

[1] Ik heb hiervoor de volgende website voor ogen: https://computerinfrastructuur.nl/

Er zijn een aantal zaken waarvan ik weet dat die niet gaan lukken, omdat hiervoor mij de nodige licenties ontbreken (vaak zijn deze te kostbaar om aan te schaffen). In mijn onderzoek zal ik daarom gebruik moeten maken van bepaalde open source programma's en dergelijke als alternatieve bronnen.

Ook heb ik niet de beschikking over bepaalde hardware die nodig is. Ik heb echter wel een tweede server nodig die krachtig genoeg is om desktop sessies te hosten. Omdat ik deze niet zomaar kan aanschaffen, heb ik deze geleend van een computerbedrijf "Comprofs[2]". Zij waren bereid mij tijdelijk een server te lenen. Ik heb deze bij hen opgehaald en geïnstalleerd op zolder.

2 INFORMATIE UITWISSELING TUSSEN COMPUTERS

In dit hoofdstuk behandel ik de basis die nodig is om te begrijpen hoe netwerken werken en computers informatie met elkaar uitwisselen.

2.1 VERSTUREN VAN INFORMATIE TUSSEN COMPUTERS

Computers moeten met elkaar kunnen communiceren. Dit doen ze met behulp van het zogeheten IPv4 of IPv6 (Internet Protocol version). Hierbij wordt informatie van een plek naar een andere plek verstuurd.

Ik zal eerst het verschil uitleggen tussen Lokaal IP-adressen en public IP-adressen. De lokale IP-adressen worden gebruikt om lokale apparaten te identificeren op een LAN-netwerk (Local Area Network). Public IP-adressen worden gebruikt om apparaten te identificeren op een WAN-netwerk (wide area network). Bij public IP-adressen zijn deze apparaten vaak modems en worden de IP-adressen toegewezen door ISP's (Internet Service Providers). Hierbij is de router een doorvoermiddel om public IP- adressen te verminderen. Dit wordt ook wel NAT (Network Address Translation) genoemd.

afbeelding 1: schematische weergave van wereld netwerk

Niet elke computer heeft een IP-adres. Dat is namelijk niet altijd nodig, want niet elk apparaat hoeft te communiceren met andere apparaten. Het verschil tussen een apparaat met een IP adres en eentje zonder een IP adres is dat een apparaat dat een IP-adres kan krijgen een NIC (Network Interface Card) heeft. Dit kan zowel hardwired of ge-connect zijn via een usb stickje of netwerkkaart.

Een MAC adres (media access control) - ook wel fysiek adres - is een serial nummer van de NIC. Deze is voor elke NIC anders en identificeert als het ware de NIC. Dit is handig voor de router zodat niet hetzelfde IP-adres aan meerdere apparaten kan worden toegewezen. Het MAC adres kan je dus niet wijzigen en is statisch.

Voorbeeld: Stel je hebt 2 apparaten

[2] Zie https://www.comprofs.nl/ voor achtergrondinformatie over dit computer bedrijf.

- Apparaat 1 B9:0B:9D:A7:77:A4
- Apparaat 2 BD:9F:68:26:27:7F

De router moet een IP-adres toewijzen aan apparaat 1. Dan zal hij deze niet meer toewijzen aan apparaat 2, want dit wordt gezien als een nieuw MAC adres (dus een andere computer). Dus apparaat 2 krijgt een nieuw IP-adres toegewezen.

Naast het IP-adres wordt meer informatie aan het apparaat toegewezen. Ik zal hierover meer uitleggen in de paragraaf 2.3.1 DHCP.

Dus het IP-adres identificeert een computer ten opzichte van andere computers. En een MAC adres identificeert de NIC en kan worden gebruikt door de router om een nieuw IP-adres uit te geven.

2.2 STRUCTUUR VAN IP ADRESSEN

Er bestaan 2 verschillende soorten mainstream gebruikte IP protocollen, namelijk IPv4 en IPv6 (internet protocol versie 4 en versie 6). Andere protocollen zijn voor nu even niet relevant.

2.2.1 INTERNET PROTOCOL VERSIE 4 (IPV4)

IPv4 is opgebouwd uit 32 bits en bevat daarom 2^{32} = 4.294.967.296 IP-adressen. Het eerste wat hier opvalt is dat dit getal minder is dan het totaal aantal mensen op aarde. Dit betekent dat er een schaarste is in het aantal IPv4 adressen. We kunnen het aantal IP adressen verhogen door een LAN netwerk te gebruiken in combinatie met NAT.

Er zijn een aantal gereserveerde IP adressen die niet kunnen worden gebruikt als public IP adressen. Dit zijn adressen zoals **10.0.0.0/8, 192.168.0.0/16 en 127.0.0.1**. Hiernaast zijn er nog een aantal adressen die je niet kan gebruiken als public IP. Deze zijn in de demo weggelaten omdat ik deze zelf niet gebruik. Voor iemand die nog nooit een IP-adres heeft gezien, zeggen de bovenstaande cijfers niets. Daarom ga ik ze hieronder kort toelichten.

127.0.0.1 is het lokale adres (local host address) dat voor elke computer hetzelfde is. Dit wordt ook wel het loopback adres genoemd. Dit is dus het adres dat terug verwijst naar jouw computer.

192.168.0.0/16 Dit is een voorbeeld van een lokaal adres. Als je zou kijken wat het IP adres van jouw computer is dan krijg je waarschijnlijk 192.168.cijfer.cijfer waarbij 192.168 voor iedereen hetzelfde is. Naast dit lokale adres heb je ook nog 10.0.0.0/8 en 172.16.0.0/12 gereserveerd voor privé adressen (lokale adressen).

In mijn thuissituatie heb ik als IP adres van mijn computer “192.168.1.cijfer/24”, dus daarom ga je dit adres vaak terugzien in dit profielwerkstuk en de door mij toegepaste methode. Misschien was het al opgevallen maar er staat /16/8/12 achter het adres. Dit zijn als het ware de bitjes die worden gereserveerd als je een IP adres opdeelt. Een IPv4 adres bestaat uit 32 bits en is opgedeeld in 4 groepen van 8 bits. Als voorbeeld neem ik 192.168.1.0/24. Kijken we naar 24 dan wordt bedoeld dat de eerste 24 cijfers gereserveerd worden voor het subnet (deelnetwerk in een netwerk) en de overige 8 cijfers voor het host-ID. Dit zou betekenen dat er 2^8=256 lokale IP adressen zijn. Dit is de reden waarom er maximaal lokale 256 IP-adressen zijn (want 0 telt ook mee). Als je dit niet begrijpt bekijk het voorbeeld hieronder:

- Hoogste binaire getal 11111111.11111111.11111111.11111111 = 255.255.255.255
- Laagste binaire getal 00000000.00000000.00000000.00000000 = 0.0.0.0

2.2.2 INTERNET PROTOCOL VERSIE 6 (IPV6)

IPv6 heeft veel voordelen ten opzichte van IPv4. Het grootste voordeel is dat bij IPv6 het adres bestaat uit 128 bits dus 2^{128}= aantal beschikbare IP adressen. Hiermee is het toekomstige probleem van te weinig IPv4-adressen verholpen.

Een voorbeeld van een IPv6 is 2001:1c00:1800:0:79e6:f0e1:3f6d:872a

Persoonlijk vind ik IPv6 lastiger en gebruik ik hem verder ook niet in de handleiding die ik ga maken. Daarom zal ik hem niet verder toelichten.

2.2.3 TCP EN UDP PROTOCOL

TCP (Transmission Control Protocol) en UDP protocol (User Datagram Protocol protocol) zijn voorbeelden van veel gebruikte protocollen. Deze protocollen helpen bij het versturen en ontvangen van informatie. Om dit goed uit te leggen verwijs ik naar het OSI-model (Open Systems Interconnection). Hierbij zijn de stappen van het overbrengen van informatie in 7 lagen opgedeeld.

OSI-model				
	Data-eenheid	Laag		Functie
Host layers	Data	7. *Application layer* (Toepassingslaag)		Protocollen voor directe uitwisseling met de applicatie.
		6. *Presentation layer* (Presentatielaag)		Formatteert en structureert data t.b.v. applicatie-interpretatie.
		5. *Session layer* (Sessielaag)		Start, onderhoudt en beëindigt sessies tussen applicaties.
	Segment (TCP) / Datagram (UDP)	4. *Transport layer* (Transportlaag)		Segmentatie, volgordelijkheid van de data-segmenten en foutcorrectie.
Media layers	Packet	3. *Network layer* (Netwerklaag)		Logische adressering, route-informatie,
	Frame	2. *Data link layer* (Datalinklaag)	LLC ('Logical Link Control')	Protocol multiplexing (Sublaag: LLC), mediumtoegang ('Token Passing' /CSMA/CD), fysieke adressering (Sublaag: MAC) en foutdetectie.
			MAC ('Media Access Control')	
	Baud / symbolen	1. *Physical layer* (Fysieke laag)		Binaire transmissie, elektrische, elektromagnetische of optische specificaties van het signaal en fysieke specificaties van het medium.

afbeelding 2: OSI-Model

De 7 lagen zijn als volgt:

7. Toepassing laag
6. Presentatie laag
5. Sessie laag

} “applicatielagen”

4. Transport laag (is het TCP UDP protocol)
3. Netwerk laag betreft het IPV4 of het IPV6 protocol, zoals hierboven reeds is toegelicht;
2. Data laag is het MAC adres
1. Fysieke laag (is de hardware)

Hierboven heb ik de fysieke data en netwerk laag al uitgelegd. Nu komt er nog het TCP en UDP bij.

Laag 5, 6 en 7 kunnen worden beschouwd als de “applicatielagen”.

Zo werkt het TCP-UDP protocol

In tegenstelling tot UDP, is TCP niet bericht- maar verbinding-georiënteerd. Wanneer de verzender data verstuurt naar de ontvanger, kan de ontvangende computer een signaal geven zodra het bericht aankomt. Tegelijkertijd kan de ontvanger ook data terugsturen naar de verzender. Dit betekent dus dat bij UDP packet loss kan optreden (verlies van informatie) zonder dat de lost packets opnieuw worden verstuurd. In de meeste gevallen is dit geen ramp, maar bij belangrijke informatie moet het bestand heelhuids aankomen. Bij streaming services wordt daarom UDP gebruikt omdat deze sneller is en niet elke keer checkt of alles aan is gekomen. Mocht er een pakket loss optreden dan wordt dit waargenomen als een vermindering in de video kwaliteit.

2.3 DHCP EN EEN STATISCH IP-ADRES

Bij het opzetten van een netwerk kun je een IP-adres laten toewijzen door een DHCP server (Dynamic Host Configuration Protocol). Je kan het adres ook zelf handmatig (statisch) instellen. Bij het handmatig instellen maak je gebruik van een statisch IP-adres dat niet verandert.

2.3.1 DHCP

Een DHCP server is een computerprotocol dat beschrijft hoe een computer dynamisch zijn netwerkinstelling van een DHCP-server kan verkrijgen. Dit houdt in dat de volgende informatie wordt verzonden aan het apparaat dat zich bij het netwerk wil aansluiten:

- IP-adres
- subnetmasker
- router
- DNS
- “optionele informatie”

Deze informatie is nodig om een verbinding tot stand te brengen.

2.3.2 STATISCH IP-ADRES

Je kan het IP adres ook zelf handmatig (statisch) instellen. Hierbij moet je alles zelf configureren wat handig kan zijn voor een server. Dit komt omdat je wilt voorkomen dat het IP-adres van een server veranderd. Dit kan resulteren in een verbinding die niet meer werkt doordat een client een IP-adres wilt bereiken dat is veranderd.

Dit is overigens wel op te lossen door middel van een DNS server maar kan in sommige omstandigheden averechts werken doordat iets niet goed is ingesteld, bovendien vereist een DNS extra configuratie. In de demo maak ik daarom - waar dat kan - gebruik van een statisch adres.

2.4 NAAM IN PLAATS VAN IP-ADRES

Wij mensen kunnen IP adressen niet goed onthouden en IP adressen willen nog wel eens veranderen. Het is dus erg vervelend om iedere keer een IP adres in te typen wanneer je bijvoorbeeld google wilt bezoeken. Hierop is iets bedacht, namelijk domeinnamen. Hierbij heb je een vaste naam die niet verandert. Maar mocht het IP adres toch veranderen is dat geen probleem, want

de domeinnaam is gelinkt aan de server dus wordt je naar het juiste IP adres verwezen. Je domein naam is dus de “postcode en nummer van je huis”.

2.4.1 DNS SERVER

Maar hoe komt de computer nu terecht op de juiste website? Hierbij wordt er gebruik gemaakt van een DNS-server (Domain Name System). Wanneer jij google.com intypt wordt de DNS-server gevraagd welk IP-adres hierbij hoort. Dit noemt men ook wel “forward lookup” en zo kom je terecht op de juiste site. Wanneer je van een IP-adres naar de domeinnaam gaat noem je dit “reverse lookup”.

De data van een DNS wordt opgeslagen in een resource record. Veel gebruikte records zijn:

- A voor het bepalen van het IPv4-adres bij een naam;
- AAAA voor het bepalen van het IPv6-adres bij een naam;
- MX (mail exchanger) voor het bepalen van de mailservers voor een domein, waarbij elke mailserver een eigen prioriteit toegewezen krijgt;
- NS (name server) voor het aangeven welke nameservers de authoritative nameservers zijn (ook gebruikt voor het verwijzen naar andere nameservers);
- SRV (Service) wordt gebruikt om services aan te duiden.

Een public IP-adres kan veranderen, maar dit komt niet vaak voor en is onhandig wanneer je een server wil hosten. In mijn geval is het public IP-adres in 3 jaar niet veranderd. Mocht het wel veranderen dan kan gebruik worden gemaakt van een DDNS (Dynamic Domain Name System). Dit is een service die op het netwerk zit. Wanneer een wijziging in het public IP wordt gedetecteerd, wordt deze wijziging doorgestuurd naar een DNS-server.

Veel computers maken gebruik van DNS cache resolvers. Dit houdt in dat veel bezochte websites woorden onthouden door het operating systeem. Dit houdt in dat wanneer je een website vaak bezoekt, het operating systeem het bijbehorende IP onthoudt. Dit zorgt ervoor dat niet elke keer de DNS server moet worden gevraagd om een IP adres te sturen. Dit is handig om websites sneller in te laden en vermindert de processnelheid van een DNS server.

2.4.2 DOMEINNAAM

Bij een domein is een onderscheid te maken tussen een sub domein en een domein. Als voorbeeld neem ik somtoday.nl. Als je dit intypt kom je terecht op de site van Somtoday. Somtoday.nl wordt dan het domein genoemd. Als je hebt “rijnlandslyceum-elo.somtoday.nl” wordt dit het subdomein genoemd. Dit komt doordat “rijnlandslyceum-elo” een sub domein onder het domein “somtoday.nl” is. Je zou kunnen zeggen dat “somtoday.nl” het dak is en “rijnlandslyceum-elo” een etage.

Dus wanneer je een link bezoekt op internet en je ziet 2 puntjes dan weet je dat het een subdomein is dat wordt beheerd door de organisatie van dat domein.

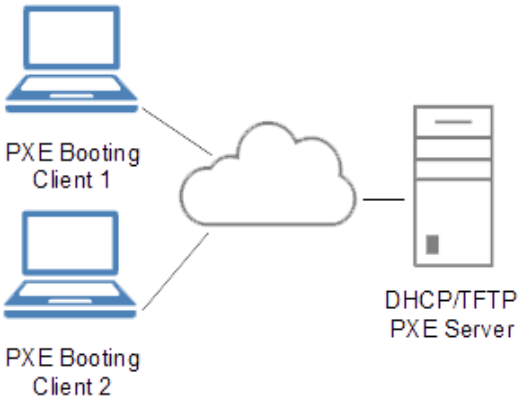
Bijvoorbeeld: “https://rijnlandslyceum-elo.somtoday.nl/home/news”. De streepjes (/) zijn de locaties (kamers) op de etage.

2.5 NETWERK BOOT

Een netwerkboot is een manier om zonder een opstart usb stickje toch te kunnen opstarten vanaf een computer. Dit is handig bij grote organisaties, want dan hoef je alleen de computer op te starten en hoef je niet elke keer een usb/cd te verplaatsen. Ook kan gebruik worden gemaakt van een netwerkboot wanneer je bijvoorbeeld WOL (Wake-on-LAN) wil opstarten (booten) en hij automatisch een “remote management interface” moet opstarten en Windows is bijvoorbeeld niet geïnstalleerd.

Bij een netwerkboot wordt er gebruik gemaakt van PXE (Preboot Execution Environment). PXE maakt gebruikt van TFTP (Trivial File Transfer Protocol). TFTP is de uitgeklede versie van FTP (File transfer protocol). Dit resulteert in een aantal extra mogelijkheden, onder andere makkelijker gebruik maken van SSL (Secure Sockets Layer) en TLS (Transport Layer Security).

Het inladen van een programma gebeurt als volgt. Tijdens een netwerkboot wordt door de DHCP-server een PXE-server IP doorgegeven. Vervolgens worden opstart-bestanden via TFTP overgebracht en kan de computer opstarten vanaf een opstart bestand.



afbeelding 3: schematische weergave van netwerkinstallatie

3 HYPERVISOR

Een hypervisor is een operating systeem zoals Windows, Linux en IOS maar met aanpassingen, waardoor de hypervisor zogeheten VM (virtual machines), containers en andere handige programma’s geïsoleerd kan laten afspelen. Natuurlijk zijn IOS (iPhone operating system), Linux en Windows compleet verschillend in wat ze kunnen. Maar het basisprincipe is hetzelfde. Dit is namelijk het mogelijk maken van communicatie tussen hardware en programma’s. De reden waarom het handig is om programma’s en operating systemen te isoleren is vrij simpel, namelijk het realiseren van goede beveiliging en het bereiken van efficiëntie.

Stel je hebt één server met daarop webservers, gebruikers data, bestanden en andere gegevens en deze server wordt via een backdoor overgenomen door een hacker, dan heb je een groot probleem. Je hebt in één keer alles aan de aanvaller gegeven. Dit wil je ten koste van alles voorkomen. Naast dit probleem zijn in een bedrijf altijd risico’s op gebruikersfouten. Dit houdt in dat wanneer een administrator “per ongeluk” adware, malware, RAT (remote access trojan) of ransomware op de server start, dit kan leiden tot aanzienlijke beveiligingsinbreuken. Het is dus niet de bedoeling dat alles in één keer wordt aangevallen en overgenomen en daarom wordt er gebruik gemaakt van VM’s.

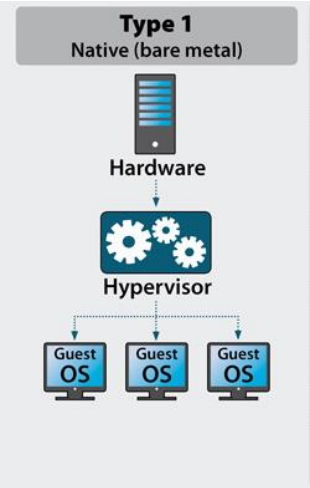
Het andere probleem is dat sommige services beter op Linux werken dan op Windows. Door een hypervisor kun je gemakkelijk webservers op Linux laten draaien en specifieke programma’s voor Windows op een Windows VM (virtual machine) laten afspelen. Daarnaast heb je het voordeel dat je gemakkelijk back ups kan maken. Redenen genoeg dus om gebruik te maken van een hypervisor.

3.1 HYPERVISOR STRUCTUREN

Bij een hypervisor zijn er 2 verschillende soorten hypervisors, namelijk type 1 en type 2. In deze paragraaf zal ik toelichten wat deze inhouden.

3.1.1 TYPE 1 HYPERVISOR

Een hypervisor maakt het mogelijk om meer dan één operating systeem op een computer te laten afspelen. Dit kan op twee manieren. Je kan hardware virtueel maken en vervolgens deze hardware gebruiken om een operating systeem te installeren. Of je kan direct het operating systeem laten communiceren met de hardware. Het direct laten communiceren van een virtuele machine met de hardware noem je een *type 1 virtueel machine*. Dit gaat dan niet volledig direct, maar via de Kernel[3]. De communicatie maakt dan gebruik van de host Kernel. Het voordeel hiervan is dat alles sneller en efficiënter gaat. Het nadeel is dat het makkelijker zou kunnen zijn om door middel van een exploit[4] uit de virtueel machine te breken en andere virtual machines aan te vallen. Is dit het risico waard om te nemen? Ja, want dit risico is nooit volledig te vermijden en er zullen altijd beveiligingsbreuken overblijven die kunnen worden misbruikt in zowel het hypervisor type 1 als 2.



afbeelding 4: schematische weergave van type 1 hypervisor

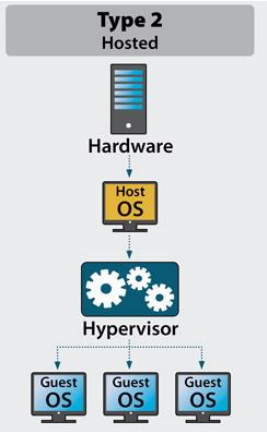
Naast het gebruik maken van een virtual machine kun je gebruik maken van PLCe passthrough (Peripheral Component Interconnect Express). Dit houdt in dat de hardware die geïnstalleerd is in PLCe slot niet communiceert met de Kernel van de host maar direct met de Kernel van de virtual machine.

Een type 1 hypervisor kan worden geïnstalleerd om te functioneren als een eigen operating systeem zoals Proxmox, xenserver of VMware Esxi. Deze operating systemen kunnen dan gebruik maken van QEMU (Quick EMUlator), LXC (Linux Container) of KVM (Kernel-based Virtual Machine). Dit zijn verschillende manieren om programma's geïsoleerd te laten afspelen.

[3] Een kernel of core is het centrale deel van een besturingssysteem. De kernel is, simpel gezegd, de supervisor (opzichter) in een besturingssysteem.
[4] Een exploit is een stukje software die gebruik maakt van een bug, glitch of kwetsbaarheid in de software van een apparaat om ongewenst gedrag te veroorzaken op de software of hardware van dat apparaat.

3.1.2 TYPE 2 HYPERVISOR

Een type 2 hypervisor is langzamer dan een type 1 hypervisor. Dit komt doordat een type 2 hypervisor altijd moet worden geïnstalleerd boven op een bestaand operating systeem zoals Windows of Linux. De hypervisor wordt dan door het operating systeem gezien als traditioneel software en geeft zo nodig computer resources aan het programma. In dit geval moet gebruik worden gemaakt van drivers die kunnen worden opgeroepen om hardware voor de VM te virtualiseren. Nadat deze hardware is gevirtualiseerd kan een operating systeem worden geïnstalleerd. Over het algemeen wordt een type 2 hypervisor veel gebruikt door de consument om bijvoorbeeld een Windows installatie uit te testen of een oud spel te spelen, dat niet werkt op de nieuwste Windows versie.



afbeelding 5: schematische weergave van type 2 hypervisor

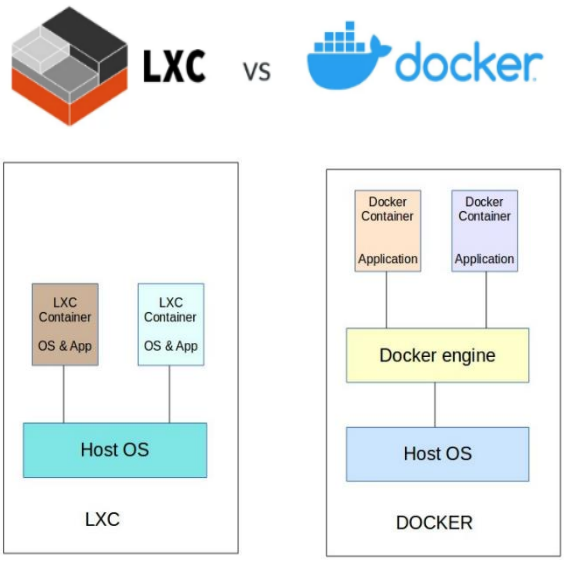
3.2 OPTIES VOOR HYPERVISORS

Het is niet handig wanneer je een programma geïsoleerd wilt laten afspelen, om een nieuwe Linux installatie voor dit programma te hebben. Eerder heb ik verteld hoe een type 1 hypervisor efficiënter werkt. Dit kan nog een stapje verder worden gebracht met behulp van “containers”.

3.2.1 HYPERVISOR EFFICIENTER LATEN WERKEN DOOR CONTAINERS

Om computer resources te verminderen kan gebruik worden gemaakt van een LXC of een docker container. Dit is handig om services en programma’s te isoleren van een operating systeem zonder dat een nieuw operating systeem hoeft te worden geïnstalleerd op een VM.

Er zit wel een groot verschil in LXC en docker. LXC kan directer met de host communiceren dan docker en dit resulteert in snellere services. Docker maakt namelijk gebruik van een “docker engine” waardoor de efficiëntie wordt verhoogd en de computer resources omlaag gaan, maar de snelheid gaat hierdoor ook een beetje omlaag. In mijn geval heb ik veel gebruik gemaakt van LXC, omdat deze ingebouwd was in de hypervisor die ik heb gebruikt.



afbeelding 6: LXC vs DOCKER

Een hypervisor kan erg verschillend zijn en het is daarom belangrijk voor een bedrijf om te weten wat in dat geval beter of slechter werkt. Een groot bedrijf kan namelijk gebruik willen maken van clusters en een klein bedrijf niet. De één wil alleen Windows virtual machines, de andere wil lichte Linux containers. In mijn geval heb ik gekozen voor de Proxmox hypervisor omdat deze opensource is. Naast de opensource licentie bevat de hypervisor handige onderdelen zoals LXC, backups, snapshots, KVM en cluster.

4 WINDOWS SERVER

afbeelding 7: Windows logo

Een goede manier om computers met Windows te beheren is met het besturingssysteem “Windows server”. Windows server geeft de mogelijkheid om veel dingen te beheren zoals deployment services, DNS, domain directory en group policies. Op de markt zijn veel alternatieven zoals bijvoorbeeld Mac OS server. Maar in geval van Mac OS server moeten alle computers in een organisatie MAC OS bevatten. Dit zou erg nadelig zijn doordat niet alle programma’s goed werken op MAC OS. Bovendien zijn iMac en macbook pro’s (laptops) erg duur en vervalt de ondersteuning snel voor deze producten. Ik heb dan ook geen enkel moment aan een alternatief voor Windows server gedacht toen ik een infrastructuur thuis ging opzetten. Een alternatief past ook niet bij het gebruikte systeem op school.

In dit hoofdstuk ga ik een aantal Windows server onderdelen bespreken die worden gebruikt om werkstations te kunnen beheren.

4.1 DOMAIN CONTROLLER

Een domain controller is de server waar de domein instellingen worden bewaard. Vaak betreft dit ook de DNS server, maar de DNS server kan ook op een andere plek worden opgezet. Als een organisatie groot is kan deze meerdere domain controllers hebben voor redundantie. In deze paragraaf ga ik een aantal services bespreken die nodig zijn om een Windows domain controller functionerend te krijgen.

Om een werkend Windows domein te maken zijn onder andere de volgende services nodig:

- LDAP (Lightweight Directory Access Protocol)
- Active directory
- Group policy

Ik licht deze toe in de volgende paragrafen.

4.1.1 LDAP

Windows server maakt gebruik van het zo geheten LDAP (Lightweight Directory Access Protocol). Hiermee kun je gegevens uitwisselen van de server naar werkstations. Zo kan bijvoorbeeld een werkstation weten wie toegang heeft tot dat werkstation en wat deze persoon wel en niet mag (autorisaties). LDAP is de service die onder meer wordt gebruikt voor de AD (active directory) maar ook voor mailservers, webservers en remote acces programma’s. Hiermee kun je bijvoorbeeld Chromebooks beheren. LDAP is dus de service die andere services met elkaar verbindt om informatie met elkaar te kunnen uitwisselen.

4.1.2 ACTIVE DIRECTORY

Active Directory is een database waarin informatie wordt opgeslagen zoals gebruikersrechten. De hoofdmap in een Active directory wordt DC (Domain Component) genoemd in. In deze DC heb je onderliggende mappen die OU (Organizational Unit) worden genoemd. Hierin kun je computers gebruikers/groepen toevoegen. Wanneer je een gebruiker toevoegt wil je dat deze niet alles kan doen. Daarom maak je gebruik van gebruikersrechten. Hiermee kun je leerlingen onderscheiden van docenten, waarbij ieder eigen gebruikersrechten krijgt toegewezen. Om dit goed te laten werken wordt gebruik gemaakt van gebruikersgroepen. Dit houdt in dat wanneer er een nieuwe gebruiker wordt aangemaakt in de leerling-groep, deze leerling niet kan inloggen op een werkstation voor docenten. Andersom geldt dat wanneer een docent een docentenrol krijgt de docent wel in de leerling-groep kan. Deze groepspermissies kun je (naast het instellen van inlog restricties) ook gebruiken om bepaalde instellingen door te voeren voor bepaalde gebruikers zonder elke gebruiker apart te veranderen. Hiernaast is het ook mogelijk om groepen toegang te geven tot map shares, Citrix werkstations en VPN services.

Member of:

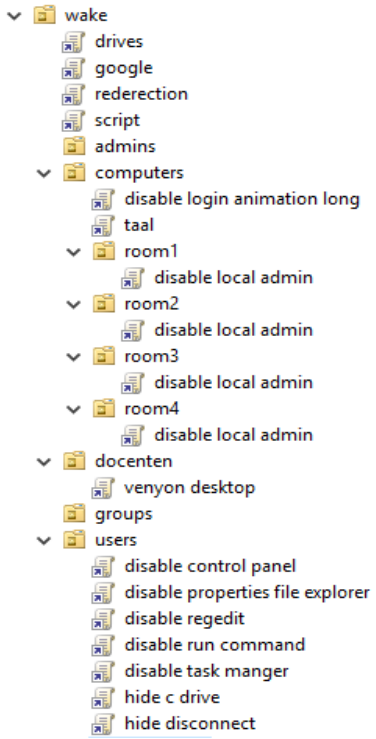
Name	Active Directory Domain Services Folder
Domain Users	wake.up/Users

afbeelding 8: AD groepsinstelling

4.1.3 GROUP POLICY

Group policy zorgt ervoor dat gebruikers bepaalde instellingen krijgen, waardoor zij bepaalde dingen wel of juist niet kunnen. Er zijn veel instellingen op een computer mogelijk en daarom kunnen binnen de group policy ook vele aanpassingen plaats vinden. Als deze vele mogelijkheden niet genoeg zijn kan je ook nog extra templates van internet downloaden voor nog meer aanpassingen.

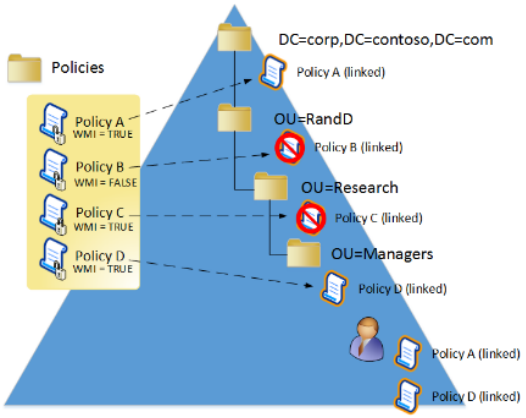
Op de afbeelding rechts heb ik een aantal policies weergegeven die ik voor mijn infrastructuur gebruik. In sommige gevallen gebruik ik onder één policy meerdere instellingen zoals redirections, snelkoppelingen, data en tijdinstellingen. Hiermee kan je roaming profiles instellen, die dan te gebruiken zijn in combinatie met folder redirections. Hiermee kun je de Windows server gebruiken om bestanden te laten synchroniseren en op deze manier automatische bestanden van één plek naar een andere plek over te brengen. Op deze manier hoeft niemand een usb stick mee te nemen om zijn bestanden op te slaan, maar maakt diegene gebruik van het SMB (Server Message Block) protocol. SMB wordt niet alleen gebruikt voor bestanden, maar ook om instellingen door te voeren zoals policies, user groups en scripts.



afbeelding 9: groep policy's

Om onderscheid te maken in welke policies voorrang hebben boven anderen, wordt gebruik gemaakt van een “policy tree”. Dit zorgt ervoor dat policy A wordt toegepast op alle onderliggende objecten, terwijl policy C alleen wordt toegepast op de Organizational Unit Research. Wanneer er dezelfde instellingen in een policy staan geldt datgene dat het dichtst bij het Organizational Unit ligt.

WMI (Windows Management Instrumentation) is voor de verdere uitleg van de policy tree niet van belang.

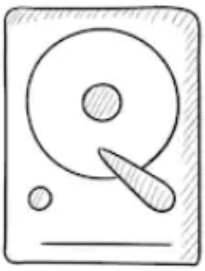


afbeelding 10: group policy tree

4.2 OPSLAG

Een gebruiker kan op verschillende manieren opslag worden toegekend. De meest makkelijke manier is het verplichten van het gebruik van een usb stickje aan alle gebruikers. Dit zou echter niet erg praktisch zijn.

Een andere manier is het opzetten van een NAS (Network-attached storage). Hiermee wordt de informatie op een server opgeslagen en kan de gebruiker vanaf elke computer binnen het netwerk diens informatie bereiken. Het opslaan van informatie over het netwerk kan op verschillende manieren worden gedaan zoals SMB/CIFS (Common Internet File System) en NFS (Network File System). Hiernaast moet worden gekeken hoe belangrijk de informatie is en hoeveel opslag een gebruiker mag hebben.



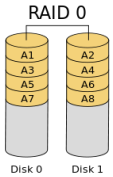
afbeelding 11: schematische weergave van een harde schrijf

4.2.1 OPSLAG VEILIGER MAKEN

Er zijn verschillende manieren om informatie te beschermen tegen een harde schijf die kapot gaat. Een veel gebruikte methode is RAID (Redundant array of independent disks). Dit zorgt ervoor dat - terwijl je informatie op een schrijf zet - de informatie wordt verdeeld over meerdere schijven. RAID kan worden geconfigureerd naar behoefte van de gebruiker. Afhankelijk van wat de gebruiker wil moet er een afweging gemaakt worden tussen opslag/redundantie/snelheid. Voor een configuratie kan worden gekozen tussen hardware of software RAID. Beide manieren hebben voor- en nadelen. Met een hardware RAID heb je een RAID kaart nodig en bij een software RAID niet.

Een voorbeeld van software RAID is ZFS (Zettabyte Filesystem). ZFS zelf is niet een software raid maar een filesysteem. ZFS kan wel worden gebruikt om een RAID op te zetten. Bij het kiezen van een RAID kan worden gekozen tussen bijvoorbeeld RAID-0, RAID-1 en RAID-5.

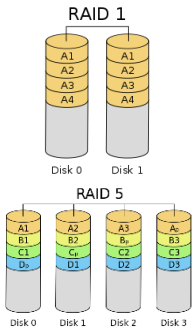
- RAID-0 is een configuratie waarbij informatie in kilobyte blokken wordt verdeeld over de schijven. Het voordeel dat hiermee ontstaat is de snelheid. Deze gaat namelijk omhoog doordat meerdere schijven tegelijk worden gebruikt. Het nadeel is echter bij een schijffout heb je kans dat alle informatie verloren gaat.



- RAID-1 is een configuratie waarbij de schrijf één op één wordt gekopieerd. Hierdoor krijg je de snelheid van 1 schijf maar tevens het voordeel dat, als één schijf kapot gaat de informatie veilig blijft.

- RAID-5 is een configuratie waarin de leessnelheid omhoog gaat en één van de schijven kapot kan gaan zonder dat er informatie verloren gaat.

Naast deze voorbeelden zijn er nog veel meer opties maar voor de doelgroep moet worden gekeken of snelheid/opslag/redundancy belangrijk zijn. Afhankelijk daarvan kan een keuze worden gemaakt welke RAID configuratie moet worden gebruikt.



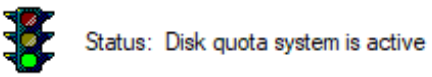
afbeelding 12: schematische weergave van RAID-0, 1 en 5

4.2.2 NETWERK SCHIJVEN

Een netwerkschrijf is een schijf waar informatie kan worden opgeslagen, terwijl de informatie niet op de computer staat. Naast zelf een opslagserver te maken is het ook mogelijk een bedrijf te betalen voor de benodigde opslag. Het voordeel is dat jezelf minder beheer hoeft uit te voeren maar het nadeel is dat je afhankelijk bent van het bedrijf waar je de opslag hebt liggen (en het kost uiteraard geld). In Windows wordt de netwerk opslag aangeduid met \\domain.com. Dit is meestal niet buiten het LAN bereikbaar omdat er anders een verhoogde kans zou bestaan op een beveiligingsbreuk.

4.2.2.1 SCHIJF QUOTA

Een schijfquota is een configuratie waarmee je de opslag van de schijf virtueel opsplitst. Hiermee kun je het aantal opslag per gebruiker instellen. Je wilt niet dat één gebruiker de hele schijf vol met informatie schrijft. Dit zou immers betekenen dat andere gebruikers minder opslagcapaciteit hebben. Quota lost dit probleem op door een limiet aan opslag per gebruiker toe te staan. Dit kan per gebruiker worden ingesteld of op groepsniveau. Wanneer dit op groepsniveau wordt ingesteld, zullen nieuwe gebruikers automatisch een maximale opslagcapaciteit toegewezen krijgen.



afbeelding 13: icoon van wanneer disk quota actief is

4.3 UITROLLEN VAN WINDOWS INSTALLATIES

In deze paragraaf leg ik uit hoe een Windows installatie met alle benodigde programma's over het netwerk kan worden geïnstalleerd. Het voordeel van Windows installaties uitrollen via het netwerk is dat de efficiëntie van updates wordt verhoogd. Bovendien hoef je niet elke computer apart te configureren, maar wordt dit automatisch voor de administrator gedaan.

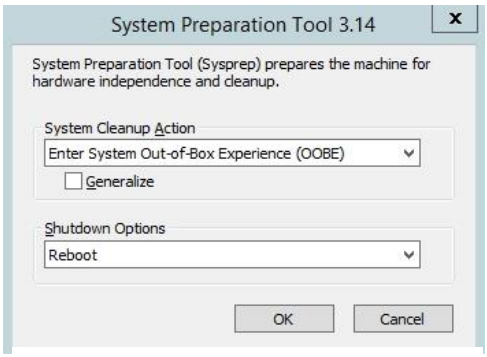
4.3.1 OPZETTEN VAN MICROSOFT DEPLOYEMENT TOOLKIT

MDT (Microsoft Deployement Toolkit) is een toolkit aangeboden door Windows om het uitrolproces te versoepelen. In dit programma kun je veel aanpassingen maken om de installatie naar behoefte aan te passen. Naast het aanmaken van een uitrol netwerkschijf wordt gebruik gemaakt van de WDS (Windows Deployment share). Deze service zorgt voor de uiteindelijke uitvoer van de netwerkboot en maakt gebruik van het TFTP (Trivial File Transfer Protocol). Dit is een eenzijdige verbinding over

UDP. Nadat instellingen zijn ingesteld in MDT kan een opstart disk (LiteTouch) worden gemaakt. Deze opstart disk wordt gebruikt door WDS om een image op de computer te installeren, die is gemaakt door Sysprep.

4.3.1.1 VASTLEGGEN VAN WINDOWS IMAGE DOOR SYSPREP

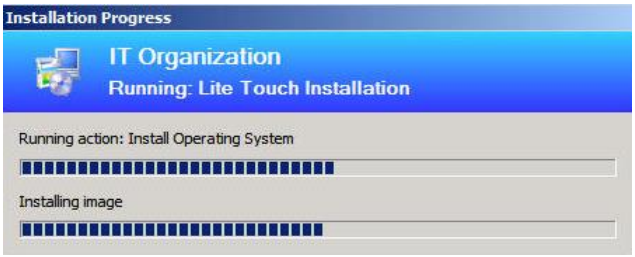
Voordat een Windows image kan worden geïnstalleerd moet deze eerst worden voorbereid. Dit wordt gedaan door het programma “Sysprep”. Sysprep zorgt er voor dat de installatie in OOBE (Out-of-box experience) wordt gezet. Het voordeel hiervan is dat onnodige informatie wordt verwijderd, zodat de Windows image wat betreft de bestandsgrootte niet te groot wordt. Nadat de image is voorbereid kan deze worden gebruikt in MDT om een configuratie op te zetten.



afbeelding 14: Sysprep programma

4.3.2 DEPLOYEN VAN WINDOWS IMAGE

De uitrol van Windows gebeurd via een netwerkboot. Tijdens de installatie kunnen er nog kleine aanpassingen gedaan worden en daarna wordt de computer geïnstalleerd met alle benodigde informatie. Nadat de installatie voltooid is kan worden ingelogd op de computer.



afbeelding 15: Deployment van image

5 COMPUTER INFRASTRUCTUUR OP HET RIJNLANDS LYCEUM WASSENAAR EN THUIS

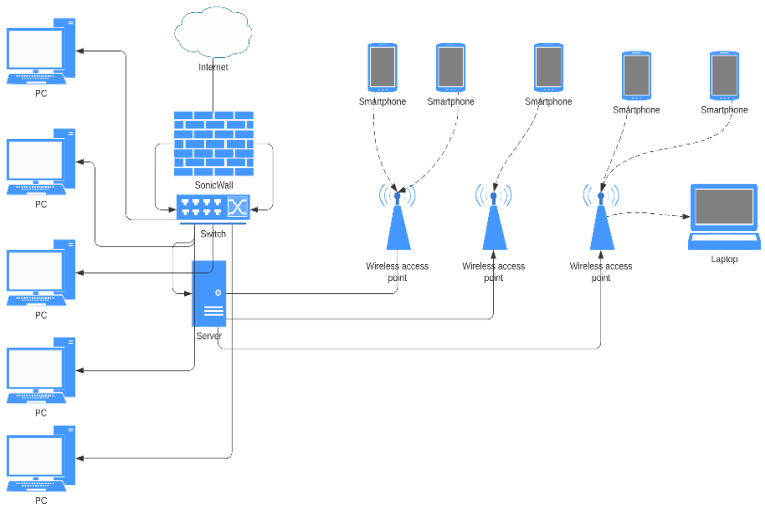
In dit hoofdstuk beschrijf ik de onderdelen die ik ben tegen gekomen op mijn school RLW (het Rijnlands Lyceum Wassenaar). Alles wat komt kijken bij deze beschrijving is gebaseerd op aannames, omdat ik niet een uitgebreide studie heb kunnen maken van de infrastructuur van het RLW. Tijdens het willen observeren van de infrastructuur op het RLW ben ik tegen een probleem opgelopen. Covid-19 heeft er namelijk voor gezorgd dat de school en dus ook de mediatheek gedurende langere tijd (5 maanden) was gesloten. Hierdoor heb ik mijn veronderstellingen niet in de praktijk van het RLW kunnen toetsen in een voorgenomen gesprek met de IT-beheerder van school. Daarom heb ik een inschatting gemaakt van de verschillende onderdelen die in die infrastructuur zijn gebruikt. Hieruit kan ik analyseren hoe de infrastructuur op het RLW zal zijn opgebouwd.

In de tweede paragraaf beschrijf ik wat ik thuis heb nagebouwd naar aanleiding van de veronderstellingen die ik in de eerste paragraaf beschrijf.

5.1 INFRASTRUCTUUR RLW

Het netwerk van het RLW is als volgt opgebouwd.

Het internet komt binnen in de SonicWall box. Hieruit wordt de verbinding verdeeld over verschillende switches. Vanuit deze switches zorgen verschillende WAP's (wireless access point's) dat de wifi verbinding vergroot wordt. Als een gebruiker wil inloggen worden LDAP services gebruikt om toegang aan de gebruiker te geven.



afbeelding 16: Schematische weergave van RLW netwerk

Hiernaast wordt een root certificatie verplicht gesteld, zodat onder andere DNSBL (DNS BlackList redirecties) kunnen worden toegepast zonder dat er certificaat foutmeldingen worden afgegeven. Alle chromebooks maken ook gebruik van LDAP. Hiermee kunnen de instellingen worden beheerd van deze chromebooks. Voor de verbindingen zijn bijna alle porten geblokkeerd. Ook de DNS kan niet worden aangepast, doordat andere DNS (servers) worden geblokkeerd (behalve de lokale servers). DNSBL en IP-Blocklists worden beheerd door SonicWall. Het overgrote deel van de Windows services liggen buiten het netwerk en worden door middel van een VPN met het netwerk in verbinding gezet.

Het Rijnlands Lyceum heeft 7 vestigingen. Elke vestiging stelt eigen eisen en heeft dus andere computer instellingen nodig. Het bijbehorende infrastructuur netwerk is dus telkens anders ingedeeld.

Om de instellingen en printers te beheren wordt gebruik gemaakt van Ivanti workspace control. Om docenten mee te laten kijken met leerlingen wordt gebruik gemaakt van iTalc. Voor de Windows deployment wordt PXE (Preboot Execution Environment) gebruikt om Windows te kunnen installeren.

Wat opvalt is dat er geen gebruikersnaam of wachtwoord hoeft te worden opgegeven tijdens een installatie. Dit is vanuit een beveiligingsperspectief een niet verstandige keuze. Wel een verbetering is dat de BIOS (Basic Input-Output) met een wachtwoord beschermd is. Dit was voorheen namelijk niet het geval. Voor de VDI (Virtual Desktop Infrastructure) wordt Citrix gebruikt. Alle Citrix desktop sessies worden buiten het Rijnlands lyceum gehost.

In de omgeving van Citrix is alles tijdelijk opgezet. Dit houdt in dat aanpassingen aan de lokale schijf na herstart worden verwijderd. De omgeving is alleen te bereiken vanuit het RLW netwerk. Dit is gedaan om de beveiliging te verbeteren. Voor opslag gebruikt het Rijnlands Lyceum OneDrive en SMB om instellingen in te laden. Deze instellingen worden ingeladen met behulp van roaming profiles en Ivanti workspace.

Om alles overzichtelijk te maken heb ik de volgende tabel gemaakt van de infrastructuur op RLW (zie de afkortingenlijst voor een toelichting op de afkortingen).

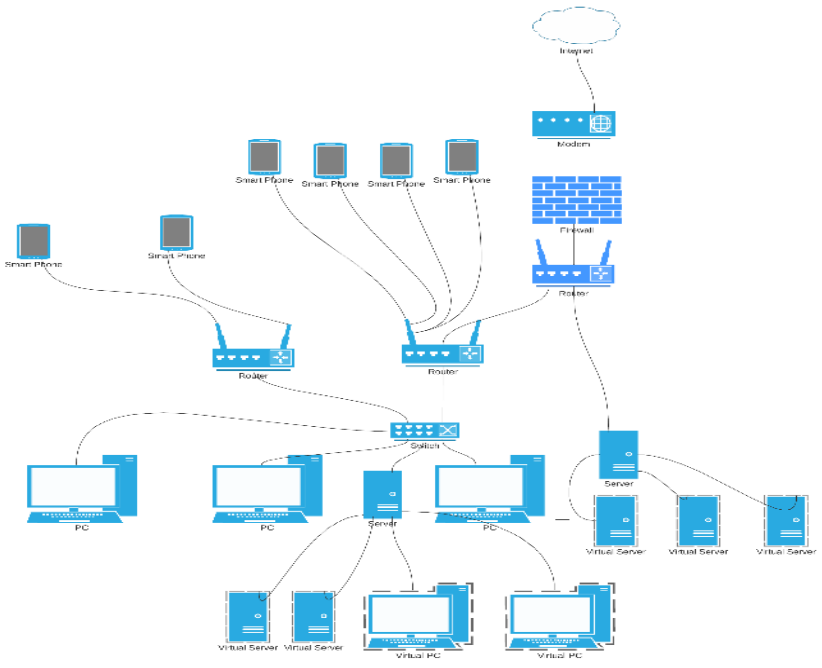
Tabel infrastructuur RLW:

Firewall	SonicWall, DNSBL, IP-Blocking, traffic shaping
Windows-Server	DNS, AD, deels buiten netwerk
Wifi-verbinding	LDAP, certificaat, WAP
Beheer van werkstations	ITalc, Ivanti workspace control
Virtual Desktop Infrastructure	Citrix, XenServer
Opslag	OneDrive, SMB, NFS, roaming profiles
netwerkinstallatie	WDS, MDT, PXE

5.2 INFRASTRUCTUUR THUIS

Thuis heb ik het netwerk als volgt opgebouwd.

Het internet komt binnen via een coax kabel en wordt omgezet door een modem naar een ethernet verbinding. De modem staat in bridge modus. Hierbij worden alle functies uitgezet en werkt alleen de eerste ethernet port. De ethernet kabel gaat vervolgens van de modem naar de pfSense box. Op de pfSense box zijn de benodigde instellingen ingesteld zoals TFTP, DHCP, DNSBL en NAT.



afbeelding 17: Schematische weergave van mijn thuisnetwerk

De verbinding wordt opgesplitst in twee verschillende LAN interfaces. Eén dient als thuisnetwerk en de andere dient als gedeeltelijke DMZ (Demilitarized zone). Voor verbindingen met WAP's wordt geen LDAP of root certificaat uitgegeven. Doorverwijzingen van DNSBL worden dan ook met een foutmelding beantwoord. Deze blokkeert overigens wel de niet toegestane websites, zoals spellen. Naast DNSBL worden IP-Blocks ook door pfSense uitgevoerd. In het opgezette thuisnetwerk is geen rekening gehouden met Chromebooks, maar wel met laptops of andere werkstations. Alleen lokale DNS (servers) werken en Windows services worden binnen het netwerk gehost.

In mijn thuisnetwerk heb ik twee hypervisors, namelijk Proxmox en Esxi. De Esxi server is toebedeeld aan het werkend maken van een Cloud desktop omgeving. De Proxmox server wordt gebruikt om een lokale werkstation te kunnen gebruiken. DNS, AD, WDS, MDT en E.T.C worden in een VM van Proxmox uitgevoerd. PXE boot kan worden uitgevoerd zonder wachtwoord op te geven tijdens gebruik van LiteTouch installatie. De BIOS van de werkstations zijn met een wachtwoord beschermd. Voor de VDI is VMware Horizon gebruikt. Deze werkt namelijk samen met ESXI. Een eigen domeinnaam - in combinatie met CloudFlare - is gebruikt om een SSL (secure socket layer) certificaat te krijgen.

De volgende tabel geeft de infrastructuur in mijn thuisnetwerk aan.

Tabel infrastructuur thuisnetwerk:

Firewall	pfSense, DNSBL, NAT, IP-Blocking
Windows-Server	Binnen netwerk, DNS, AD
Wifi-verbinding	Twee WAP's
Beheer van werkstations	Venyon,
Virtual Desktop Infrastructure	Horizon, Esxi, Instant cloning,
Opslag	SMB, roaming profiles
netwerkinstallatie	WDS, MDT, PXE

5.3 RLW VERGELEKEN MET THUIS

Wat zijn nu de overeenkomsten en vergelijkingen tussen het RLW en wat ik thuis heb gebouwd? Welke keuzes heb ik gemaakt en op welke afwegingen zijn deze keuzes gebaseerd om thuis voor bepaalde onderdelen te kiezen?

Om direct een idee te krijgen wat de overeenkomsten en vergelijkingen zijn heb ik de tabellen uit de vorige paragraaf gebruikt. Onderstaande tabel laat in één oogopslag de directe vergelijkingen zien. De tabel bevat de belangrijkste vergelijkingen en begrippen en is dus niet bedoeld om alle onderdelen van het infrastructuurnetwerk compleet weer te geven.

Tabel vergelijking RLW met thuis:

	RLW	**Thuis**
Firewall	SonicWall, DNSBL, IP-Blocking, traffic shaping	pfSense, DNSBL, NAT, IP-Blocking
Windows-Server	DNS, AD, deels buiten netwerk	Binnen netwerk, DNS, AD
Wifi-verbinding	LDAP, CERTIFICAAT, WAP	WAP
Beheer van werkstations	ITalc, Ivanti workspace control	Venyon
Virtual Desktop Infrastructure	Citrix, XenServer	Horizon, Esxi, Instant cloning,

Opslag	OneDrive, SMB, NFS, roaming profiles	SMB, roaming profiles
Netwerkinstallatie	WDS, MDT, deels buiten netwerk	WDS, MDT

De keuzes die ik voor de verschillende onderdelen heb gemaakt zijn te verklaren uit verschillen in de beschikbaarheid van licenties, de bij mij beschikbare tijd om zaken te installeren of de aanwezigheid van voldoende budget voor het al dan niet kunnen aanschaffen van servers, software of bepaalde licenties. Tijdens het opzetten van het infrastructuur netwerk thuis heb ik uit budget overwegingen vaak gekozen voor opensource alternatieven. Ik had immers geen budget beschikbaar om die producten aan te schaffen die wel door het RLW aangeschaft konden worden. Ik heb gebruik gemaakt van Proxmox, Venyon of pfSense: dit zijn open source producten die vrij verkrijgbaar zijn op het internet.

Voor de Cloud omgeving heb ik gekozen voor VM Horizon. Ik heb hiervoor de licentie aangevraagd en gedurende de proefperiode dit pakket geïnstalleerd op mijn computer en gebruikt. Na afloop van de proefperiode verviel de licentie helaas waardoor ik er niet langer gebruik van kon maken.

Eerder was ik al bekend met Esxi. Ik heb daarom gedacht dat het wel makkelijk zou zijn om dit te gebruiken. Hoewel ik dit heb onderschat is het me wel gelukt. Voor extra beheeropties had ik extra moeite kunnen doen door een Ivanti licentie aan te vragen, maar voor wat ik nodig had was dit niet noodzakelijk. In plaats hiervan heb ik meer tijd gestopt in de ontwikkeling van andere onderdelen. Voor group policy heb ik een aantal instellingen van school overgenomen en zelf bedacht. Hierbij valt te denken aan de verborgen schijven, bureaublad-achtergrond, verbergen van de laatste login en het moeten gebruiken van “ctrl + alt + del” bij inloggen.

Hieronder zie je het inlogscherm van het door mij gebouwde cloud omgeving. Door in te loggen kom je in de cloud desktop omgeving van mijn thuisnetwerk[5].

afbeelding 18: Weergave van de door mij gemaakte inlogpagina op mijn thuisnetwerk

[5] Door het verlopen van enkele licenties werkt deze omgeving helaas niet meer, maar kan in het filmpje worden bekeken hoe dit is opgezet.

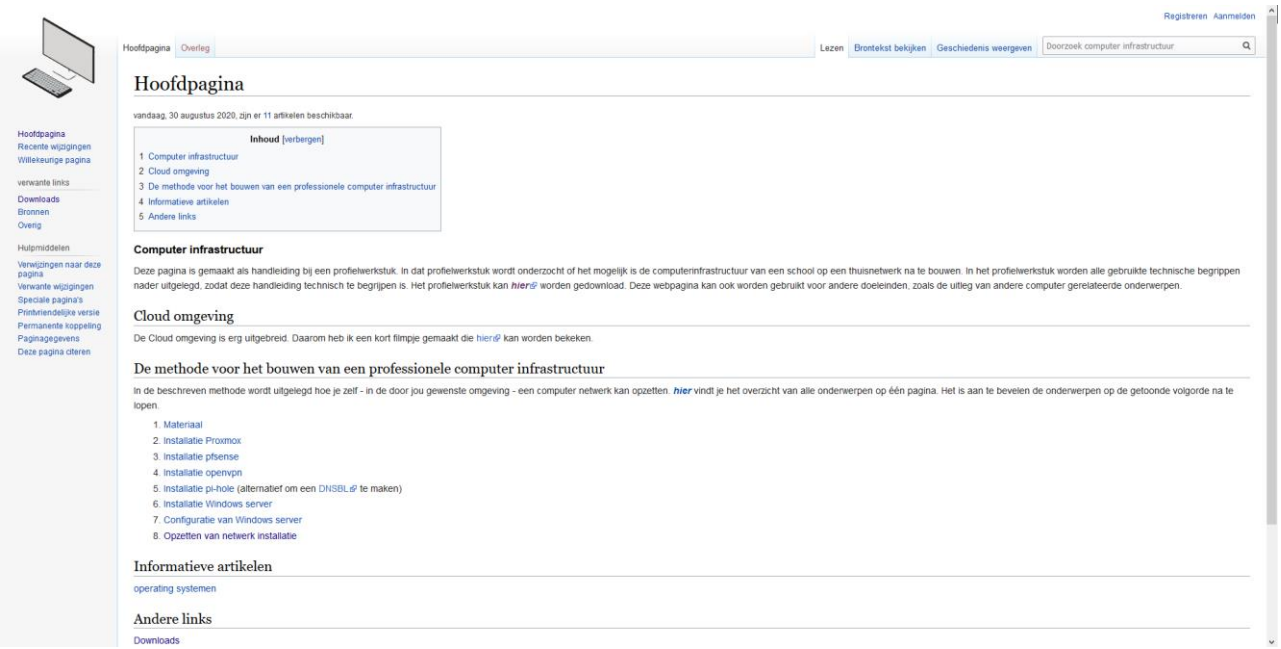
6 OPGELEVERDE PRODUCTEN

Ik heb veel tijd gestoken in het uitzoeken van de wijze waarop thuis een computer infrastructuur opgezet en ingericht kan worden. Ik wilde graag met deze informatie een handleiding of demo maken, zodat anderen ook desgewenst een eigen computer infrastructuur thuis konden nabouwen en dit profielwerkstuk ook een “praktisch product” zou opleveren. Op deze manier kon ik mijn opgedane kennis omzetten in een eigen product. Dit product vormt een onderdeel van dit profielwerkstuk. Dat geldt ook voor het filmpje dat ik van het ontwerpproces heb gemaakt. Tot slot heb ik van de gelegenheid gebruik gemaakt een aantal aanbevelingen te doen om eventueel aan te brengen in de bestaande infrastructuur van het RLW.

6.1 EIGEN WEBSITE

Ik heb een eigen website gemaakt, waarop ik een demo/handleiding heb opgesteld en uitgewerkt om de bouw van een computerinfrastructuur toe te lichten. In het maken van deze website is veel tijd en energie gestopt. Ik verwijs graag naar deze website:

https://computerinfrastructuur.nl/



afbeelding 19: Weergave van de hoofdpagina van mijn website.

Ik heb gebruikt gemaakt van mediawiki als basis voor de website. Op de website heb ik een aantal plug-ins geïnstalleerd, waardoor het werken met de website wordt verbeterd. Hierbij kan gedacht worden aan het gebruiken van mail, een teksteditor en verbeterde opslag voor bijvoorbeeld foto’s.

6.2 YOUTUBE FILMPJE

Naast deze website heb ik een filmpje gemaakt die de VDI (Virtual Desktop Infrastructure) kort uitlegt. Ik laat hierin de inlog pagina zien om in een cloud desktop sessie te kunnen inloggen. Het was mijn bedoeling dat de login zou werken op het moment van het afronden en indienen van mijn

profielwerkstuk. Maar doordat de gebruikte licenties afliepen (vanwege het beëindigen van de proefperiode) voordat het profielwerkstuk werd ingeleverd, werkt de VDI helaas niet meer. Daarom heb ik in plaats van deze login pagina dit korte filmpje gemaakt dat met tekst en beeld uitlegt wat deze omgeving inhoud:

Graag nodig ik de lezer uit dit filmpje te bekijken.

https://www.youtube.com/watch?v=VqIvApjCOGQ

6.3 AANBEVELINGEN VOOR INFRASTRUCTUUR RLW

Tijdens het bouwen van mijn eigen website en het werken aan dit profielwerkstuk ben ik tegen bepaalde punten aangelopen die zouden kunnen worden verbeterd op het RLW. Ik breng daarom ook de volgende aanbevelingen uit aan de beheerder van het IT netwerk van het RLW:

1. *Vervang iTlac door Venyon:*
   Voor remote management gebruikt de school nog steeds iTalc. Op zichzelf is dit geen groot probleem. Het programma heeft alle benodigde functies en doet wat het moet doen. Daarom zal er geen directe noodzaak zijn tot snelle vervanging. Desondanks is het niet erg verstandig om iTalc te blijven gebruiken, omdat iTalc al een tijdlang niet meer geüpdate wordt. Het programma kan makkelijk worden vervangen door het alternatief Venyon. Venyon is gebaseerd op iTalc, dus veel verschil zal er niet zijn. Echter de beveiliging zal zeker worden verbeterd.

2. *Sla alles wat niet belangrijk is op de werkstations op en laat alleen grote programma's op een Cloud desktop afspelen:*
   Er zijn een aantal problemen met de cloud omgeving zoals het ontstaan van vertraging. Op dit moment is het systeem op het RLW niet voldoende geoptimaliseerd om iets simpels als een filmpje te kunnen afspelen. Een oplossing kan zijn alles wat niet belangrijk is te zetten op de werkstations en alleen grote programma's op een Cloud desktop te laten afspelen. Een wat duurdere oplossing, maar wat wel goed zal werken, is gebruik te gaan maken van hardware acceleratie. Xseon platinum cpu's zijn niet gebouwd om meerdere video streams tegelijk te kunnen afspelen en kan om deze reden problemen opleveren.

3. *Een geconstateerd probleem is dat de netwerkschrijf vol zit zonder dat dit echt het geval is:*
   Voor opslag ben ik als gebruiker een aantal keer tegen gekomen dat de netwerkschijf vol zit zonder dat dit het geval was. Dit probleem is niet erg gemakkelijk op te lossen, maar zal waarschijnlijk komen doordat quota niet goed de verwijdering van bestanden afhandelt. Dit is te reproduceren door de netwerkschijf vol te schrijven en daarna alles te verwijderen. Dit moet een aantal keer worden uitgevoerd totdat niet meer op de schijf kan worden bijgeschreven. Er kunnen diverse mogelijke oorzaken voor dit probleem zijn. Zeker in oudere Windows-server versies was dit een veel voorkomend probleem.

4. *Bescherm de toegang tot de harde schijf van het RLW beter:*
   Wat niet erg schadelijk is maar wel vragen oproept is dat het erg gemakkelijk is de harde schrijf van het RLW via een alternatieve route te bereiken om een programma te installeren.

Uiteraard is dit alleen mogelijk met run directories die binnen de programma directory kunnen worden geïnstalleerd.

5. *Limiteer de hoeveelheid te bewaren data per gebruiker op OneDrive:*
   Er is op dit moment binnen het RLW nog geen quota opgezet voor OneDrive, waardoor je deze met data zou kunnen volschrijven. Nu is het risico dat iemand dit wil doen niet zo groot, maar het is zeker aan te bevelen een maximum in te stellen aan de capaciteit die elke gebruiker aan data op de schijf zou mogen opslaan.

7 CONCLUSIE

Ik ga in dit hoofdstuk na of ik de door mij gestelde doelen tijdens het verrichten van mijn onderzoek heb bereikt. Vervolgens beantwoord ik de deelvragen aan de hand van de uitgewerkte hoofdstukken. Tot slot geef ik antwoord op de hoofdvraag uit mijn onderzoek.

7.1 BEREIKTE DOELEN

In het begin van mijn onderzoek had ik mij een aantal dingen ten doel gesteld die ik wilde bereiken. Heb ik deze doelen bereikt?

- De instellingen en documenten van de gebruikers moeten op één server worden gesynchroniseerd, zodat wanneer zij inloggen op een andere computer, zij hun documenten en instellingen automatisch meenemen en instellingen van Chrome moeten ook mee woorden ge-synchroniseert;
  - Gelukt
- Ik wil dat Windows makkelijk kan worden geïnstalleerd via een netwerkboot. Hierdoor kunnen bepaalde programma's en applicaties (zoals printers, permissies, register aanpassingen, taal, group policy etc) worden versoepeld.
  - Gelukt
- Een gebruiker moet kunnen inloggen via de browser zodat die een desktop sessie krijgt toegewezen zoals Citrix;
  - Gelukt
- Ik moet spellen kunnen blokkeren en zien wat wordt gedaan op het netwerk zoals welke websites worden bezocht.
  - Gelukt

Ik kan concluderen dat ik mijn gestelde doelen heb bereikt en dat het mij gelukt is de voorgenomen onderdelen uit te denken en na te maken in mijn thuisnetwerk.

7.2 DEELVRAGEN

Om een antwoord te kunnen geven op mijn onderzoeksvraag[6] heb ik een aantal deelvragen gesteld, welke ik ben gaan onderzoeken en uitwerken. De antwoorden op de deelvragen zijn als volgt:

1. Welke technische onderwerpen en begrippen moet ik begrijpen voordat ik in staat ben een infrastructuurnetwerk thuis na te bouwen?

   Antwoord: In hoofdstuk 2 tot en met hoofdstuk 4 heb ik de belangrijkste technische begrippen opgenomen, toegelicht en uitgelegd, zodat de lezer beter begrijpt wat nodig is om te komen tot de bouw van een computer infrastructuur.

2. Hoe ziet het netwerk van het RLW (Rijnlands lyceum Wassenaar) er uit?

   Antwoord: In hoofdstuk 5 heb ik uiteengezet hoe het netwerk van het RLW in elkaar zit. Het was aanvankelijk de bedoeling dat ik het netwerk van school uitgebreid zou onderzoeken om goed te kunnen beoordelen hoe dit is opgezet. Mijn plan was een afspraak te maken met de IT-beheerder van school. Door de corona crisis is de school echter onverwacht langere tijd gesloten, waardoor het niet gelukt is met de netwerkbeheerder van school af te spreken. Daarom heb ik zelf een inschatting gemaakt van hoe de infrastructuur op het RLW er uit ziet. Daarbij heb ik gebruik gemaakt van mijn eerdere observaties van het netwerk; ook heb ik een aantal aannames moeten doen.

3. Is het mogelijk een handleiding/demo te bouwen zodat anderen mijn resultaat kunnen nabouwen?

   Antwoord: Ja, dat is mogelijk. Ik heb een website gemaakt die dient als demo/handleiding bij dit profielwerkstuk. Het was de bedoeling dat deze stapsgewijs beoordeeld kon worden door een gebruiker om te kunnen beoordelen of de stappen in de handleiding/demo voldoende zijn uitgelegd. Helaas is de handleiding niet door iemand in de praktijk getest. Dit komt doordat het erg lastig was iemand te vinden die tijd kon vrijmaken om een dergelijke handleiding/demo te testen. Wel is het gelukt de website met de handleiding te maken.

7.3 DE HOOFDVRAAG

Mijn onderzoeksvraag was “Hoe bouw je een infrastructuur zoals op school gebruikt wordt, thuis na?”

Antwoord: Er is geen eenduidig antwoord op deze vraag mogelijk. De infrastructuur van het RLW kan thuis op verschillende manieren worden nagebouwd. Wel kan een infrastructuur netwerk thuis worden gebouwd dat de nodige onderdelen van het RLW nabouwt. Het is gelukt een omgeving thuis te bouwen waarin een gebruiker kan inloggen op een computer en deze informatie krijgt

[6] Mijn onderzoeksvraag was “Hoe bouw je een infrastructuur zoals op school gebruikt wordt, thuis na?”

gesynchroniseerd van de server. Het zal echter niet lukken thuis technisch precies hetzelfde systeem van het RLW na te bouwen wegens beperkingen in de beschikbare tijd, geld, kennis en licenties.

Voor alle producten die je kan kiezen tijdens het opzetten van de verschillende benodigde onderdelen van een infrastructuurnetwerk kunnen altijd andere onderdelen of producten worden gekozen. Er zal nooit één goede keuze zijn die andere opties uitsluit, omdat afhankelijk van wat het doel van het infrastructuur netwerk is, er andere uitganspunten gekozen kunnen (en soms moeten) worden en er dus andere resultaten opgeleverd zullen worden.

Via mijn website heb ik een handleiding opgesteld met behulp waarvan een computer infrastructuur kan worden gebouwd. Maar dit sluit niet uit dat het ook op andere manieren kan worden aangepakt of ingevuld. Ik heb in elk geval veel geleerd over hoe het netwerk van school er uitziet en hoe je er zelf één moet bouwen.

8 BIJLAGEN

De bijlagen van dit profielwerkstuk bestaan uit een logboek, een bronnenverantwoording, een lijst met verwijzingen naar de gebruikte afbeeldingen en een begrippenlijst.

8.1 LOGBOEK

Datum	**Tijdsbesteding**	**Activiteiten**	**Extra's**
maart 2019 – mei 2020	25 uur	Verkennen, nadenken en experimenteren met allerlei technische onderwerpen die ik kan gebruiken voor het thuis nabouwen van een professioneel computer netwerk. Ik heb alles eerst in de praktijk uitgezocht en uitgeprobeerd. Mijn opzet is om eerst te bekijken of alles werkt. Later wil ik alles beschrijven en over de bevindingen rapporteren in mijn profielwerkstuk. Tijdens het schrijven van het profielwerkstuk was ik nog niet klaar met veel dingen. Deze heb ik dus tijdens het schrijven aangepast	Ik heb de volgende onderdelen onderzocht en op mijn eigen computernetwerk geconfigureerd en uitgeprobeerd: - DHCP - Proxmox (hypervisor) - Apache (webserver) - Mailserver (deels gelukt) - Domeindirectory - DNS - PfSense (router, firewall) - SMB (Bestanden en opslag services) - MDT (maken van een aangepaste ISO) - openVPN - Groep policy - 3 gebruiker en groep permissies - etc.
1/2/2020	3 uur		Tijd besteed aan het werkend maken van een netwerkinstallatie
5/2/2020	2,5 uur	Samen met docenten uitgedacht wat de beste opties waren voor het uitwerken van het profielwerkstuk. Ik heb hieraan thuis gewerkt.	

8/2	4 uur	Uitwerking van deelvragen en de helft van de inleiding geschreven.	
9/2	2 uur	Uitwerking overige deelvragen, logboek, en inleiding.	
13/2	1 uur	Verbeteren logboek en fouten verbeterd uit hoofdstuk 1	
Tijdvak 2			
15/2	4 uur	Maken van introductie, opzet paragraaf internet adressen en structuur.	
16/2	2 uur	Nakijken opzet en indeling	
1/3	2 uur	2.4 en 2.5	
2/3	1,5 uur	2,4.1 en 2.4.2 en verbetering van overige fouten	
2/3	2 uur	Meer nakijken en hoofdstuk 2 afronden	
3/3	1 uur	Begin hoofdstuk 3	
4/3	1 uur	Logboek verbeteren en aan hoofdstuk 3 gewerkt	
4/3	2 uur	Aan hoofdstuk 3 gewerkt	
7/3	4 uur	Aan mijn eigen website op wiki gewerkt	
7/3	1 uur	Aan 3.1 en 3.2 gewerkt	
Tijdvak 3			
13/3	4 uur	Aan 3.2 gewerkt	Aan website gewerkt: Hoofdstuk 1 en veel extra's zoals betere permissies email servers etc
19/3	1 uur		Chrome synchronisatie met Windows-server
10/4	5 uur		Aan website gewerkt: Hoofdstuk 2 en deel hoofdstuk 3 + overig
12/4	3 uur		Aan website gewerkt: Hoofdstuk 2 afgerond en aan 3 begonnen + overig
13/4	3 uur		Problemen met MDT opgelost en netwerk boot ge-optimaliseert
27/4	5 uur	Aan 3.2 en 3.3 gewerkt. Begin gemaakt met hoofdstuk 4	index.php verkorten naar hoofdpagina
28/4	3 uur	Hoofdstuk 3 afgerond; verder gewerkt aan hoofdstuk 4	
29/4	3 uur	hoofdstuk4 afgerond en aan hoofdstuk 5 begonnen	Aan website gewerkt
4/5	6 uur	Server opgehaald bij bedrijf (www.comprofs.nl) . Thuis de drives formatteren van de server en begin maken van inrichting van de server	Mindmap gemaakt over aanleggen netwerken
7/5	3 uur		Verder van opzetten Esxi en VMS.

8/5	4 uur		Opzetten van connectie server security server en aantal policy's
9/5	3 uur		Maken van golden image
13/5	4 uur		Optimalisatie en opstart problemen oplossen. Uitleg filmpje gemaakt.
Tijdvak 4/			
13/7	3 uur	Overleg met docent wat moet worden aangepast. Na overleg met docent 5000 woorden met nadere uitleg geschrapt en deels verplaatst naar website.	
25/7	2 uur	Aan hoofdstuk 4 gewerkt	
19/8	4 uur	Aan hoofdstuk 4 gewerkt	
22/8	2 uur	Hoofdstuk 4	
23/8	2 uur	Hoofdstuk 5	Aan Hoofdstuk 6 gewerkt
24/8	5 uur	Hoofdstuk 7	
25/8	4 uur	Hoofdstuk 6 en 7	
26/8	4 uur	Hoofdstuk 7, Bronnen, opmaak controleren	Aan website gewerkt.
27/8	3 uur	Afkortingenlijst gemaakt	Aan website gewerkt.
28/8	3 uur		Aan website gewerkt
29/8	2 uur		Aan website gewerkt
30/8	6 uur	Alles controleren op spelling en opmaak	Afbeeldingen benoemd en bronvermelding van afbeeldingen opgenomen
Totaal	120 uur		

8.2 BRONNEN

Onderstaande bronnen werden voor het hele profielwerkstuk gebruikt:

https://stackoverflow.com/

https://www.reddit.com/

https://www.wikipedia.org/

https://docs.microsoft.com/

https://www.youtube.com/

https://www.tomshardware.com/

https://www.howtogeek.com/

https://askubuntu.com/

https://docs.vmware.com/

https://pve.Proxmox.com/pve-docs/

https://docs.netgate.com/pfsense/en/latest/

https://www.quora.com

Verder heb ik informatie gehaald uit het volgende boek: “Netwerkbeheer met Windows server 2019”, deel 1 Inrichting en beheer op een LAN, Jan Smets, Uitgeverij Brinkman, ISBN: 978-90-5752-397-7.

8.2.1 HOOFDSTUK 2

Afbeelding 1: https://www.dezaak.nl/2582/draadloos-netwerk-beveiligen.html

Afbeelding 2: https://nl.wikipedia.org/wiki/OSI-model

Afbeelding 3: https://en.wikipedia.org/wiki/Preboot_Execution_Environment

https://nl.wikIPedia.org/wiki/Subnet

https://nl.wikIPedia.org/wiki/Netmask

https://nl.wikIPedia.org/wiki/IP-adres

https://nl.wikIPedia.org/wiki/Dynamic_Host_Configuration_Protocol

https://nl.wikIPedia.org/wiki/RFC_1918

https://nl.wikIPedia.org/wiki/OSI-model

https://nl.ccm.net/faq/5500-wat-is-het-verschil-tussen-udp-en-tcp

https://nl.wikIPedia.org/wiki/Dynamic_Host_Configuration_Protocol
https://en.wikIPedia.org/wiki/Dynamic_DNS

https://www.quora.com/Does-changing-my-computer%E2%80%99s-DNS-prevent-my-ISP-from-tracking-my-browsing-activity

https://www.lifewire.com/what-is-a-dns-cache-817514

https://stackoverflow.com/questions/246930/is-there-any-difference-between-a-guid-and-a-uuid

8.2.2 HOOFDSTUK 3

Afbeelding 4: https://mobile.serverwatch.com/imagesvr_ce/1566/hypervisor-2.jpg

Afbeelding 5: https://mobile.serverwatch.com/imagesvr_ce/1566/hypervisor-2.jpg

Afbeelding 6: https://bobcares.com/blog/lxc-vs-docker/

https://bobcares.com/blog/lxc-vs-docker/

https://www.upguard.com/articles/docker-vs-lxc

https://vapour-apps.com/what-is-hypervisor/

Voetnoot 3: Zie https://nl.wikipedia.org/wiki/Kernel

voetnoot 4: https://nl.wikipedia.org/wiki/Exploit_(computerbeveiliging)

8.2.3 HOOFDSTUK 4

Afbeelding 7: https://www.cleanpng.com/png-windows-server-2012-r2-windows-server-2008-client-4137139/

Afbeelding 8: foto van mijn eigen computerscherm

Afbeelding 9: scherm foto

Afbeelding 10: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v=ws.11)

Afbeelding 11: https://www.shutterstock.com/nl/image-vector/hard-disk-vector-sketch-icon-isolated-464278742

Afbeelding 12: https://nl.wikipedia.org/wiki/Redundant_array_of_independent_disks

Afbeelding 13: scherm foto

Afbeelding 14: scherm foto

Afbeelding 15: scherm foto

8.2.4 HOOFDSTUK 5

Afbeelding 16: gemaakt met https://www.lucidchart.com/pages/nl

Afbeelding 17: gemaakt met https://www.lucidchart.com/pages/nl

Afbeelding 18: afkomstig van YouTube filmpje

Afbeelding 19: afkomstig van mijn wiki pagina “https://computerinfrastructuur.nl”

8.2.5 AFBEELDINGEN

8.3 BEGRIPPENLIJST

- **AD** (Active directory) = database waar onder andere gebruikers permissies staan
- **CIFS** (Common Internet File System) = network file share waarbij gebruikersnaam en wachtwoord nodig is om share te kunnen bereiken.
- **DC** (Domain Component) = onderdeel in AD database
- **DDNS** (Dynamic Domain Name System) = update van A record wanneer IP veranderd
- **DHCP** (Dynamic Host Configuration Protocol) = server in een netwerk die onder andere IP-adressen uitdeelt
- **DNSBL** (DNS BlackList) = block list voor domein namen zodat er geen IP adres kan worden opgehaald of een omleiding wordt toegepast
- **DNS** (Domain Name System) = database/system waar IP-adressen in staan opgeslagen voor de juiste domein namen
- **IP-adres** (internet protocol) = adres voor een computer
- **IPv4** en **IPv6** (internet protocol versie 4 en 6) = IP-adres van een computer
- **IOS** (iPhone operating system) besturingssysteem voor iPhone/ipad
- **ISP** (Internet Service Provider) = provider voor internet en andere diensten zoals TV
- **KVM** (Kernel-based Virtual Machine) = vorm van virtualisatie
- **LXC** (Linux Container) = vorm van virtualisatie
- **LDAP** (Lightweight Directory Access Protocol) = service die onder andere wordt gebruikt voor AD
- **MAC-adres** (Media access control) = serial nummer van een NIC
- **MX** (Mail exchanger) = DNS record
- **MDT** (Microsoft deployement toolkit) = toolkit die door windows wordt aangeboden om bijvoorbeeld een windows installatie via LiteTouch te kunnen installeren
- **NAT** (Network Address Translation) = van één adres meerdere adressen maken
- **NAS** (Network-attached storage) = opslag over het netwerk kunnen gebruiken
- **NFS** (Network File System) = netwerk opslag
- **NIC** (Network Interface Card) = apparaat/PCLe kaart die wordt gebruikt om een internet connectie tot stand te brengen
- **NS** (Name server) = beheerden van DNS records
- **OSI-model** (Open Systems Interconnection) = model dat weergeeft hoe een internet connectie werkt
- **OS** (Operating systeem) = besturingssysteem
- **OU** (Organizational Unit) = onderdeel van AD database

- **PLCe** (Peripheral Component Interconnect Express) = slot op moederboord waar je een PCLe kaart in kan doen
- **PXE** (Preboot Execution Environment) = opstart process
- **QEMU** (Quick EMUlator) = vorm van virtualisatie
- **RAT** (Remote access trojan) = vorm van een virus op een computer
- **RAID** (Redundant array of independent disks) = configuratie waarmee je opslag kan beschermen
- **RLW** (Rijnlands Lyceum Wassenaar) = vestiging waarvan ik de infrastructuur heb nagebouwd
- **SRV** (Service) = DNS record
- **SMB** (Server Message Block) = file system
- **SSL** (Secure socket layer) = cryptografische protocollen die gegevens coderen
- **TLS** (Transport Layer Security) = cryptografische protocollen die gegevens coderen
- **TCP** (Transmission Control Protocol) = protocol dat wordt gebruikt bij het versturen van informatie
- **TFTP** (Trivial File Transfer Protocol) = protocol dat wordt gebruikt voor het versturen van informatie
- **UDP** (User Datagram Protocol protocol) = protocol dat wordt gebruikt voor het versturen van informatie
- **VDI** (Virtual Desktop Infrastructure) = benodigdheden voor een Cloud bureaublad omgeving
- **VM** (Virtual machines) = onderliggend system van een host computer
- **VPN** (Virtual private network) = manier om IP adres te veranderen
- **WAP** (Wireless access point) = apparaat dat wifi uitzendt
- **WOL** (Wake-on-LAN) = methode om computer op te starten wanneer deze uit staat
- **WDS** (Windows Deployment share) = service om een computer te laten vanaf een netwerk
- **WMI** (Windows Management Instrumentation) = subsysteem van powershell nodig voor een hoop dingen
- **ZFS** (Zettabyte Filesystem) = file system dat wordt gebruikt om informatie te beschermen