ERHVERVSAKADEMI AARHUS
BUSINESS ACADEMY AARHUS

3. semester

ITEK-E22a

AVK Gummi A/S

Projekt udarbejdet af:

Aishaali M. Mohamuud & Chanett Koldsø

Vejledere:

Anders T. Eriksen & Peter Jeppesen

Anslag: 85.142

Afleveringsdato: 11-12-2023

ERHVERVSAKADEMI AARHUS
BUSINESS ACADEMY AARHUS

Sekundær forside

SEKTION	ANSVARLIG PERSON
PROJEKTHÅNDTERING	
Work Breakdown Structure	Aishaali, Chanett
Gantt planlægning i Clickup	Aishaali, Chanett
Logføring	Aishaali, Chanett
KLARLÆGNING AF CASE & DESIGN AF INFRASTRUKTUR	
Kundebesøg & interview	Chanett
Behovsanalyse	Aishaali, Chanett
Opsætning af trusselsoversigt	Aishaali, Chanett
Udformning af krav	Aishaali, Chanett
Opsætning af topologi design	Aishaali, Chanett
Opstilling af liste over virtuelle maskiner	Aishaali, Chanett
Opstilling af plan over VLANs	Aishaali, Chanett
Opstilling af IP plan	Aishaali, Chanett
IMPLEMENTERING AF INFRASTRUKTUR	
Opsætning & konfiguration af DNS/Domain server i vCenter	Chanett
Opsætning & konfiguration af Webserver i vCenter	Aishaali, Chanett
Opsætning & konfiguration af pfSense server i vCenter	Aishaali, Chanett
Opsætning & konfiguration af Backupserver i vCenter	Aishaali, Chanett
Opsætning & konfiguration af pfSense Desktop i vCenter	Aishaali, Chanett
Opsætning & konfiguration af PC i vCenter	Chanett
Opsætning af firewall regler	Aishaali, Chanett
Opsætning af VPN	Aishaali, Chanett
Opsætning af AD DS	Chanett
Opsætning af OUs, SGs, Users, Administrators	Chanett
Opsætning af Shares	Chanett
Opsætning af tilladelser	Chanett
Opsætning af backupløsning	Chanett
Opsætning af topologi i GNS3	Chanett
Konfiguration af GNS3 netværk	Aishaali, Chanett
Konfiguration af protokoller i netværk	Aishaali, Chanett
Systemtests	Aishaali, Chanett
RAPPORT	
Resumé	Aishaali, Chanett
1. Introduktion	Aishaali, Chanett
2. Metoder og værktøjer	Aishaali, Chanett

8. Konklusion	Aishaali, Chanett
9. Bilagsoversigt	Aishaali, Chanett
10. Kildeliste	Aishaali, Chanett

Resumé

I forbindelse med det 3. semesters eksamensprojekt på IT-teknologuddannelsen ved Erhvervsakademi Aarhus har Gruppe 5 udarbejdet en case, der fokuserer på omstrukturering af en svag it-infrastruktur efter et ransomware angreb i en produktionsvirksomhed. Projektet, der integrerer fagområder som Enterprise Network, Virtualization, Security, Directory Services, og Business Continuity, har også inddraget Project Management.

Projektet indledes med planlægning af it-infrastrukturen og kulminerer i specifikationen af krav. Implementeringen foregår gennem en sammenkobling af et GNS3 projekt og virtuelle maskiner i VMware vCenter. Fokus i GNS3 projektet ligger på redundans med etherchannel og VRRP, VLANs, og trunking, mens vCenter anvendes til opsætning og konfiguration af servere og PC'er med forskellige operativsystemer som Windows og Ubuntu.

Arbejdsopgaver, metoder, og værktøjer er struktureret efter fagområder, og rapporten følger en Work Breakdown Structure. Projekt Management dækker hele projektarbejdet, inklusive planlægning, udførelse, og dokumentation ved hjælp af værktøjer som WBS-diagram og Gantt kort.

I perspektivering evaluerer Gruppe 5 samarbejdsprocessen og påpeger udfordringerne ved sygdom og tidsmangel. Selvom de har opnået positiv kommunikation og samarbejde, erkender de tekniske udfordringer ved omstruktureringen af GNS3 projektet og identificerer områder, der kræver nærmere opmærksomhed, såsom VLANs på virtuelle maskiner og opdeling af IP-adresser.

I konklusionen præsenteres den opnåede redundante it-infrastruktur med teknologier som RAID-1 storage, etherchannel, RSTP, og VRRP. Der etableres en firewall og specifikke regler for trafik mellem områder. Et velfungerende domæne netværk med organisatoriske enheder og brugertilladelser muliggør deling af filer, mens VPN-forbindelse og SNMP sikrer fjernadgang og monitorering af netværksenheder. Dog konkluderes det, at visse krav som Zabbix overvågning, Group Policies for password-politik, og implementering af Cloud backup ikke er opfyldt.

Indholdsfortegnelse

1. Introduktion

På IT-teknologuddannelsen ved Erhvervsakademi Aarhus afholdes 3. semesters eksamensprojekt. Projektgruppen skal selv udarbejde en case, som skal dække de fagområder, der er arbejdet med på semestret i fagene: Enterprise Network, Virtualization, Security, Directory Services og Business Continuity. Projektet skal også inddrage Project Management.

Gruppe 5's case bygger på en produktionsvirksomhed, der i et tiltænkt scenarie har haft et en svag it-infrastruktur og derfor været udsat for et ransomware angreb. Derfor ønsker kunden at omstrukturere hele deres IT-infrastruktur med øget fokus på sikkerhed. Dette er et scenarie, som mange virksomheder desværre oplever i virkeligheden. Som nyuddannet it–teknolog er det derfor vigtigt at kende til dét at planlægge, designe, opsætte og konfigurere en it-infrastruktur fra bunden. Hertil også få kendskab til eksterne værktøjer, som kan bruges. I projektet inddrages fx backup programmet Veeam.

Projektet begynder med planlægning af it-infrastrukturen, som til sidst udmunder i en specifikation af krav, som listes op i afsnit 4. Krav.

Implementeringen af it-infrastrukturen er en sammenkobling af et GNS3 projekt og virtuelle maskiner i VMware vCenter. GNS3 projektet viser netværkstopologien og det er her, netværket konfigureres med Layer 2 og Layer 3 switches samt PC'er. Her vil der være fokus på redundans med etherchannel og VRRP samt opsætning af VLANs med tilhørende trunking. I det virtuelle miljø i vCenter vil der blive opsat og konfigureret en række servers og PCs, som skal konfigureres. Her er der tale om operativsystemer som Windows og Ubuntu, som hver har sine konfigurationsprocesser. Begge danner grundlag for meget forskellige typer af arbejdsopgaver, som man som nyuddannet møder i it-branchen.

Opdelingen af arbejdsopgaver, arbejdsmetoder og værktøjer er delt op efter fag i afsnit 2. Metoder og Værktøjer. Selve rapporten følger stort set den struktur, der er opsat i afsnit 6.2 Work Breakdown Structure.

Slutteligt dækker Project Management projektarbejdet som helhed – hvordan det planlægges, tilrettelægges, udføres og dokumenteres. Hertil gøres brug af værktøjer som fx et WBS-diagram og Gantt-kort.

2. Metoder & Værktøjer

I forbindelse med det afsluttende projekt på 3. semester arbejdes der med en række metoder og værktøjer fra alle tre semesters fagområder. Nedenfor listes de metoder og værktøjer, som har haft en stor betydning for projektarbejdet. Fagene tæller bl.a. Enterprise Networking, Virtualization, Security, Directory Service, Business Continuity og Project Management.

I forbindelse med projektarbejdets udviklingsproces er der arbejdet med følgende:

PROJECT MANAGEMENT	
VÆRKTØJER	**METODER**
Miro.com til Mindmap	Vandfaldsmetoden
Draw.io til WBS diagram	Work Breakdown Structure
Click-up til Gantt Chart	Tidsestimering og planlægning
Google Drev til fildeling	Logføring
Discord til remote briefing	Statusmøder & online briefinger

I forbindelse med faget Virtualisering, er der i opbygning af it-infrastrukturen arbejdet med følgende:

VIRTUALISERING	
VÆRKTØJER	**OPGAVER**
TrueNAS	Konfiguration af ESXi servers RAIDs storage
vSphere Hypervisor ESXi	Oprettelse af virtuelle maskiner
vSphere Client (vCenter)	Online konfiguration af virtuelle systemer
VMware Tools	Installation af VMware tools på virtuelle Windows enheder
pfSense, FreeBSD 13 & Ubuntu Server 2.7.0	Opsætning og konfiguration af Ubuntu server til firewall
Windows Server 2016 og 2019	Installation og konfiguration af Windows servers
Ubuntu Desktop 2.5.2	Installation og konfiguration af Ubuntu Desktop til firewall GUI interface
Windows 10 Education N	Installation og konfiguration af Windows PCs
Apache2	Oprettelse af webserver

Protokol: RDP	Opsætning af Remote Desktop Protocol til remote access
Protokol: DNS	Opsætning af DNS server

I forbindelse med faget Enterprise Network, er der i opsætning af it-infrastrukturen arbejdet med følgende:

ENTERPRISE NETWORK		
VÆRKTØJER	**OPGAVER**	**PROTOKOLLER**
MS Excel	Oprettelse af IP Plan	RSTP
Notepad ++	Oprettelse og vedligeholdelse af conf fil	SNMP
GNS3	Konfiguration af L2 og L3 switches	VRRP
	Oprettelse af VLANs & Trunking	VRRP
	Konfiguration af protokoller	
	Opsætning af Etherchannel	
MIB Browser	Konfiguration af MiB Browser til SNMP overvågning	

I forbindelse med faget Business Continuity er der sat fokus på følgende:

BUSINESS CONTINUITY		
REDUNDANS	**MONITORERING**	**BACKUP**
Etherchannel	MIB Browser	Veeam
VRRP	vCenter GUI	

I forbindelse med faget Directory Services er der arbejdet med følgende:

Directory Services	
OPGAVER	
Oprettelse af Organisational Units (OUs)	Oprettelse af Shares i Server Manager
Oprettelse af Security Groups (SGs)	Oprettelse af mappesystem i Windows
Oprettelse af Users & Administrators	Oprettelse af filer i mappesystem
Opsætning af tilladelser for Security Groups	Opsætning af tilladelser for Users

I forbindelse faget Security er der arbejdet med følgende:

SECURITY	
OPGAVER	
Oprettelse af Webserver i DMZ	Opsætning & konfigutraion af firewall
Oprettelse af VPN access med OpenVPN	Opsætning af firewall regler
SSL sikring af HTTP(S)	Installation af antivirus på PCs

3. Kunden

Kunden er AVK Gummi A/S. AVK Gummi A/S er en produktionsvirksomhed, der producerer gummielementer til brug i industrien inden for grupperingerne: drikkevand, energi, fødevare, healthcare og tekniske produkter. Her er der fx tale om belægning af gummi på spjældventiler, gummipakninger til rør på mejerier, luftventiler til Husqvarna motorsave eller gummibeslag til babygitre. Deres kunder tæller bl.a. Arla, Husqvarna, AVK International, Kieselmann m.fl..

Virksomheden har 199 ansatte og ligger på adressen Mosegårdsvej 1, 8670 Låsby. Selve bygningen har et samlet bygningsareal på **16.419m²** og består af fire større produktionshaller, en lager- & forsendelseshal, en kontorbygning, kantine samt omklædning. Produktionshallerne måler i omegnen af 40x100m, lager/forsendelse måler sammenlagt 40x60m og kontor/kantine måler tilsammen 60x100m.

De har registreret kapitel på 5.000.000 kr. og har afsat 950.000 kr. til at danne den nye it-infrastruktur.

Virksomheden har desuden datterselskaberne AVK Sealing Technology i Kina, AVK Ravestein i Holland samt AVK Elastomer Technology Inc. i Virginia, USA. Men vores hovedfokus ligger hos AVK Gummi A/S i Låsby. Herefter benævnes AVK Gummi A/S som kunden.

DISCLAIMER: Det skal noteres at ransomware angrebet samt alle andre formaliteter er et fiktivt scenarie tiltænkt som baggrund for projektet og ikke et scenarie, der har fundet sted.

3.1 Behov

Efter et ransomware angreb den 31. oktober 2023, har kunden ansat **AC/IT Sharks** til at genopbygge en komplet it-infrastruktur fra bunden.

Kunden ytrer følgende behov:

1. Netværket skal gerne opdeles efter afdeling. Det skal ligeledes være muligt for de enkelte afdelinger - internt - at kunne dele mapper og filer med hinanden. Det skal desuden være muligt for kontormedarbejdere at arbejde hjemmefra. Der ønskes mulighed for trådløs

tilkobling til intranet og internet. Yderligere ønskes der opsat netværksadgang til besøgende.

2. Der skal opstilles PCs i alle afdelinger. Disse PCs skal alle kunne tilgå systemet, således at en medarbejder kan tilgå sine programmer og arbejdsprocesser, uanset hvor i bygningen, man befinder sig.
3. Grundet den store produktionsmængde har virksomheden stort behov for et pålideligt netværk med færrest mulige udsving i netværksforbindelsen. De ønsker også et fleksibelt netværk, da de i fremtiden ønsker at udvide virksomhedens arealer.
4. Givet det seneste ransomware angreb ønskes der særligt fokus på sikkerhed. Den lokale IT administrator ønsker desuden mulighed for at monitorere systemet remote.

3.1.1 Behovsanalyse

Efter det indledende interview med kunden, afklarede vi en række problematikker og svagheder gennem en trusselsanalyse. Disse er listet op i Bilag 1: Trusselsoversigt.

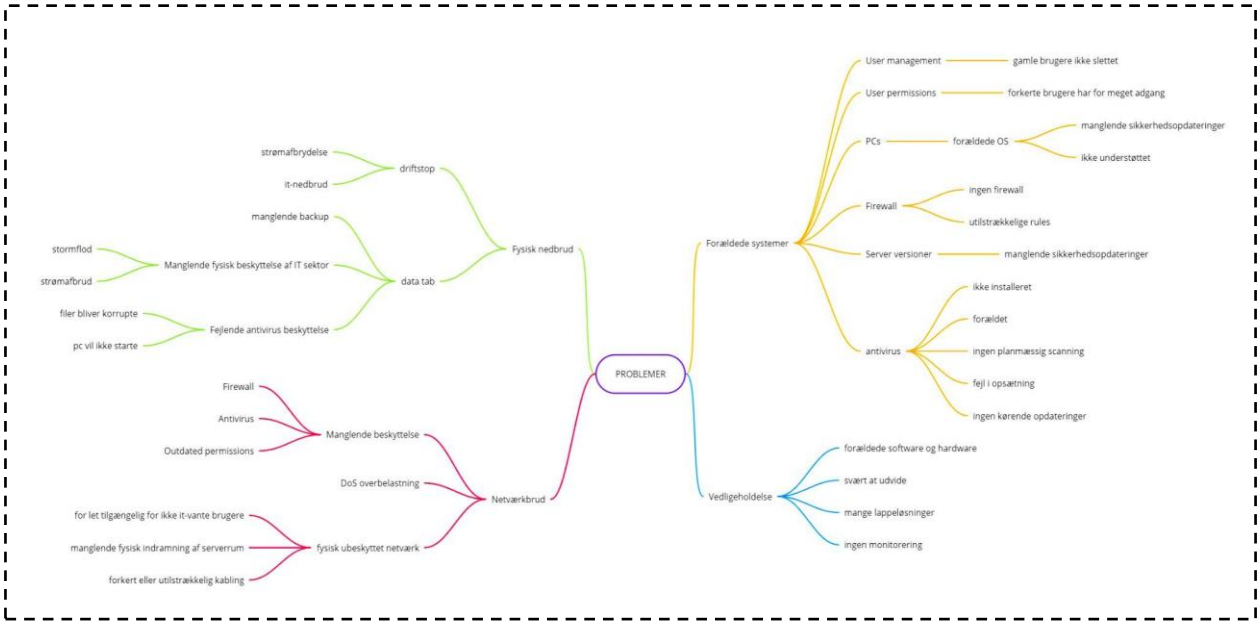


Diagram 3.1.1.1: Trusselsoversigt, Bilag 1.

Kundens it-infrastruktur bar præg af forældede systemer - fx havde alle PC'er i produktions- og lagerhaller installeret Windows XP som operativsystem, og alle manglede vigtige sikkerhedsopdateringer. Grundet de mange enheder fandt kunden det tidskrævende og besværligt at vedligeholde systemer. Derudover var beskyttelse mod fysiske nedbrud og netværksnedbrud i it-infrastrukturen mangelfuld.

Behovsanalysen deles op i følgende underafsnit 3.1.1.1 It-infrastruktur og 3.1.1.2 Sikkerhed.

3.1.1.1 It-infrastruktur

Netværket bør sættes op med en kombination af følgende servere: database server, DNS-server, webserver, backup server og monitorerings-server. Hertil kan opstilles et større antal PC'er fordelt på arealerne i produktionen, lageret og kontorerne. Disse skal være forbundet til internettet via trådløs forbindelse. Der bør være særligt fokus på redundans med benyttelse af etherchannel med RSTP og RAIDs. Grundet deres stigende behov for at kunne udvide netværket og med ønske om monitorering, kan et virtuelt miljø kombineret med fysiske bruger enheder være en effektiv løsning samtidig med at det er en mere økonomisk og miljøvenlig løsning.

3.1.1.2 Sikkerhed

Da indtrængerne fik adgang til kundens system gennem en exploit i en Cisco-enhed, der manglende en række vigtige sikkerhedsopdateringer, vil der være særligt fokus på sikkerhed, bl.a. ved at:

- Opsætte en stærk firewall med dertilhørende regler
- Sætte fokus på at systemer opdateres automatisk på daglig basis
- Give tilstrækkelige, men tilsvarende begrænsede brugertilladelser, da disse afgør hvilke systemer og software, der kan tilgås fra PC'er, eftersom kunden ønsker at alle PC'er skal have fuld adgang.
- Give fjernadgang via VPN
- Deling af filer og mapper begrænses til kun at kunne gøres inden for hver enkelt afdeling.
- At der på alle PC-maskiner installeres en antivirus

4. Krav

På baggrund af behovsanalysen opstilles følgende krav til IT-Infrastrukturen.

Netværksløsningen skal:

- opdeles på følgende afdelinger: IT, Økonomi, Salg/Indkøb & Markedsføring, Produktion & Lager, HR/Management og Guest.
- tillade deling af filer og mapper internt i afdelingerne
- kunne tilgås både kablet og trådløst
- kunne tilgås eksternt (fx fra hjemmeadressen)
- tilbyde besøgende internetadgang
- være redundant
- være fleksibelt
- have opsat PCs i alle afdelinger
- kunne monitorere vigtige områder i it-infrastrukturen
- beskyttes med firewall og antivirus
- beskyttes med brugertilladelser og en stærk fælles password politik
- optimeres med automatiske systemopdateringer
- sikres med backups både lokalt og remote

5. PROJEKTMODULER

I denne sektion opdeles rapporten i seks hovedafsnit, der følger vores WBS-diagram (Bilag 2: WBS-diagram). Disse afsnit kan afvige en smule fra WBS-strukturen, men vil helt generelt gå i dybden med de enkelte områder og opdeles grundlæggende i underafsnittene "Design", "Implementation" og "Test". De følgende hovedafsnit opdeles således:

Afsnit 5.1
PLANLÆGNING

Afsnit 5.2
VIRTUALISERING

Afsnit 5.3
NETVÆRK (GNS3)

Afsnit 5.4
SIKKERHED

Afsnit 5.5
ACTIVE DIRECTORY DOMAIN SERVICES

Afsnit 5.6
BACKUP MED VEEAM

5.1 PLANLÆGNING

Planlægningen af projektet startede med en blotlægning af kundens situation, efterfulgt af en behovsanalyse samt opstilling af krav til netværksløsningen. Dette redegøres for i afsnit 3. Kunden og afsnit 4. Krav. Disse krav ville danne baggrund for den it-infrastruktur, som skulle opsættes og konfigureres. Herefter udarbejdedes et WBS-diagram (Bilag 2: WBS-diagram), som skulle danne grundlag for den strukturelle implementering i projektforløbet. Denne blev efterfølgende implementeret som et Gantt-kort (Bilag 3: Gantt-Chart) ved brug af applikationen Click-Up. Disse

to værktøjer gennemgås i detaljer i afsnit 6.2: Work Breakdown Structure og afsnit 6.3: Gantt Chart.

Ud fra virksomhedens fysiske lokation og størrelse - og med basis i deres behov - blev en topologi designet (Bilag 4: Topologidesign) som en rettesnor for den videre implementering. Overvejelserne omkring design af topologien gennemgås i dybden i afsnit 5.1.1 Topologi Design.

Efter at have skabt et overblik med et topologidesign, blev en oversigt klargjort over de virtuelle netværks-miljøer som set i afsnit 5.1.2 Plan over VLANs. Afsnit 5.1.3 IP Plan præsenterer kort vores plan over ip-adresser, men denne er vedlagt i bilagene som Bilag 5: IP Plan.

5.1.1 Topologi Design

Som nævnt tidligere blev netværkstopologien baseret på virksomhedens fysiske størrelse og virksomhedens placering af kontorlokaler og produktionshaller.

Kontorlokalerne huser følgende afdelinger: Økonomi, Salg, Indkøb, Markedsføring, HR, Management og IT. Disse forventes delt op i én af to typer VLANs strukturer. Enten sammensluttes de i et overordnet VLAN "Office" eller de delvis sammensluttes i de mindre VLANs "Økonomi", "Salg, Indkøb og Markedsføring", "HR & Management" og "IT".

Produktionssektoren deles ligeledes op i én af to VLAN strukturer. Enten det overordnede VLAN "Production" eller de to mindre VLANs "Production" og "Lager & Forsendelse".

IT-afdelingen vil huse den primære Layer 3 switch med routing funktionalitet, ligeledes vil også servers og lagringsenheder være at finde her. Fra den primære Layer 3 switch føres et 1000BASE-T kobberkabel ud til en Layer 2 switch i kontorlokalerne. Fra denne bruges tre 1000BASE-T kobberkabler til at forbinde til tre access points - en i kontorlokalet, en i den tilstødende kantine og den sidste i en tilstødende gang, der fører til omklædningsrummene. Med en afstand på mellem 40-80m fra switch til access point vil en 1000BASE-T være tilstrækkelig, hvor 1000BASE-T tilbyder en max afstand på 100m[1]. Ethernet stik vil også skulle kobles i kontorbygningens

[1] s. 37, CCNA 200-301, Official Cert Guide, Volume 1" af Wendel Odom

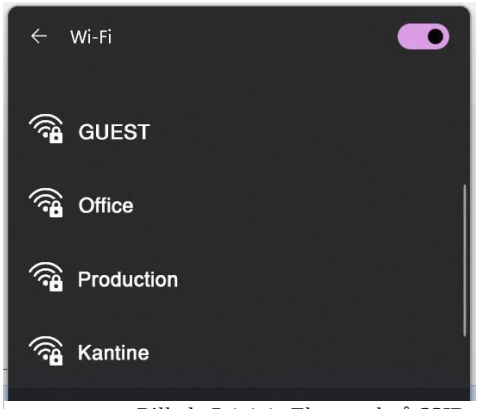
indervægge, så direkte opkobling også er en mulighed. Denne kabling vil ligeledes være med brug af 1000BASE-T standarden.

Fra Layer 3 switchen i it-afdelingen føres yderligere tre forbindelser ud til to andre switches. En Layer 2 switch i produktionshal nr. 2 og en sekundær Layer 3 switch med routing funktionalitet i produktionshal nr. 4. En redundant etherchannel vil skulle opsættes på én af disse switches, her illustreret som Layer 2 switchen. De to switches i produktionshallerne forbindes ligeledes med hinanden. Kabling mellem de tre switches vil alle være af fiberkabel typen 1000BASE-LX. Dette dels for at udnytte den længere rækkevidde på op til 5000m, som fiberkabler muliggør[2] og dels for at forhindre en kortslutning ved tilfælde af lynnedslag, som potentielt vil kunne riste enhederne, hvis de forbindes med kobberkabler. Begge kabeltyper tilbyder hastigheder på op til 1000Mpbs[3], hvilket vurderes tilstrækkeligt til virksomhedens behov. Desuden er den sekundære Layer 3 switch nøje placeret i produktionsbygningens fjerne ende, således at den bedst muligt skærmes mod brand fra kontorbygningen.

Der forefindes mellem 4-6 PC'er i hver produktionshal samt tilsvarende antal PC'er i lager og forsendelse. Disse skal have mulighed for LAN internetopkobling via ethernet-udtag i væggene. Disse ethernet-udtag udspringer fra de to switches i produktionshallerne, derfor kan opsætning af flere switches blive en nødvendighed, hvis flere enheder på sigt skal kobles på LAN'et. Antallet af PC'er i kontorlokaler er variable, da der også forefindes bærbare computere på kontorerne.

Det forventes at der opsættes et minimum på to access points i hver produktionshal, et i forsendelse, et i lager, et i kantine, et på gangen til omklædningsrummet og minimum ét access point i kontorlokalet.

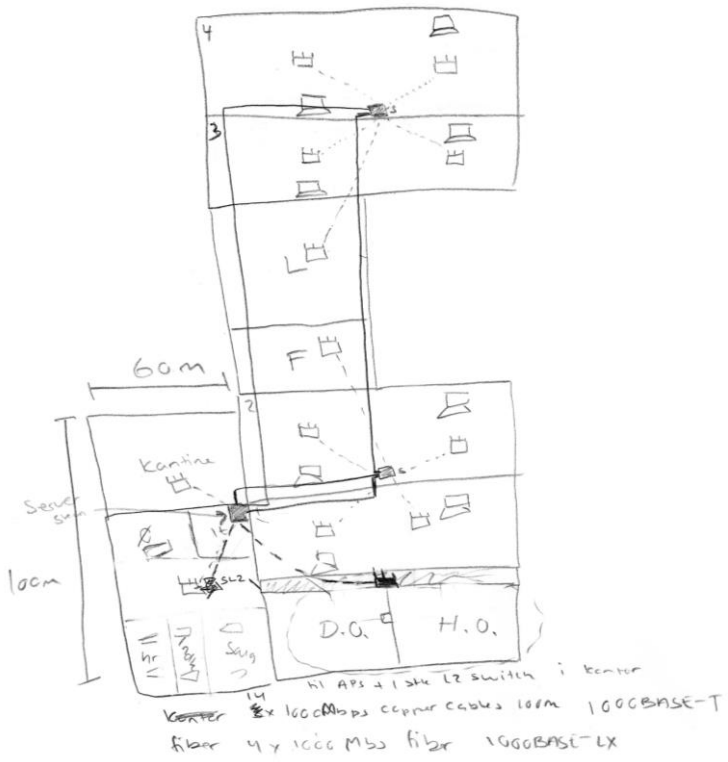
Forventede SSIDs kan fx være GUEST, Kantine, Office, Production m.v.. Alle SSID bør kræve et sikret password. GUEST netværk kan sættes op med adgang kun med password udleveret ved receptionen i kontorbygningen. Dette er blot forslag til en umiddelbar løsning.



Billede 5.1.1.1: Eksempel på SSIDs

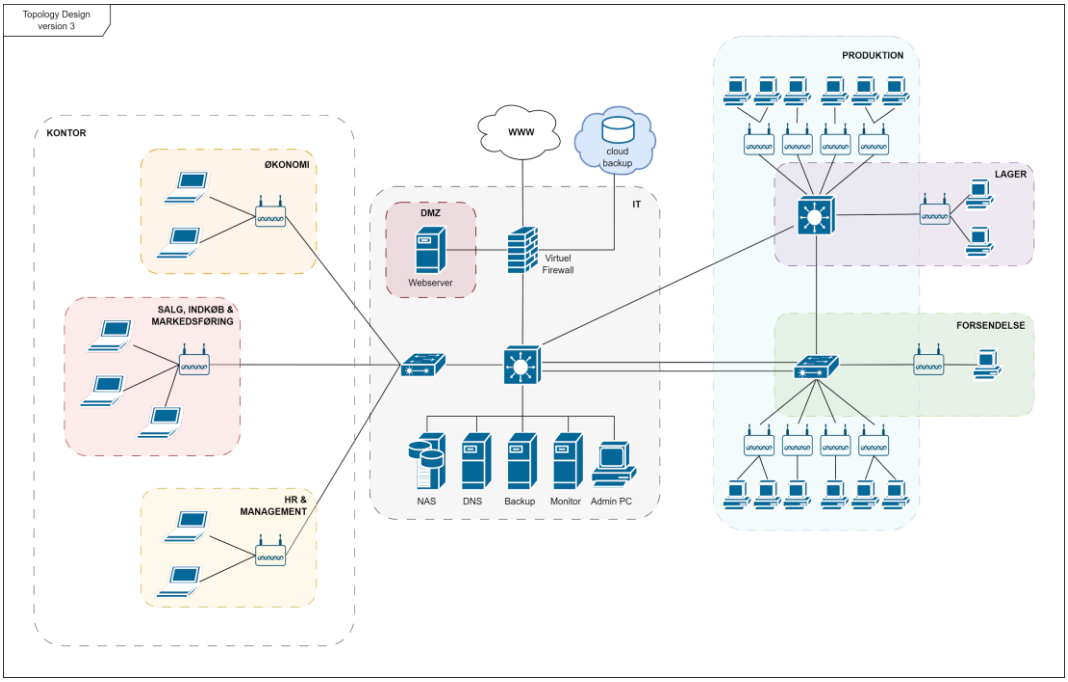
[2] s. 37, CCNA 200-301, Official Cert Guide, Volume 1" af Wendel Odom
[3] s. 37, CCNA 200-301, Official Cert Guide, Volume 1" af Wendel Odom

For at undgå interferens kan det anbefales at bruge kanalerne 1, 6 og 11 alt efter hvor mange overlapninger, der forekommer. Den første håndtegnede skitse illustreres nedenfor:



Billede 5.1.1.2: Første udkast over netværkstopologi

På baggrund af billede 5.1.1.2 samt beskrevne overvejelser udfærdigedes nedenstående topologi design med brug af webapplikationen draw.io.



Billede 5.1.1.3: Topologidesign (Bilag 4: Topologidesign)

5.1.2 Plan over VLANs

Gruppen havde til dette projekt fået tildelt VLANs 3050-3059. Disse er blevet fordelt således:

VLAN 3050	DEVICE
VLAN 3051	LAN
VLAN 3052	DMZ
VLAN 3053	Office
VLAN 3054	Production
VLAN 3055	Backup
VLAN 3056-3058	Available
VLAN 3059	GUEST

5.1.3 IP Plan

Der er her blevet udformet en IP Plan til projektet. Her kan VLAN interface for Device, LAN, WAN, Office, Prod og Guest ses og desuden hvilke IP-adresser der er tildelt interfaces. Som nævnt i tidligere afsnit, er det fra gruppens tildelte range, 3050-59. Her ender det på .121 for SW1-IT-L3. Den fulde IP-planen kan ses i Bilag 5: IP-Plan.

10.130.50.121	SW1-IT-L3	Vlan3050 / DEVICE	Fixed
10.130.051.121	SW1-IT-L3	Vlan3051 / LAN	Fixed
10.130.053.121	SW1-IT-L3	Vlan3053 / Office	Fixed
10.130.054.121	SW1-IT-L3	Vlan3054 / Production	Fixed
10.130.059.121	SW1-IT-L3	Vlan3059 / Guest	Fixed

Billede 5.1.3.1: Udsnit af IP plan (Bilag 5: IP Plan)

5.2 Virtualisering

Dette afsnit fokuserer på opsætningen og konfigurationen af de virtuelle maskiner brugt i it-infrastrukturen. Afsnittet opdeles i tre underafsnit: 5.2.1 Design og 5.2.2 Implementering.

5.2.1 Design

Jf. behovsanalysen i afsnit 3.1.1 og de specificerede krav i afsnit 4. Krav, er der valgt en virtuel løsning. Det skyldes et særligt stort behov for et pålideligt, redundant og skalerbart netværk. Virtuelle løsninger yder fem store fordele, som IBM beskriver i blogindlægget "*5 benefits of virtualization*" fra den 8. april 2021[4]. De fem fordele listes op således:

1) Virtualisering er en billigere løsning
2) Virtualisering reducer nedetid og forbedrer modstandsdygtighed i katastrofesituationer
3) Virtualisering forøger effektiviteten og produktiviteten
4) Virtualisering kan kontrollere uafhængighed og DevOps
5) Virtualisering er mere miljøvenlig (organisatorisk og miljømæssig)

Et virtuelt miljø vil derfor dække behovet for redundans, skalerbarhed og pålidelighed.
Der forventes oprettet følgende virtuelle maskiner:

- ➔ Datastore
- ➔ Domain server
- ➔ Webserver (DMZ)
- ➔ pfSense Server til firewall
- ➔ pfSense Desktop til firewall GUI
- ➔ PCs
- ➔ Backup server

5.2.2 Implementering

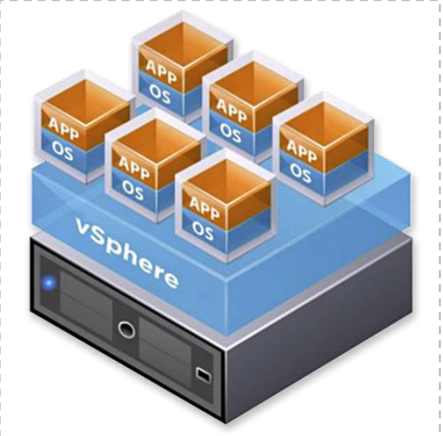
Dette afsnit redegør for opsætningen af de virtuelle maskiner samt hvordan disse er implementeret i it-infrastrukturen.

[4] https://www.ibm.com/blog/5-benefits-of-virtualization/

5.2.2.1 ESXi storage servers

5.2.2.1.1 VMware vSphere Hypervisor ESXi

Til løsningen af dette projekt benyttes skolens lagringsenheder. På disse maskiner er installeret type 1 VMware vSphere Hypervisor (ESXi) - en software, der muliggør dannelse af virtuelle maskiner på en rå enhed. Hypervisoren kan allokere og kontrollere serverens samlede kapacitet og fordele denne ud til de virtuelle maskiner, som derved kan udnytte maskinens fulde kraft. Disse maskiner vil i resten af rapporten benævnes ESXi servere.



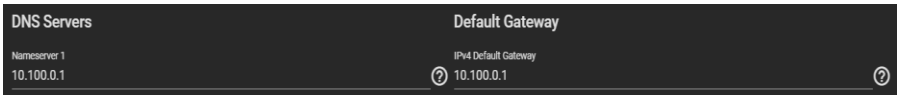
Kilde: https://www.vmware.com/products/vsphere-hypervisor.html

Det specielle ved vSphere Hypervisor er, at den understøtter "thin provisioning", som bruges til alle virtuelle maskiner i projektets it-infrastruktur. Thin provisioning gør det muligt at tildele mere harddiskplads til virtuelle servere, end der rent fysisk er installeret på maskinen. Det er muligt fordi virtuelle maskiner ikke bruger hele kapaciteten, når de kører, men kun noget af den - dvs. variabelt diskforbrug. Ved at konfigurere den virtuelle maskines harddisk til at køre i thin provisioning, deler den virtuelle maskine sin harddiskplads med andre virtuelle maskiner. Det er væsentligt i dette projekt, idet der arbejdes med mange virtuelle maskiner, der tilsammen overskrider den plads, som er os tildelt. Thin provisioning nævnes her, da dén konfiguration går igen i alle servere og det vil derfor ikke blive yderligere uddybet i de kommende afsnit.

5.2.2.1.2 RAID (Redundant Array of Independent Discs) storage - DONE

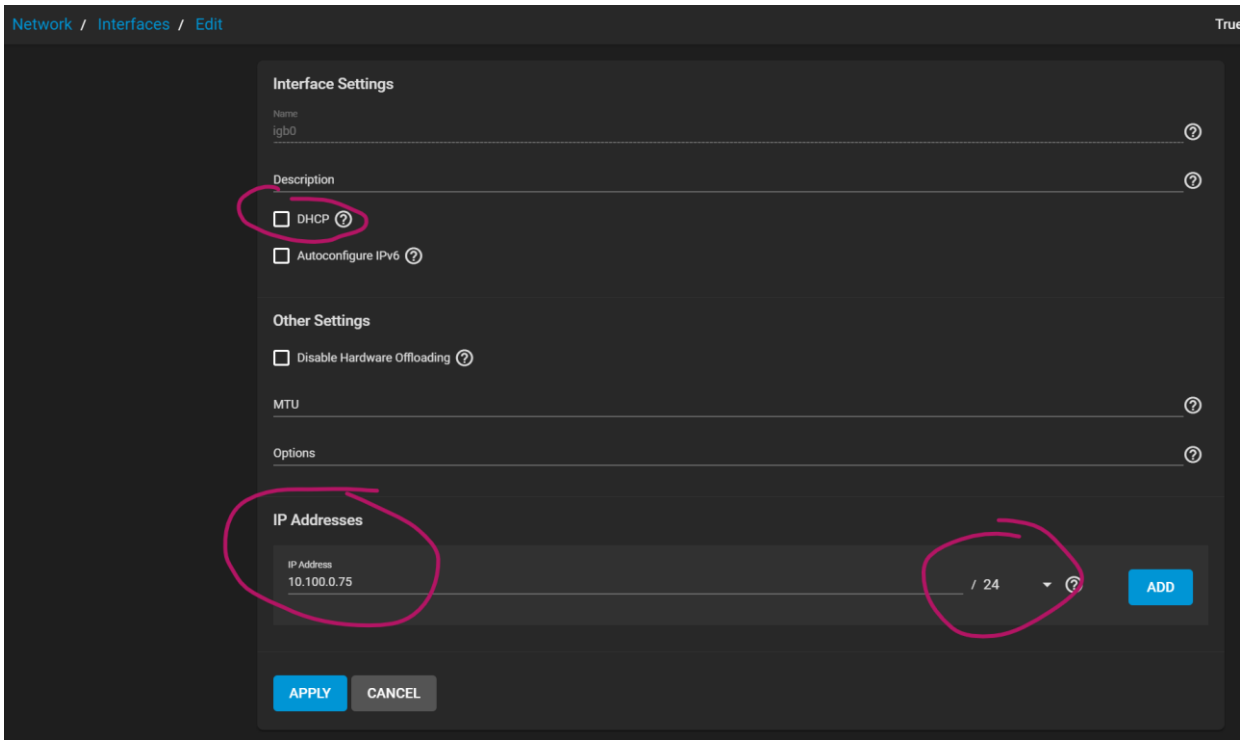
Til projektet er der tildelt en samlet harddiskplads på 350GB, som skulle konfigureres før brug. Dette blev gjort med brug af TrueNAS (også kendt som FreeNAS).

Først skulle en statisk IP adresse, Gateway og DNS konfigureres. Dette blev gjort under **Network > Global Configuration >** "Default Gateway" og "DNS Servers" blev begge sat til **10.100.0.1.**



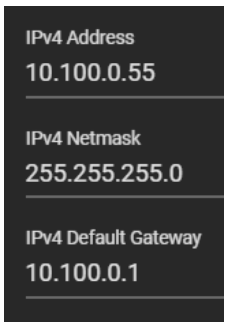
Billede 5.2.2.1.2.1: Konfiguration i TrueNAS

Den statiske IP adresse skulle opsættes under **Network ▸ Interfaces.** Her blev først DHCP slået fra, IP adressen blev herefter sat til **10.100.0.75/24** på `igb0` interfacet.



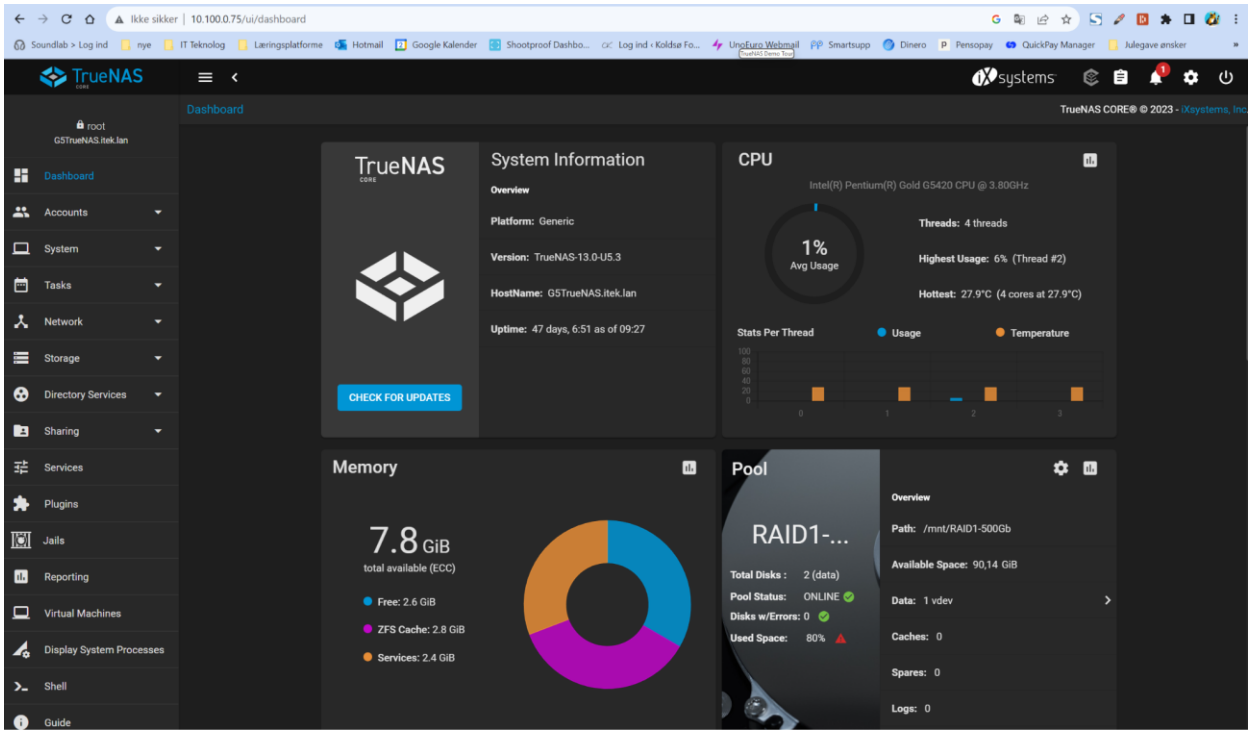
Billede 5.2.2.1.2.2: Opsætning af statisk ip adresse i TrueNAS

Under **Network ▸ IPMI** skulle sættes en statisk IP-adresse unik for gruppen - denne blev sat til 10.100.0.55/24 med samme default gateway 10.100.0.1.



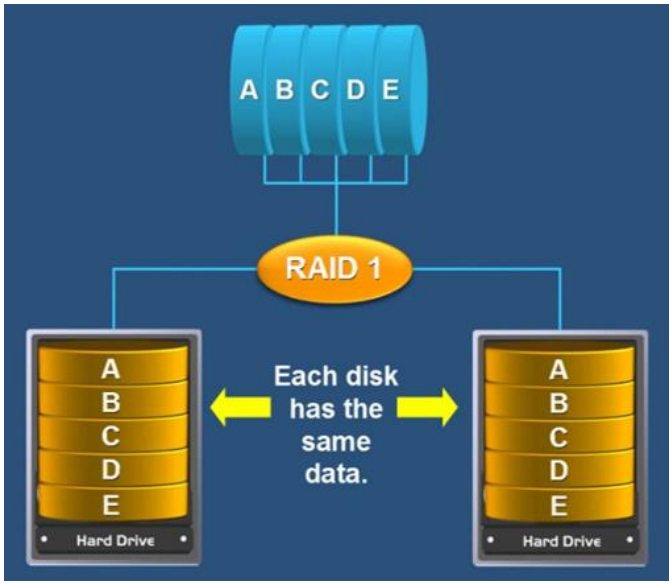
Billede 5.2.2.1.2.3: Opsætning af IPMI i TrueNAS

Efter konfiguration af IP, DNS og default gateway, blev der oprettet en RAID1 pool. På billede 5.2.2.1.2.4 ses et overblik over vores lagringsenhed på TrueNAS' webinterface. Af billedet fremgår det, at vores lagringsenhed således er sat op som en RAID1.



Billede 5.2.2.1.2.4: Overblik over lagringsenhed på TrueNAS

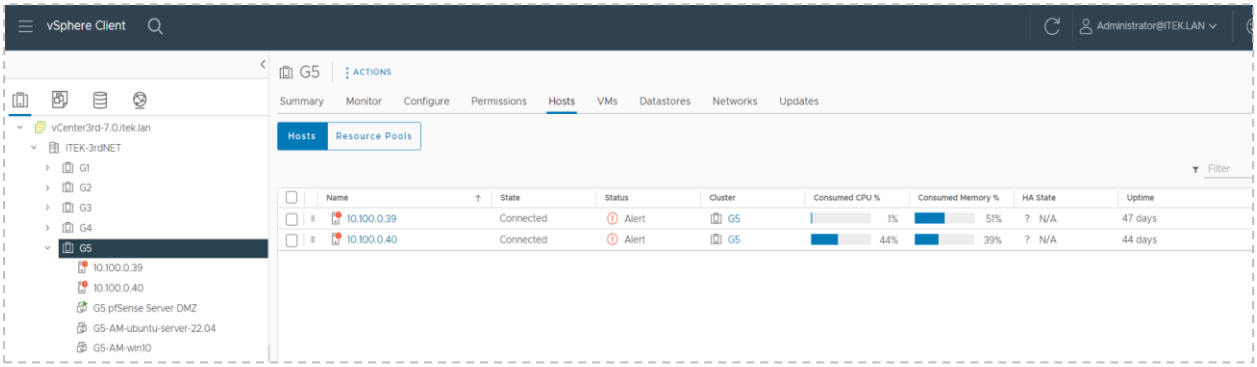
En RAID1 er en meget redundant, men relativt langsom løsning. Den skriver langsomt, fordi den skal skrive samme data to steder samtidig. Det er også en relativ tung løsning, hvad angår harddiskplads, da halvdelen af den samlede plads således bruges som backup. Den er redundant, fordi den samme data gemmes på begge harddiske - skulle den ene harddisk gå ned, så er alle data fortsat intakt på den anden harddisk.



Billede 5.2.2.1.2.5: Illustration af en RAID1 opsætning. Kilde: https://www.youtube.com/watch?v=U-OCdTeZLac

I en reel case, ville den mest optimale løsning for en virksomhed som AVK Gummi A/S være en RAID 10. En sammenslutning af RAID 0 og RAID 1. Det er en løsning, der kræver et minimum på 4 diske, men til gengæld udnytter den skrivehastigheden fra RAID 0's striping metode og pålideligheden fra RAID 1's mirroring metode. Læsehastigheden er den samme for begge RAIDs. Forskellen mellem en RAID 1 og RAID 10 illustreres nedenfor.

Herefter skulle der oprettes en Zvol (ZFS volume) på 350GB - det er et filsystem, der kræves for at kunne konfigurere en iSCSI Share, som var næste skridt. Det svarer lidt til en virtuel partition. Efter konfigurationen skulle der oprettes en datastore i vCenter. Herefter kunne vi tilgå de to ESXi storage servers gennem VMwares vSphere Client software. I billedet nedenfor ses at gruppens to ESXi servers tilhører clusteret G5 og har host IP **10.100.0.39** og **10.100.0.40**. Disse kan ses under fanen Hosts.

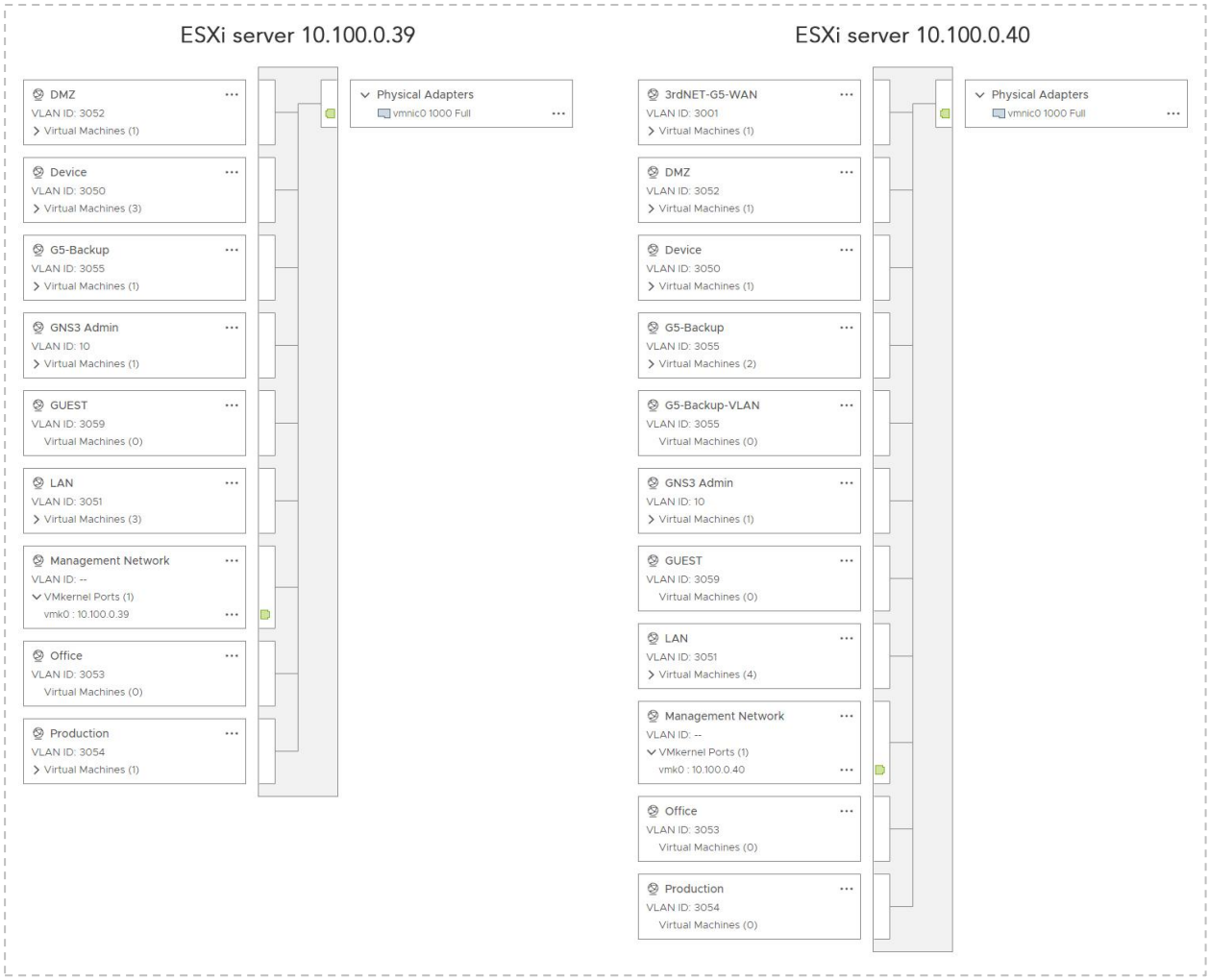


Billede 5.2.2.1.2.6: Oversigt over ESXi servers på vCenter

Det er på disse to ESXi servere, de virtuelle maskiner installeres.

5.2.2.2 Virtual Switches & VLANs

Før de virtuelle maskiner kan opsættes og konfigureres, er det nødvendigt at få oprettet de VLANs og virtuelle switches, som de virtuelle maskiner afhænger af. Til projektet havde gruppen fået tildelt VLANs i følgende range: 3050-3059. Fordelingen af virtual switches og VLANs på de to ESXi servers illustreres på billede 5.2.2.1.2.7 på næste side:



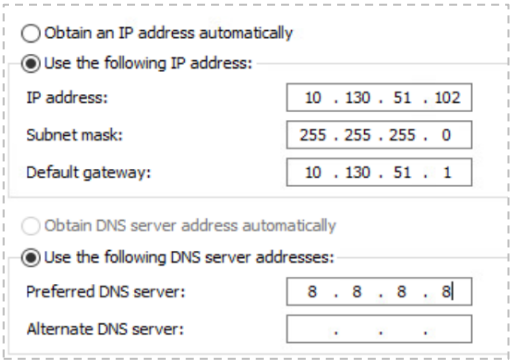
Billede 5.2.2.1.2.7: Oversigt over virtuelle switches og VLANs i vCenter

5.2.2.3 DNS / Domain server

Til at starte med skulle der oprettes en Windows DNS server, hvor nedenstående billede er et overblik over den virtuelle maskine. Den blev navngivet G5-Domain-N og vil i starten fungere som gruppens DNS server. I afsnit 5.5 Active Directory Domain Services gennemgås hvordan DNS serveren "promotes" til at være en domæneserver og hvordan domænenetværket "G5" oprettes.

Efter den grundlæggende opsætning blev følgende handlinger foretaget:

- ➔ Serveren bliver tildelt navn: G5-Domain-N
- ➔ Statisk IP adresse, default gateway og DNS konfigureres

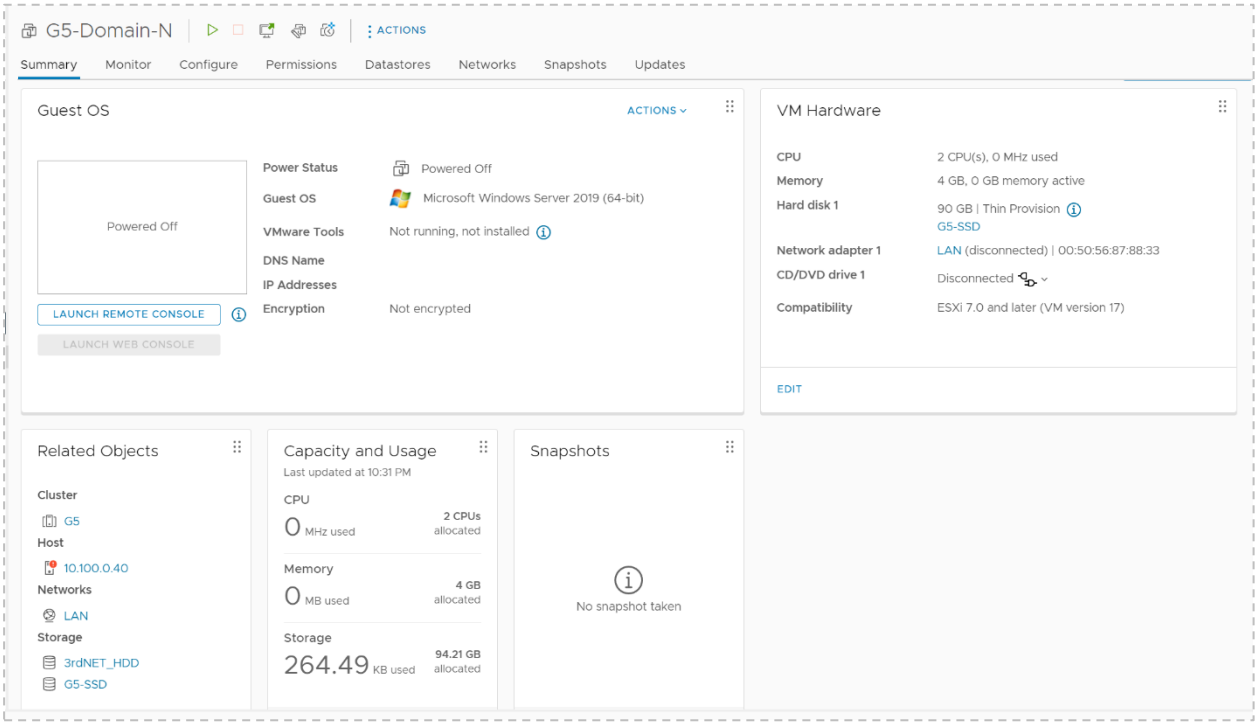


Billede 5.2.2.1.2.8: Opsætning af statisk IP

➔ Serveren blev fuldt opdateret

RDP (Remote Desktop Protokol) opsættes og testes (se afsnit 5.2.2.3.2 Test af RDP (Remote Desktop Protocol).

På billede 5.2.2.1.2.9 ses en oversigt over den virtuelle maskine i vCenter.

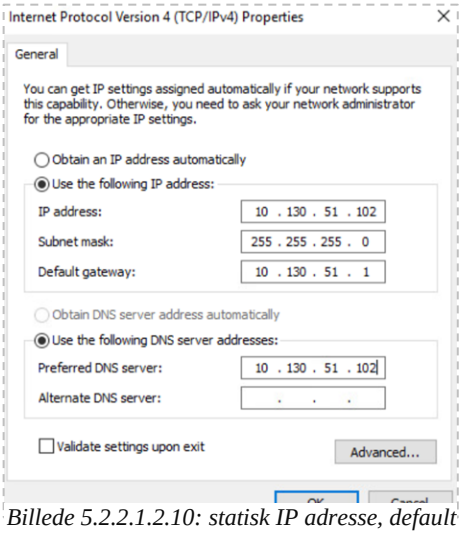


Billede 5.2.2.1.2.9: Oversigt over Domain server på vCenter

Herefter skulle DNS opsættes.

5.2.2.3.1 Opsætning af DNS & DNS Forwarding

Eftersom Domain serveren skal omdannes til gruppens DNS server, konfigureres Preferred DNS server med Domain serverens egen IP adresse uden en Alternate DNS server. Dette illustreres på billedet til højre.

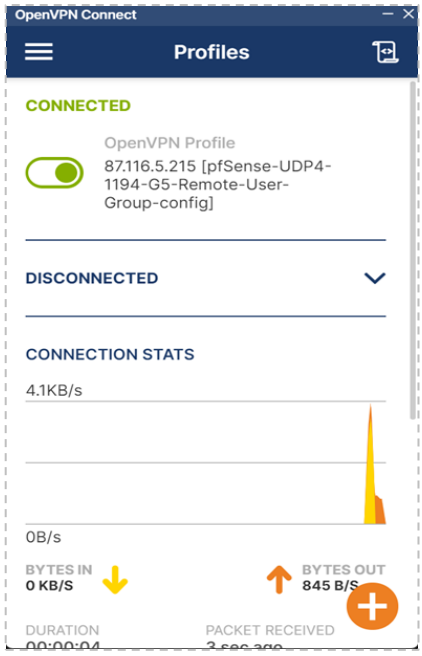


Billede 5.2.2.1.2.10: statisk IP adresse, default gateway og DNS server konfigureres

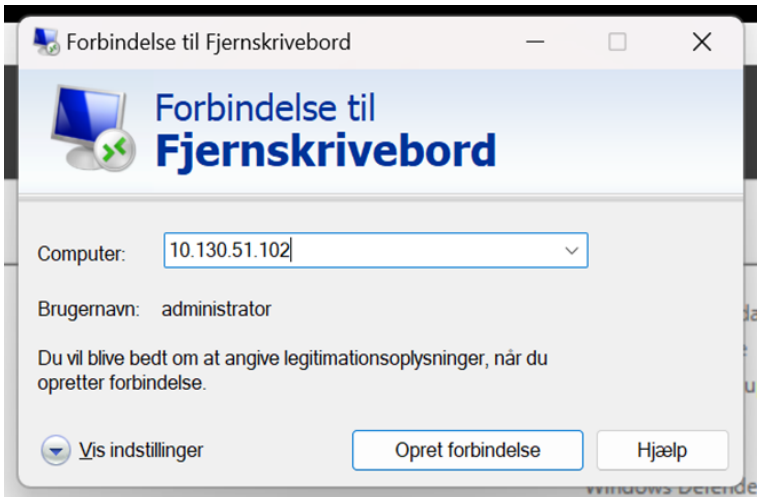
Herefter opsættes DNS forwarding, som verificeres og testes (afsnit 5.2.2.3.3 Test af DNS funktionalitet).

5.2.2.3.2 Test af RDP (Remote Desktop Protocol)

Det er muligt, gennem en VPN-forbindelse, at forbinde til Domain server på ip 10.130.51.102 via fjernskrivebord på en Windows PC. Her indtastes fx bruger am-admin og password: 3semNET! - og så er man koblet på Domain serveren.

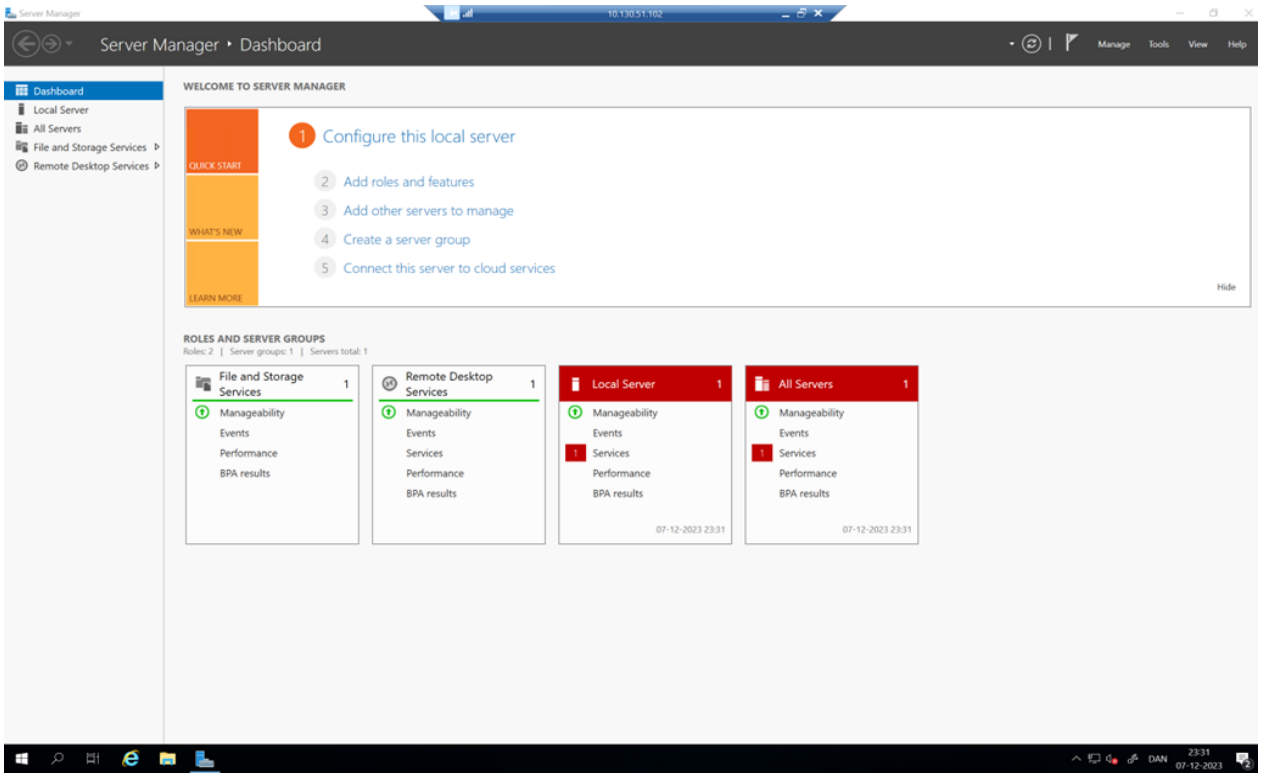


Billede 5.2.2.3.2.1: Opkobling med OpenVPN



Billede 5.2.2.3.2.2: Opkobling via Remote Desktop

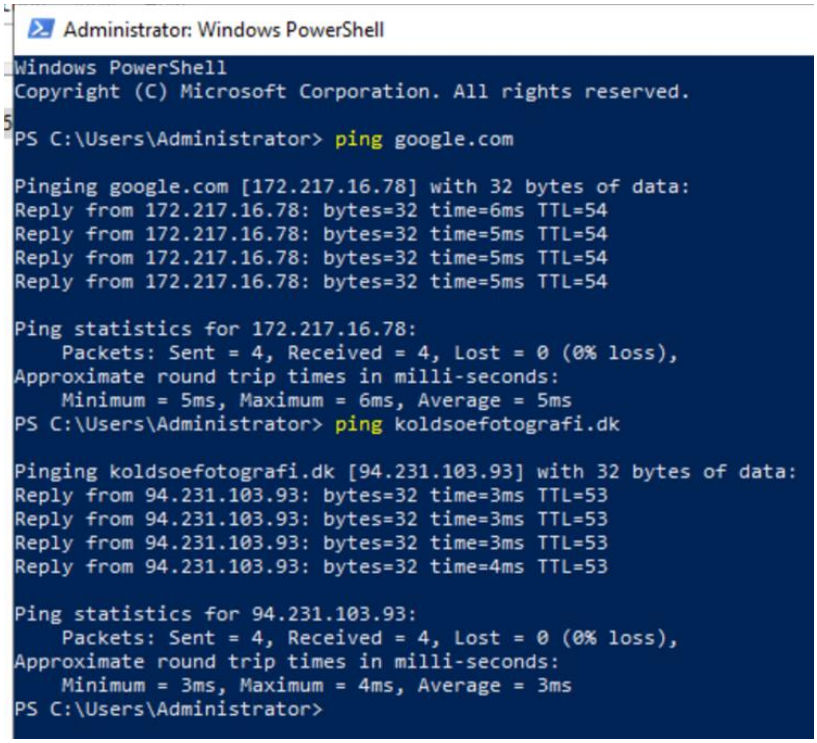
Billede 5.2.2.3.2.3 bekræfter at fjernadgang til server opnås.



Billede 5.2.2.3.2.3: Fjernadgang til server

5.2.2.3.3 Test af DNS funktionalitet

På dette screenshot dokumenteres det, at DNS kan omsætte websiderne google.com samt koldsoefotografi.dk - DNS virker som ønsket.



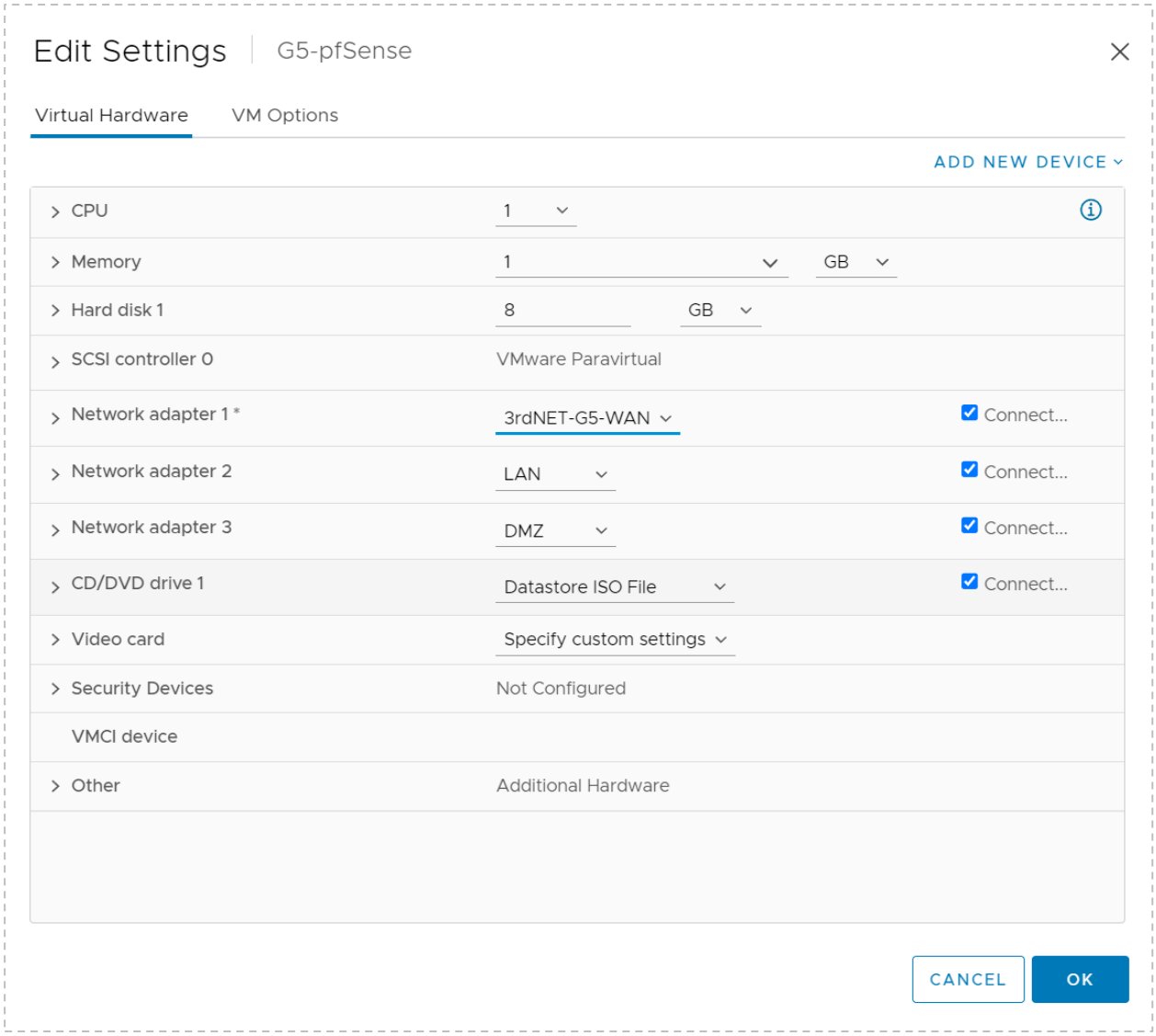
Billede 5.2.2.3.3.1: Test af DNS funktionalitet

5.2.2.4 pfSense Server

Jf. kravspecifikationer i afsnit 4. Krav skal der installeres en firewall. En særskilt server oprettes til dette formål og installeres på ESXi 10.100.0.40. Serveren konfigureres med følgende specifikationer, jf. Ubuntu System Requirements[5]:

- ESXi server: 10.100.0.40
- OS: FreeBSD 13 (or later) (64-bit)
- 1 CPU kerne
- 1 GB RAM
- 8 GB harddisk (Thin Provision) på G5-SSD
- Network Adapter forbindes til VLAN 3051 “LAN”
- ISO fil: pfsense vers. 2.7.0 AMD64.

[5] https://ubuntu.com/tutorials/install-ubuntu-server#2-requirements



Billede 5.2.2.4.1: Oversigt over server specifikationer

Herefter skulle firewall'en konfigureres, dette dokumenteres i afsnit 5.4.1 Firewall.

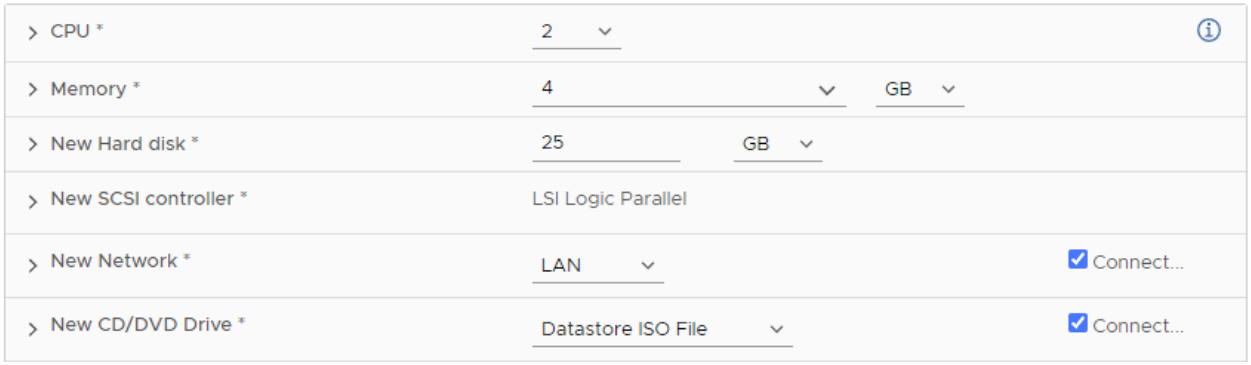
5.2.2.5 pfSense Desktop

For at kunne konfigurere vores nyligt opsatte pfSense firewall, skulle der installeres en pfSense Desktop, som kunne tilgå firewall'en via en brugervenlig GUI. Her blev en ny virtuel maskine opsat med følgende specifikationer, jf. Ubuntu System Requirements[6].

- ESXi server: 10.100.0.39
- OS: Ubuntu Linux (64-bit)

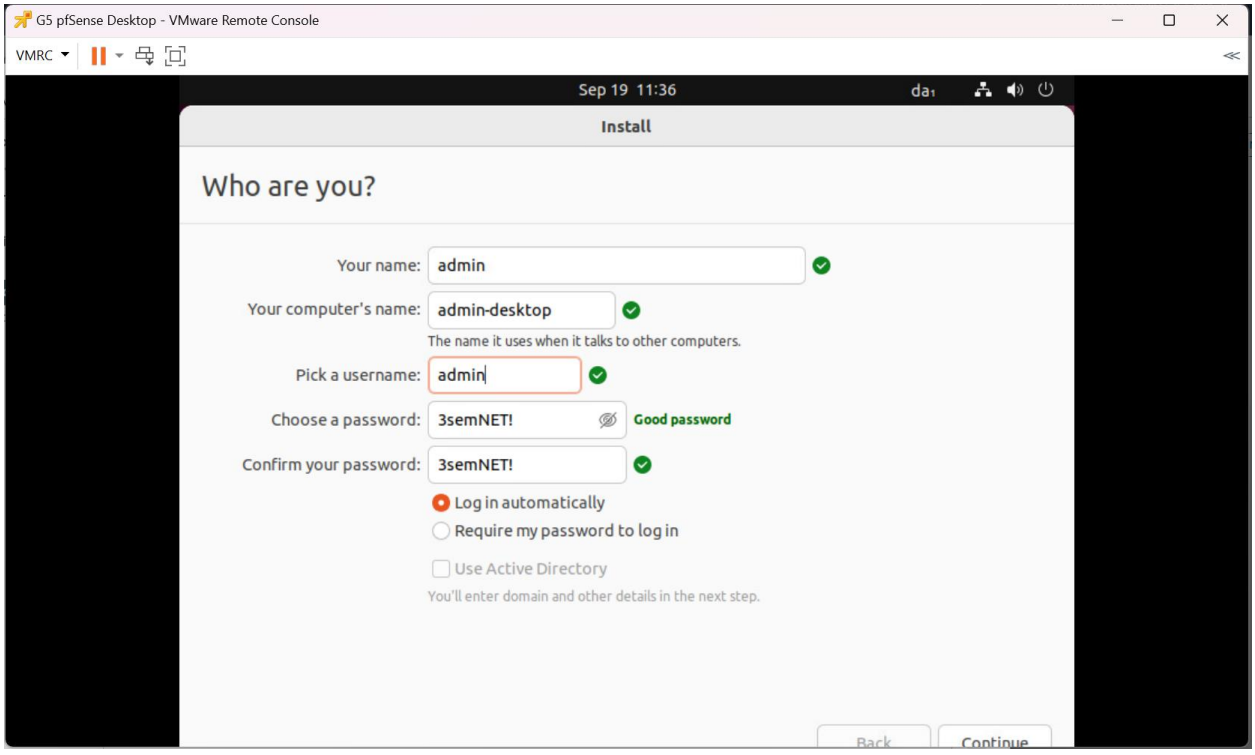
[6] https://help.ubuntu.com/community/Installation/SystemRequirements

- 2 CPU kerner
- 4 GB RAM
- 25 GB harddisk (Thin Provision) på G5-SSD
- Network Adapter forbindes til VLAN 3051 "LAN"
- ISO fil: pfsense vers. 2.5.2 AMD64.



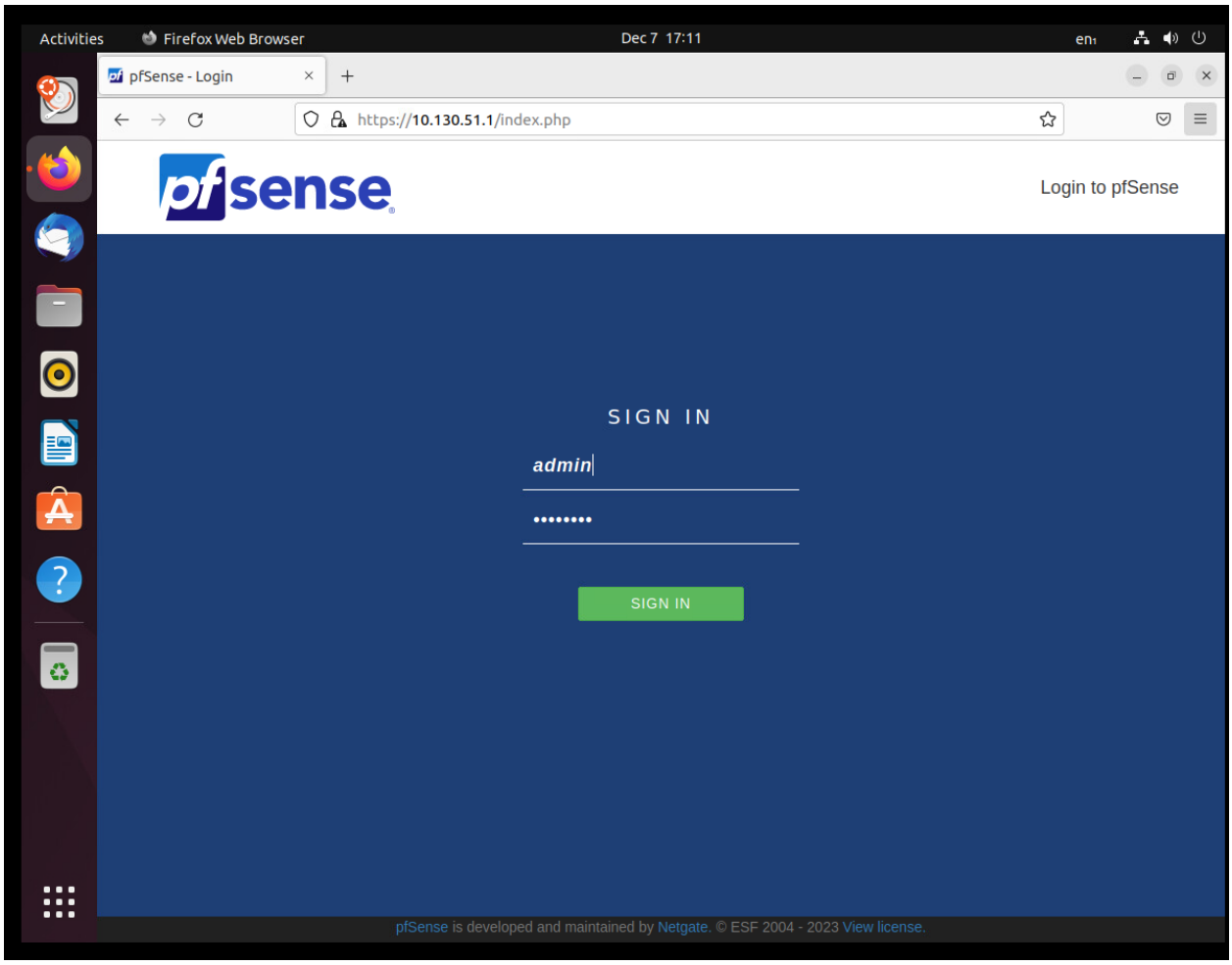
Billede 5.2.2.5.1: Oversigt over specifikationer på Ubuntu Desktop

Ved installation af softwaren opsættes brugernavn, computernavn og password.



Billede 5.2.2.5.2: Opsætning af brugernavn, pc-navn og password på Ubuntu Desktop

Efter installation af softwaren, kunne man tilgå firewall'en ved at indtaste ip-adressen konfigureret i firewall'en - 10.130.51.1.



Billede 5.2.2.5.3: Der er adgang til Firewall'ens GUI

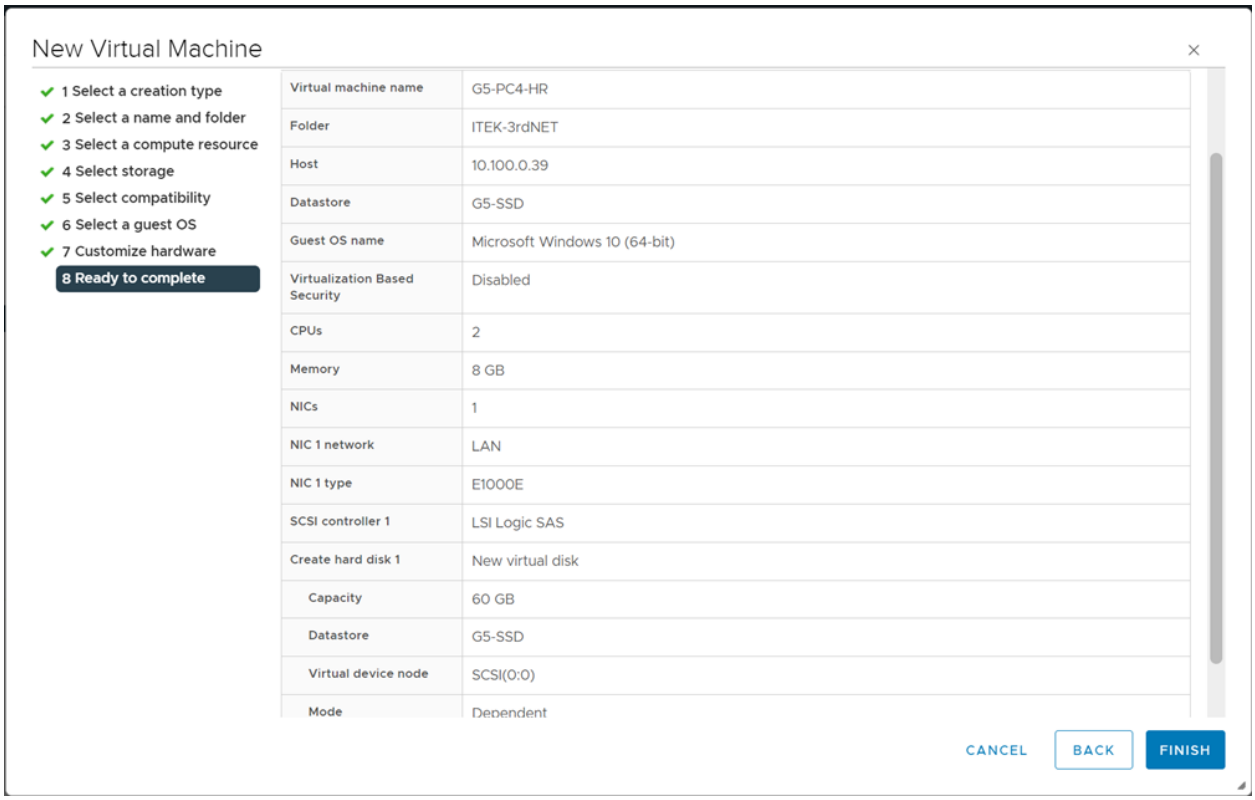
Den videre konfiguration af firewall'en via pfSense Desktop gennemgås i afsnit 5.4.1.1.1 Opsætning af interface regler via Ubuntu Desktop GUI.

5.2.2.6 Virtuelle PC'er

Med firewall'en på plads og med administrator brugere oprettet (se afsnit 5.5.1.1 Administrator) blev den første virtuelle computer G5-PC4-HR opsat og installeret. Der blev brugt følgende specifikationer:

- ESXi server: 10.100.0.39
- OS: Windows 10 Education N
- 2 CPU kerner
- 8 GB RAM

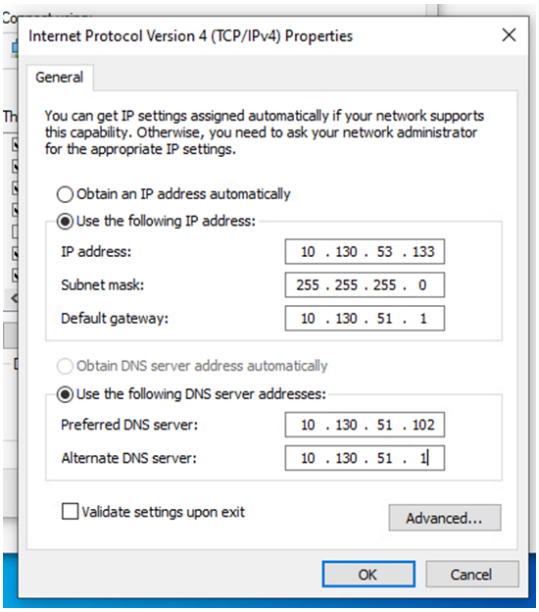
- 60 GB harddisk (Thin Provision) på G5-SSD
- Network Adapter forbindes til VLAN 3051 "LAN"
- ISO fil: Windows 10 Education N



Billede 5.2.2.6.1: Oversigt over PC specifikationer

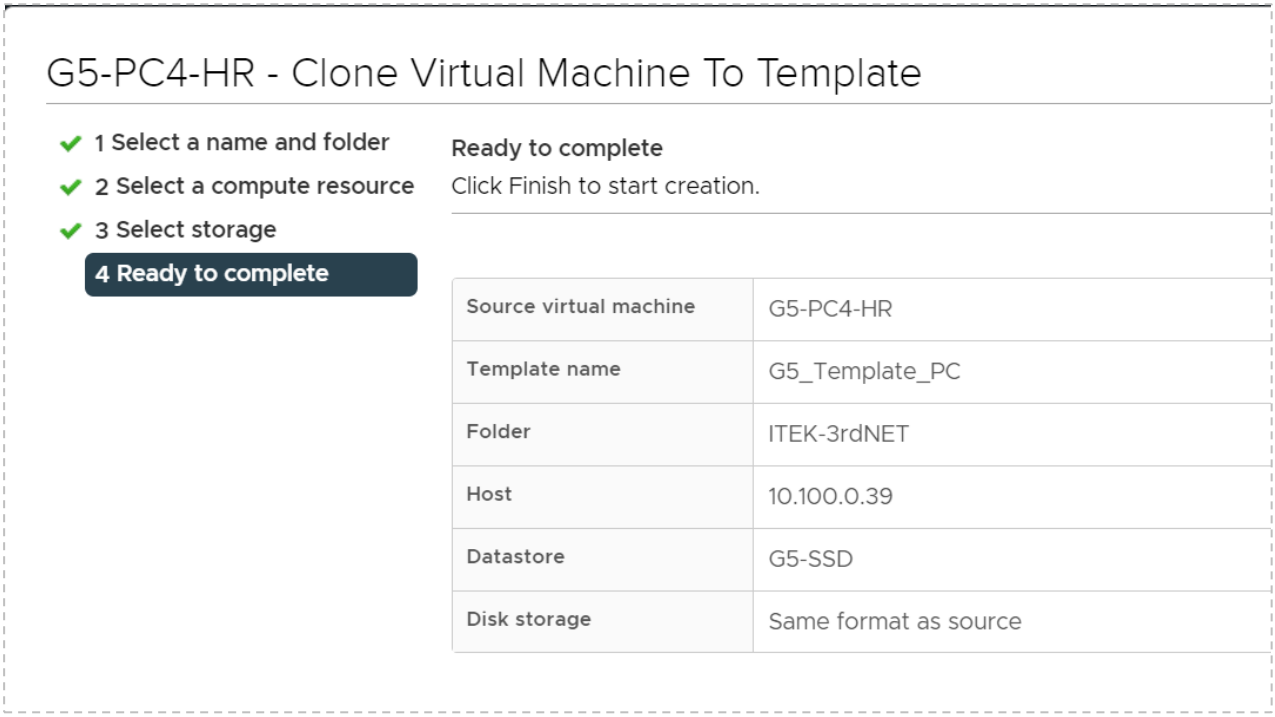
Efter succesfuld installation blev følgende foretaget:

- ➔ Opsætning af statisk ip: 10.130.53.133/24
- ➔ Opsætning af default gateway: 10.130.51.1
- ➔ Opsætning af DNS: 10.130.51.102
- ➔ Fuld opdatering med Windows Update
- ➔ Installation af VMware Tools
- ➔ Installation af AVG Antivirus
- ➔ Installation af Google Chrome browser
- ➔ Join to domain "G5"
- ➔ Oprettelse af gendannelsespunkt



Billede 5.2.2.6.2: IP konfiguration på PC

Herefter blev pc'en lukket ned og en template baseret på den virtuelle maskine blev dannet.



Billede 5.2.2.6.3: Der laves template ud fra PC

Dette er en basisopsætning for PC'er og denne vil kunne klones til nye virtuelle PC'er ud fra det oprettede template. På sigt vil denne PC skulle kobles på Office VLAN 3053 og have en ny ip-adresse, som jf. Bilag 5: IP Plan er 10.130.53.133/24. Af tidsmæssige årsager vil denne omstrukturering muligvis blive udeladt. Det er fra tidligere dokumenteret, at forbindelse kan opnås mellem PC'er i forskellige VLAN, som vist i GNS3 sektionen.

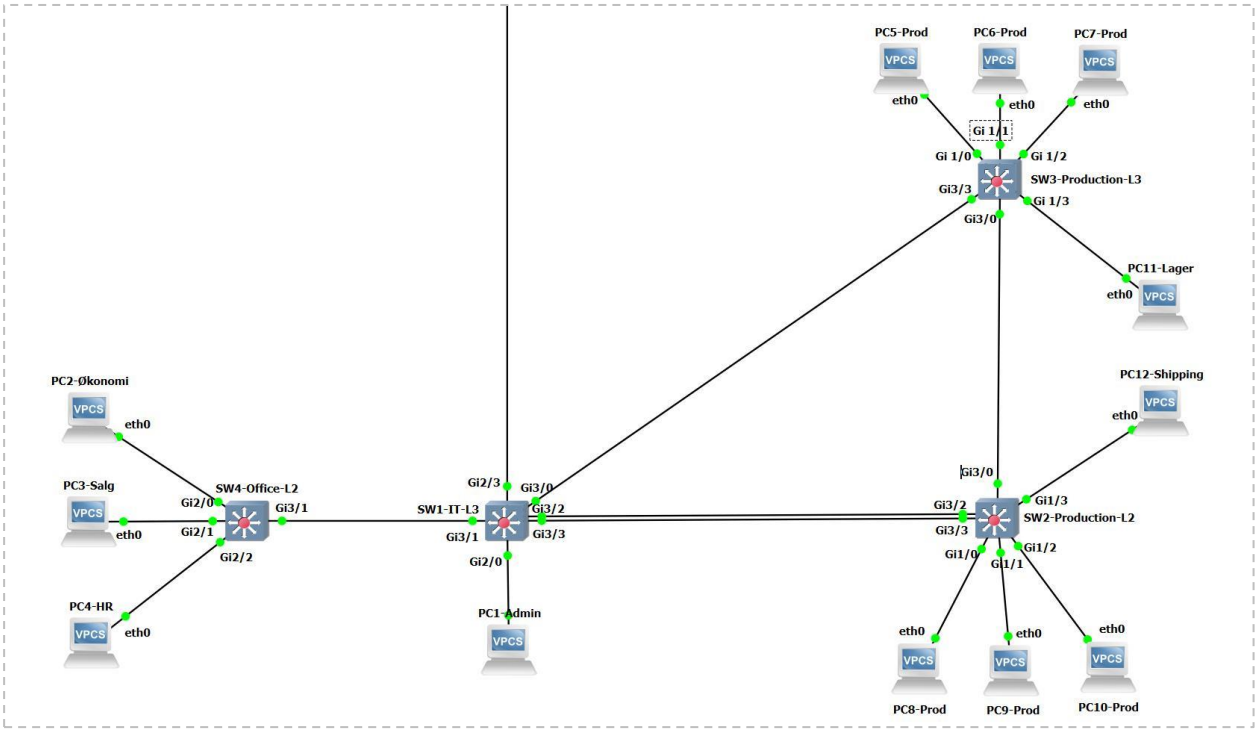
5.3 Netværk (GNS3)

De følgende underafsnit fokuserer på designet, opsætningen og konfigurationen af netværksløsningen, som skal illustrere virksomhedens nye it-infrastruktur. Netværksløsningen opsættes her med brug af softwaren GNS3 og baserer sig på de krav, der blev opstillet i afsnit 4. Krav. Cheatsheet med konfigurationer findes i Bilag 6: Cheatsheet. GNS3 topologien findes i Bilag 7: GNS3 Topologi, og de fire switches' individuelle konfigurationer findes i Bilag 8-11: Conf-fil, SWX. Yderligere leveres GNS3 projektet Project4_GNS3.gns3project som projektfil i Bilag 12.

Dette afsnit deles op i følgende underafsnit: 5.3.1 Design, 5.3.2 Implementering og 5.3.3 Test af GNS3 infrastruktur.

5.3.1 Design

Brugen af GNS3 gør det muligt at teste netværkskonfigurationerne i et virtuelt miljø og passer sig godt til dette eksamensprojekt. GNS3 opsætningen som illustreret nedenfor baserer sig på det tidligere udformede topologidesign omtalt i afsnit 5.1.1 Topologi design.



Billede 5.3.2.1.1: GNS3 topologi

Som det ses deles enhederne i GNS3 op i afdelingerne Office, IT og Production. Hver PC i Office netværket repræsenterer en underafdeling. I produktionen repræsenterer PC11 og PC12 ligeledes hver sin underafdeling ligesom PC 5-10 repræsenterer produktionsafdelingen. For at simplificere topologien repræsenteres kun et udvalg af PC'er og ikke alle de PC-enheder, som det forventes skulle udgøre den endelige opsætning i virksomheden. Ligeledes er det ikke muligt at illustrere access points i GNS3 opsætningen, så overvejelserne omkring disse står kun beskrevet i afsnit 5.1.1 Topologi design.

Alle PC'er i netværket skal kunne opnå forbindelse til DHCP og via DORA processen få tildelt en IP adresse. PC'er i det ene VLAN skal v.h.a. ICMP kunne pinge PC'er i et andet VLAN, alle fire switches samt pinge 8.8.8.8. Sidstnævnte tester forbindelsen ud til internettet. Denne kommunikation mellem VLANs vil foregå v.h.a. trunking.

For nemhedens skyld navngives switches med "switch nr. + afdeling + switch type", hvilket bør overskueliggøre konfigurationerne i konfigurationsfilen.

5.3.2 Implementering

Efter at have klarlagt det overordnede topologidesign blev GNS3 projektet oprettet med en cloud og en switch, som skulle agere som et WAN bindeled til ESXi serveren. Disse udgør ikke en del af den endelige it-infrastruktur, men fungerer udelukkende figurativt så vores netværksløsning kan tilgå internettet.

Efter denne opstart blev der indsat fire switches - to Layer 3 switches med routing funktionalitet og to Layer 2 switches samt et mindre antal PC'er. Disse enheder blev herefter forbundet, hvorefter en basiskonfiguration af de fire switches blev foretaget.

Fælles password og ip route blev sat på alle switches, VLANs blev opsat og navngivet inden for den tildelte range 3050-3059, som det fremgår af Bilag 5: IP Plan og herefter blev VLANs tilknyttet et fast interface på hver switch.

```
Common

Enable secret 3semNET!
Username test password test
Username ck password 3semNET!

ip route 0.0.0.0 0.0.0.0 10.130.51.1

Switch Common:

vlan 3051
name LAN
vlan 3053
name Office
vlan 3054
name Production
vlan 3059
name Guest

 interface range gi0/0 - 3
 description LAN
 no negotiation auto

 interface range gi1/0 - 3
 description Production
 no negotiation auto

 interface range gi2/0 - 3
 description Office
 no negotiation auto

 interface range gi3/0 - 3
```

Billede 5.3.2.1: Udsnit af Cheatsheet (bilag 6)

Til højre vises netop disse konfigurationer fra sektionen Common og Switch Common i Bilag 6: Cheatsheet.

En kommando kan også vise, hvilke porte der er tilknyttet de enkelte VLANs.

```
SW1-IT-L3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
3050 Devices                          active
3051 LAN                              active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
3053 Office                           active    Gi2/0, Gi2/1, Gi2/2
3054 Production                       active    Gi1/0, Gi1/1, Gi1/2, Gi1/3
3059 Guest                            active
```

Billede 5.3.2.2: Visning af VLANs og interface tilknytninger

Guest kunne fx sagtens forbindes til en specifik port, men det var ikke nødvendigt for projektet at have alle VLANs forbundne. Ensartethed i konfigurationen blev prioriteret.

5.3.2.1 Opsætning af protokoller

5.3.2.1.1 DTP (Dynamic Trunking Protocol)

VLAN Trunking er en nødvendighed for at netværksenhederne kan kommunikere sammen på tværs af VLANs. I korte træk er VLAN Trunk en protokol, der understøtter alle VLANs kendt af de enkelte switches og som kan opsættes simpelt med en statisk konfiguration[7], som det er gjort i dette GNS3 projekt. Protokollen skal opsættes på alle forbindelser i netværket for at hosts kan få adgang til VLANs og switches kan overføre pakker til hosts i andre VLANs.

Der konfigureres to typer af switchport modes: Trunk og Access. Per default er mode sat til auto som favoriserer Access. Derfor skal mode ændres, før man kan aktivere Trunk tilstanden. Dette gøres som vist i Bilag 6: Cheatsheet under Switch Common > `interface range gi3/0-3`:

[7] s. 30, "CCNA Routing and Switching ICND2 200-105 Official Cert Guide" af Wendell Odom

```
description Trunk
no negotiation auto
switchport trunk encapsulation dot1q
switchport mode trunk
```

Billede 5.3.2.1.1: Udsnit af Cheatsheet

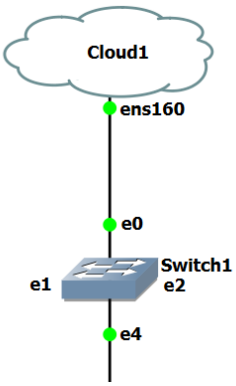
Her deaktiveres `auto negotiation`, således at tilstanden kan ændres manuelt til `trunk encapsulation dot1q` og `trunk mode` kan herefter aktiveres. Dette gør sig gældende for alle interfaces i Gi3/0-3 - dette er de interfaces, som forbinder alle switches med hinanden.
For at en host kan sende en pakke til en anden host i et andet VLAN, skal forbindelserne mellem switches være i `trunk mode` - dette er uanset om VLAN er en anden eller den samme, så længe at pakken skal igennem mere end én switch.

De resterende forbindelser på interfaces Gi0/0-3, Gi1/0-3 og Gi2/0-3 sættes i `access mode`, hvor der ligeledes angives hvilke VLANs de enkelte interfaces kan få adgang til, da de forbinder hosts til switches og dermed kun skal have adgang til VLANs - og ikke mere end det. Konfigurationen for disse kan ses på billede 5.3.2.1.2.

Som en sidenote kan nævnes, at Switch1, som har internetopkoblingen, ligeledes har fået konfigureret sine porte.

```
interface range gi0/0 - 3
description LAN
no negotiation auto
switchport mode access
switchport access vlan 3051
spanning-tree portfast
spanning-tree bpduguard enable

interface range gi1/0 - 3
description Production
no negotiation auto
switchport mode access
switchport access vlan 3054
spanning-tree portfast
spanning-tree bpduguard enable

interface range gi2/0 - 3
description Office
no negotiation auto
switchport mode access
switchport access vlan 3053
spanning-tree portfast
spanning-tree bpduguard enable
```

Billede 5.3.2.1.2: Udsnit af Cheatsheet



Billede 5.3.2.1.4: Switch1 som set i GNS3

Port	VLAN	Type
0	3050	dot1q
1	3050	access
2	3050	access
3	3050	access
4	3050	dot1q

Billede 5.3.2.1.4: Konfiguration af porte i Switch1

```
SW1:

hostname SW1-IT-L3
spanning-tree vlan 3050-3059 priority 8192
snmp-server chassis-id SW1-IT-L3
interface Vlan3051
 ip address 10.130.51.121 255.255.255.0
 No shutdown
interface GigabitEthernet2/3
 description to Cloud
 no negotiation auto
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3050
 switchport mode trunk
 spanning-tree bpdufilter enable
!
```

Billede 5.3.2.1.6: Der forbindes til native vlan 3050 via Gi2/3 til Switch1

Som det ses i et lille udsnit fra konfigurationsvinduet, er port 0 og 4 sat til `encapsulation dot1q` og er dermed trunks. På topologien ses det at Ethernet4 port går ned til SW1-IT-L3 og Ethernet0

porten går til Cloud. For at SW1-IT-L3 kan tilgå internettet, har det været nødvendigt at konfigurere en trunk forbindelse på interface Gi2/3, der er forbundet til Switch1. Ligeledes angives det i konfigurationen at det specifikt er `native vlan 3050`, som den skal skabe forbindelse til.

En simpel test i afsnit 5.3.3.4 Test at trunking vil vise, om vores trunk er aktiv og fungerer.

5.3.2.1.2 RSTP (Rapid Spanning Tree Protocol)

Inden netværket gøres redundant med etherchannel konfigureres RSTP. Formålet med denne protokol er at blokere ARP (Address Resolution Protocol) pakker i at cirkulere i uendelig loop og dermed overbelaste switchene med broadcast storms. Det er et broadcast frame og sendes derfor ud på alle interfaces - med en to-vejs forbindelse mellem SW1-IT-L3 og SW2-Produktion-L2, ville den samme ARP pakke blive sendt på begge interfaces. Modtager switchen ville herefter sende pakken videre ud på alle sine interfaces, og på et tidspunkt vil disse ARP pakker nå retur til den oprindelige sender, som så ville sende dem ud igen.

RSTP bruger BPDUs til at identificere de redundante links og herudfra vælge hvilken port, der er den bedst egnede til at videresende meddelelser. Herefter blokeres nogle interfaces fra at sende datapakker ud, men de kan godt modtage. På denne måde brydes loop'en.

Til højre ses konfigurationen af Rapid Spanning Tree på SW1-IT-L3. Ud fra bridgeværdien som udgøres af prioritet og MAC adresse, vælges dén switch med laveste værdi som ROOT og de andre switches som enten DESIGNATED PORT eller ALTERNATIVE PORT. Sidstnævnte er i blocking state, hvor de to førstnævnte er i forwarding state.[8] En test af RSTP funktionen kan ses i afsnit 5.3.3.5 Test af Rapid Spanning Tree Protocol.

```
SW1:

hostname SW1-IT-L3
spanning-tree vlan 3050-3059 priority 8192
snmp-server chassis-id SW1-IT-L3
interface Vlan3051
```

Billede 5.3.2.1.2.1: Udsnit af Cheatsheet

[8] https://networklessons.com/spanning-tree/introduction-to-spanning-tree

Når et link eller en forbindelse fejler, vil én af de blokerede porte øjeblikkeligt blive sat i forwarding state udenom de andre tilstande (listening og learning), såfremt Portfast er aktiveret på det pågældende interface. I Bilag 6: Cheatsheet fremgår det af Switch Common-sektionen at følgende interfaces har aktiv Portfast: Gi0/0-3, Gi1/0-3 og Gi2/0-3. Dette illustreres også ved billede 5.3.2.1.2.2 til højre.

```
spanning-tree mode rapid-pvst
interface range gi0/0 - 3
description LAN
spanning-tree portfast
spanning-tree bpduguard enable

interface range gi1/0 - 3
description Production
spanning-tree portfast
spanning-tree bpduguard enable

interface range gi2/0 - 3
description Office
spanning-tree portfast
spanning-tree bpduguard enable

interface range gi3/0 - 3
description Trunk
no spanning-tree portfast
no spanning-tree bpduguard enable
```

Billede 5.3.2.1.2.2: Udsnit af Cheatsheet

Slutteligt skal spanning tree topologien beskyttes mod udefrakommende trusler. RSPT udsender og modtager BPDUs på alle interfaces - og dette skal modificeres, således at BPDUs sendt fra PC interfaces blokeres. Dette for at forhindre ubudne gæster i at tilslutte en PC direkte til en switch og med et værktøj, at kunne generere BPDUs med højere bridgeværdi. I et sådant tilfælde ville PC'en blive den nye root bridge og al trafik fra netværkets switches ville således gå igennem PC'en. Med et program som Wireshark ville den ubudne gæst kunne tilegne sig enorme mængder af data.[9] Derfor blev switchene konfigureret i Switch Common sektionen, som vist i Bilag 6: Cheatsheet (og i udsnittet fra billede 5.3.2.1.2.2) til at aktivere BPDU Guard på interfaces Gi0/0-3, Gi 1/0-3 og Gi 2/0-3. BPDU Guard sætter de interfaces, der modtager BPDUs i `err-disable mode`. BPDU Guard deaktiveres på interface Gi3/0-3, da alle forbindelser mellem netværkets switches er forbundet på disse interfaces.

5.3.2.1.3 SNMP (Simple Network Management Protocol)

SNMP er en protokol, der bruges til at hente statistisk data fra netværksenheder. Disse data gemmes på eksterne servere og kan tilgås ved at oprette forbindelse til et program som fx MIB Browseren. Forbindelsen til browseren skal foretages fra en PC i netværket.

For at monitorering skal være succesfuld, oprettes snmp-server community og snmp-server contact i den grundlæggende konfigurering og i den individuelle konfigurering af switches tilføjes en snmp-server chassis-id. Konfigurationen kan ses i nedenstående udsnit fra switch-konsollen:

```
SW1-IT-L3#show running-config | include snmp
snmp-server community ITEK3sem RO
snmp-server contact eaackol@students.eaaa.dk
snmp-server chassis-id SW1-IT-L3
```

```
SW2-Production-L2#show running-config | include snmp
snmp-server community ITEK3sem RO
snmp-server contact eaackol@students.eaaa.dk
snmp-server chassis-id SW2-Production-L2
```

[9] "Spanning Tree BPDU guard" af NetworkLessons.com

```
SW3-Production-L3#show running-config | include snmp
snmp-server community ITEK3sem RO
snmp-server contact eaackol@students.eaaa.dk
snmp-server chassis-id SW3-Production-L3
```

```
SW4-Office-L2#show running-config | include snmp
snmp-server community ITEK3sem RO
snmp-server contact eaackol@students.eaaa.dk
snmp-server chassis-id SW4-Office-L2
```

Funktionaliteten af SNMP konfigurationen testes i afsnit 5.3.3.6 Test af SNMP.

5.3.2.1.4 VRRP (Virtual Router Redundancy Protocol)

VRRP bruges til at sikre høj tilgængelighed ved at tillade flere lag 3 switches samarbejder og præsentere en enkelt virtuel IP-adresse og gateway for hosts på subnettet. Hvis den primære eller master switch svigter, overtager den næste switch så netværket forbliver sikret.

I konfigurationsfilen Bilag 6: Cheatsheet, opsættes VRRP på tre VLANs: Office, Production og Guest. Det giver dermed redundans og høj tilgængelighed for enhederne på de tre VLANs. Det sikrer så, at hvis master switch fejler, findes den næste med højeste prioritet. Ved at have en virtuel IP-adresse, kan trafikken i netværket bestemme retningen til den næste master.

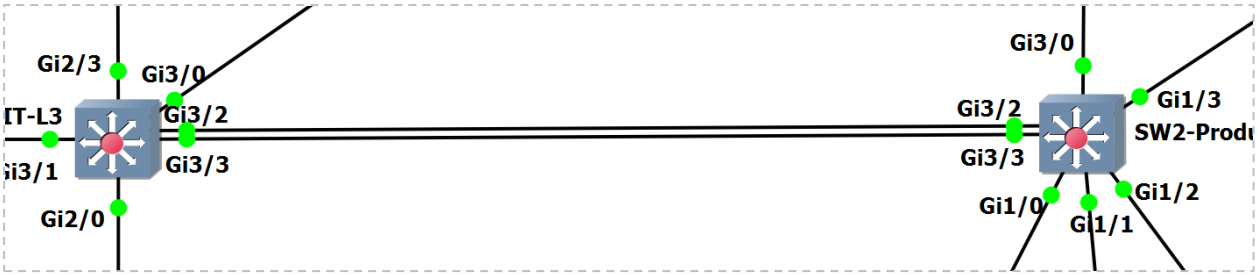
```
interface Vlan3053
 description Office
 ip address 10.130.53.121 255.255.255.0
 vrrp 53 ip 10.130.53.1
 vrrp 53 priority 110
 vrrp 53 track 1 decrement 20
!
interface Vlan3054
 description Production
 ip address 10.130.54.121 255.255.255.0
 vrrp 54 ip 10.130.54.1
 vrrp 54 priority 110
 vrrp 54 track 1 decrement 20
!
interface Vlan3059
 description Guest
 ip address 10.130.59.121 255.255.255.0
 vrrp 59 ip 10.130.59.1
 vrrp 59 priority 110
 vrrp 59 track 1 decrement 20
!
```

Billede 5.3.2.1.4.1: vrrp for VLAN-interfaces

På billede 5.3.2.1.4.1, vises hvordan hver VLAN-interface - VLAN 3053, 3054 og 3059 - har en tilknyttet vrrp gruppe, som så har et unikt ID - 53,54 og 59 - og deraf den fælles virtuelle IP-adresse - 10.130.5X.1. Prioriteten afgør så hvilken enhed der bliver master. Samlet set giver vrrp redundans til netværket og minimerer downtime i tilfælde af problemer.

5.3.2.2 Opsætning af etherchannel

Jf. de opstillede krav i afsnit 4. Krav, er der behov for et redundant netværk, hvor der altid er sikret forbindelse, hvis et link skulle gå ned. Til dette formål integrerer vi en etherchannel - dette gøres mellem SW1-IT-L3 og SW2-Production-L2 på Gi3/2-3 interfaces. I GNS3 ser etherchannel således ud:



Billede 5.3.2.2.1: Etherchannel set i GNS3

Udover at brugen af flere links mellem samme enheder skaber et redundant netværk, så har en etherchannel også den store fordel, at sammenlægningen (link aggregation) af de individuelle links forhøjer den samlede båndbredde. Fx vil to 1Gbit forbindelser sammenlagt give en båndbredde på 2Gbit. Så hvor 1 gigabit (Gb/Gbit) = 1.000.000.000 bits vil en 2Gbit forbindelse have 2.000.000.000 bits. En test af hvorvidt konfigurationen af link aggregation fungerer demonstreres i afsnit 3.5.5.8 Test af Etherchannel.

I nedenstående konfigurationer fra Bilag 6: Cheatsheet vil man også se, at etherchannel er konfigureret som en trunk. Alle ændringer til en etherchannel bør foregå i `interface port-channel1`[10], hvorfor det også er heri trunk switchports er konfigureret. Det er af samme årsag at switchport konfigurationerne fjernes fra interface Gi3/2-3.

SW1-IT-L3	SW2-Production_L2

`interface range gi3/2 - 3`
` no switchport mode trunk`
` no switchport trunk encapsulation dot1q`
` no description Trunk`
` negotiation auto`
`end`
`!`
`interface port-channel1`
` description Trunk`
` switchport trunk encapsulation dot1q`
` switchport mode trunk`
` no negotiation auto`
`end`
	`interface range gi3/2 - 3`
	` no switchport mode trunk`
	` no switchport trunk encapsulation dot1q`
	` no description Trunk`
	` negotiation auto`
	` channel-group 1 mode on`
	`!`
	`interface port-channel1`
	` description Trunk`
	` switchport trunk encapsulation dot1q`
	` switchport mode trunk`
	` no negotiation auto`
	`end`

[10] Etherchannel on Cisco IOS Catalyst Switch (networklessons.com)

5.3.3 Test af GNS3 infrastruktur

5.3.3.1 Test af DHCP

Efter den grundlæggende basiskonfiguration blev det testet at PC'erne kunne få forbindelse til DHCP. Her er der taget udgangspunkt i PC1 og PC2 fra VLAN 3053 og PC 10 og PC11 fra VLAN 3054.

```
PC1-Admin> dhcp
DDORA IP 10.130.53.2/24 GW 10.130.53.1
```

```
PC2-Økonomi> dhcp
DDORA IP 10.130.53.3/24 GW 10.130.53.1
```

```
PC11-Lager> dhcp
DDORA IP 10.130.54.2/24 GW 10.130.54.1
```

```
PC10-Prod> dhcp
DDORA IP 10.130.54.3/24 GW 10.130.54.1
```

Billede 5.3.3.1.1: dhcp test i GNS3 PC konsoller

Som set i billede 5.3.3.1.1 kunne det bekræftes at dhcp fungerede som forventet.

5.3.3.2 Test af forbindelse til VLANs switch & main switch

5.3.3.2.1 Første test

Efter dhcp test blev det først testet, hvorvidt PC'erne kunne pinge deres egen gateway - for VLAN 3053 er default gateway 10.130.53.1 og for VLAN 3054 er default gateway 10.130.54.1.

```
PC1-Admin> ping 10.130.53.1

84 bytes from 10.130.53.1 icmp_seq=1 ttl=255 time=4.773 ms
84 bytes from 10.130.53.1 icmp_seq=2 ttl=255 time=3.554 ms
84 bytes from 10.130.53.1 icmp_seq=3 ttl=255 time=3.308 ms
84 bytes from 10.130.53.1 icmp_seq=4 ttl=255 time=1.398 ms
84 bytes from 10.130.53.1 icmp_seq=5 ttl=255 time=4.948 ms
```

Billede 5.3.3.2.1.1: Ping til egen default gateway fra PC1

```
PC2-Økonomi> ping 10.130.53.1

84 bytes from 10.130.53.1 icmp_seq=1 ttl=255 time=4.480 ms
84 bytes from 10.130.53.1 icmp_seq=2 ttl=255 time=4.135 ms
84 bytes from 10.130.53.1 icmp_seq=3 ttl=255 time=10.230 ms
84 bytes from 10.130.53.1 icmp_seq=4 ttl=255 time=4.352 ms
84 bytes from 10.130.53.1 icmp_seq=5 ttl=255 time=25.837 ms
```

Billede 5.3.3.2.1.2: Ping til egen default gateway fra PC2

```
PC10-Prod> ping 10.130.54.1

84 bytes from 10.130.54.1 icmp_seq=1 ttl=255 time=6.402 ms
84 bytes from 10.130.54.1 icmp_seq=2 ttl=255 time=6.581 ms
84 bytes from 10.130.54.1 icmp_seq=3 ttl=255 time=6.687 ms
84 bytes from 10.130.54.1 icmp_seq=4 ttl=255 time=7.389 ms
84 bytes from 10.130.54.1 icmp_seq=5 ttl=255 time=6.854 ms
```

Billede 5.3.3.2.1.3: Ping til egen default gateway fra PC10

```
PC11-Lager> ping 10.130.54.1

84 bytes from 10.130.54.1 icmp_seq=1 ttl=255 time=7.308 ms
84 bytes from 10.130.54.1 icmp_seq=2 ttl=255 time=7.106 ms
84 bytes from 10.130.54.1 icmp_seq=3 ttl=255 time=7.127 ms
84 bytes from 10.130.54.1 icmp_seq=4 ttl=255 time=7.729 ms
84 bytes from 10.130.54.1 icmp_seq=5 ttl=255 time=4.780 ms
```

Billede 5.3.3.2.1.4: Ping til egen default gateway fra PC11

5.3.3.2.2 Anden test

Efter at have bekræftet forbindelsen fra PC'erne til deres eget VLANs gateway, testede vi forbindelsen til main switchens gateway - den som fungerer som vores router. Der er default gateway 10.130.51.1 og ligger i VLAN "LAN".

```
PC1-Admin> ping 10.130.51.1

84 bytes from 10.130.51.1 icmp_seq=1 ttl=63 time=6.236 ms
84 bytes from 10.130.51.1 icmp_seq=2 ttl=63 time=6.210 ms
84 bytes from 10.130.51.1 icmp_seq=3 ttl=63 time=2.731 ms
84 bytes from 10.130.51.1 icmp_seq=4 ttl=63 time=3.248 ms
84 bytes from 10.130.51.1 icmp_seq=5 ttl=63 time=5.331 ms
```

Billede 5.3.3.2.2.1: Ping til 1.130.51.1 fra PC1

```
PC2-Økonomi> ping 10.130.51.1

84 bytes from 10.130.51.1 icmp_seq=1 ttl=63 time=9.662 ms
84 bytes from 10.130.51.1 icmp_seq=2 ttl=63 time=9.451 ms
84 bytes from 10.130.51.1 icmp_seq=3 ttl=63 time=9.463 ms
84 bytes from 10.130.51.1 icmp_seq=4 ttl=63 time=6.080 ms
84 bytes from 10.130.51.1 icmp_seq=5 ttl=63 time=6.838 ms
```

Billede 5.3.3.2.2.2: Ping til 1.130.51.1 fra PC2

```
PC10-Prod> ping 10.130.51.1

84 bytes from 10.130.51.1 icmp_seq=1 ttl=63 time=6.717 ms
84 bytes from 10.130.51.1 icmp_seq=2 ttl=63 time=10.624 ms
84 bytes from 10.130.51.1 icmp_seq=3 ttl=63 time=5.773 ms
84 bytes from 10.130.51.1 icmp_seq=4 ttl=63 time=5.078 ms
84 bytes from 10.130.51.1 icmp_seq=5 ttl=63 time=7.789 ms
```

Billede 5.3.3.2.2.3: Ping til 1.130.51.1 fra PC10

```
PC11-Lager> ping 10.130.51.1

84 bytes from 10.130.51.1 icmp_seq=1 ttl=63 time=6.545 ms
84 bytes from 10.130.51.1 icmp_seq=2 ttl=63 time=7.408 ms
84 bytes from 10.130.51.1 icmp_seq=3 ttl=63 time=7.163 ms
84 bytes from 10.130.51.1 icmp_seq=4 ttl=63 time=4.485 ms
84 bytes from 10.130.51.1 icmp_seq=5 ttl=63 time=5.152 ms
```

Billede 5.3.3.2.2.4: Ping til 1.130.51.1 fra PC11

5.3.3.3 Test af forbindelse til Google's server

Som sidste skridt blev det testet om PC'erne og de fire switches kunne pinge Google's nameserver 8.8.8.8.

```
PC1-Admin> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=53 time=10.088 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=53 time=20.465 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=53 time=9.279 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=53 time=8.704 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=53 time=7.929 ms
```

Billede 5.3.3.3.1: Ping til 8.8.8.8 fra PC1

```
PC2-Økonomi> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=53 time=29.917 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=53 time=9.853 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=53 time=12.589 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=53 time=13.146 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=53 time=11.385 ms
```

Billede 5.3.3.3.2: Ping til 8.8.8.8 fra PC2

```
PC10-Prod> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=53 time=11.067 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=53 time=11.238 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=53 time=10.271 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=53 time=13.813 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=53 time=12.165 ms
```

Billede 5.3.3.3.3: Ping til 8.8.8.8 fra PC10

```
PC11-Lager> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=53 time=10.035 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=53 time=18.926 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=53 time=10.625 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=53 time=11.048 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=53 time=11.883 ms
```

Billede 5.3.3.3.4: Ping til 8.8.8.8 fra PC11

Herefter blev det testet om de to Layer 3 switches kunne pinge Google's nameserver 8.8.8.8.

```
SW1-IT-L3>ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/11 ms
```

Billede 5.3.3.3.5: Ping til 8.8.8.8 fra SW1-IT-L3

```
SW3-Production-L3>ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/17 ms
```

Billede 5.3.3.3.6: Ping til 8.8.8.8 fra SW3-Production-L3

Dette kunne lade sig gøre grundet den konfigurerede:

`ip route to 0.0.0.0 0.0.0.0 10.130.51.1.`

5.3.3.4 Test af Trunking

5.3.3.4.1 Første test

Den første test viser alle trunks, om de er aktive, om der bruges dot1q protokol (802.1q) og hvilken state de befinder sig i. Testen vil også vise, hvilke VLANs der er tilladt på hvilke porte samt hvilke VLANs, der er sat i spanning tree forwarding state. Kommandoen `show interface trunk` bruges.

```
SW1-IT-L3#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi2/3       on               802.1q         trunking      3050
Gi3/0       on               802.1q         trunking      1
Gi3/1       on               802.1q         trunking      1
Po1         on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi2/3       1-4094
Gi3/0       1-4094
Gi3/1       1-4094
Po1         1-4094

Port        Vlans allowed and active in management domain
Gi2/3       1,3050-3051,3053-3054,3059
Gi3/0       1,3050-3051,3053-3054,3059
Gi3/1       1,3050-3051,3053-3054,3059
Po1         1,3050-3051,3053-3054,3059

Port        Vlans in spanning tree forwarding state and not pruned
Gi2/3       1,3050-3051,3053-3054,3059
Gi3/0       1,3050-3051,3053-3054,3059
Gi3/1       1,3050-3051,3053-3054,3059

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,3050-3051,3053-3054,3059
```

Billede 5.3.3.4.1.1: Visning af trunk interfaces på SW1-IT-L3

```
SW2-Production-L2#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi3/0       on               802.1q         trunking      1
Gi3/1       on               802.1q         trunking      1
Po1         on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi3/0       1-4094
Gi3/1       1-4094
Po1         1-4094

Port        Vlans allowed and active in management domain
Gi3/0       1,3051,3053-3054,3059
Gi3/1       1,3051,3053-3054,3059
Po1         1,3051,3053-3054,3059

Port        Vlans in spanning tree forwarding state and not pruned
Gi3/0       1,3051,3053-3054,3059
Gi3/1       1,3051,3053-3054,3059
Po1         1,3051,3053-3054,3059
```

Billede 5.3.3.4.1.2: Visning af trunk interfaces på SW2-Production-L2

```
SW3-Production-L3#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi3/0       on               802.1q         trunking      1
Gi3/1       on               802.1q         trunking      1
Gi3/2       on               802.1q         trunking      1
Gi3/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi3/0       1-4094
Gi3/1       1-4094
Gi3/2       1-4094
Gi3/3       1-4094

Port        Vlans allowed and active in management domain
Gi3/0       1,3051,3053-3054,3059
Gi3/1       1,3051,3053-3054,3059
Gi3/2       1,3051,3053-3054,3059
Gi3/3       1,3051,3053-3054,3059

Port        Vlans in spanning tree forwarding state and not pruned
Gi3/0       none
Gi3/1       1,3051,3053-3054,3059
Gi3/2       1,3051,3053-3054,3059

Port        Vlans in spanning tree forwarding state and not pruned
Gi3/3       1,3051,3053-3054,3059
```

Billede 5.3.3.4.1.3: Visning af trunk interfaces på SW3-Production-L3

```
SW4-Office-L2#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi3/0       on               802.1q         trunking      1
Gi3/1       on               802.1q         trunking      1
Gi3/2       on               802.1q         trunking      1
Gi3/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi3/0       1-4094
Gi3/1       1-4094
Gi3/2       1-4094
Gi3/3       1-4094

Port        Vlans allowed and active in management domain
Gi3/0       1,3051,3053-3054,3059
Gi3/1       1,3051,3053-3054,3059
Gi3/2       1,3051,3053-3054,3059
Gi3/3       1,3051,3053-3054,3059

Port        Vlans in spanning tree forwarding state and not pruned
Gi3/0       1,3051,3053-3054,3059
Gi3/1       1,3051,3053-3054,3059
Gi3/2       1,3051,3053-3054,3059

Port        Vlans in spanning tree forwarding state and not pruned
Gi3/3       1,3051,3053-3054,3059
```

Billede 5.3.3.4.1.4: Visning af trunk interfaces på SW4-Office-L2

5.3.3.4.2 Anden test

Den næste test skal dokumentere, hvorvidt en PC i ét VLAN kan pinge en PC i et andet VLAN og dermed bekræfte funktionaliteten af trunking.

```
PC2-Økonomi> dhcp
DORA IP 10.130.53.3/24 GW 10.130.53.1

PC2-Økonomi> ping 10.130.54.3

84 bytes from 10.130.54.3 icmp_seq=1 ttl=63 time=25.629 ms
84 bytes from 10.130.54.3 icmp_seq=2 ttl=63 time=7.370 ms
84 bytes from 10.130.54.3 icmp_seq=3 ttl=63 time=12.240 ms
84 bytes from 10.130.54.3 icmp_seq=4 ttl=63 time=9.770 ms
84 bytes from 10.130.54.3 icmp_seq=5 ttl=63 time=10.384 ms
```

Billede 5.3.3.4.2.1: Ping fra PC i VLAN 3053 til PC i VLAN 3054

PC2-Økonomi befinder sig i VLAN'et 3053 Office og får her tildelt IP adressen 10.130.53.3/24. Herefter bekræftes det at PC2-Økonomi kan pinge PC10-Prod, der befinder sig i VLAN 3054.

Konklusion: trunking protokollen er aktiv.

5.3.3.5 Test af Rapid Spanning Tree Protocol

Før der skulle testes for RSTP, startede man ved kommandoen `spanning-tree bpdufilter enable`. Denne kommando konfigurerer BPDU-filtrering på en given switchport. Normalt er BPDU-filtrering deaktiveret som standard på switchport, men ved brug af denne kommando aktiveres BPDU-filtrering på den specifikke port.

For at test af STP skulle starte, kræves der en blokering eller suspendering af et af kablerne, her suspender man linket mellem SW2 og SW3 via port Gi3/0. Dette kan ses på nedenstående screenshot der viser før suspendering, hvor Gi3/0 har en `Alternate Role`. Dette fortæller at linket er blokeret mellem de to switches.

```
SW3-Production-L3#sh spanning-tree vlan 3051

VLAN3051
  Spanning tree enabled protocol rstp
  Root ID    Priority    11243
             Address     0c71.6d5a.0000
             Cost        4
             Port        16 (GigabitEthernet3/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    35819  (priority 32768 sys-id-ext 3051)
             Address     0ce5.2746.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    P2p Edge
Gi0/1               Desg FWD 4         128.2    P2p Edge
Gi0/2               Desg FWD 4         128.3    P2p Edge
Gi0/3               Desg FWD 4         128.4    P2p Edge
Gi3/0               Altn BLK 4         128.13   P2p
Gi3/1               Desg FWD 4         128.14   P2p
Gi3/2               Desg FWD 4         128.15   P2p
```

Billede 5.3.3.5.1: Port states på SW3-Production-L3

På nedenstående screenshot, hvor der også blev kørt sh spanning-tree vlan 3051, kan det ses hvordan Gi3/0 opfører sig efter suspendering. Gi3/0 er nu blevet root mellem de to switches og er blevet valgt som dén switch med den højeste prioritet.

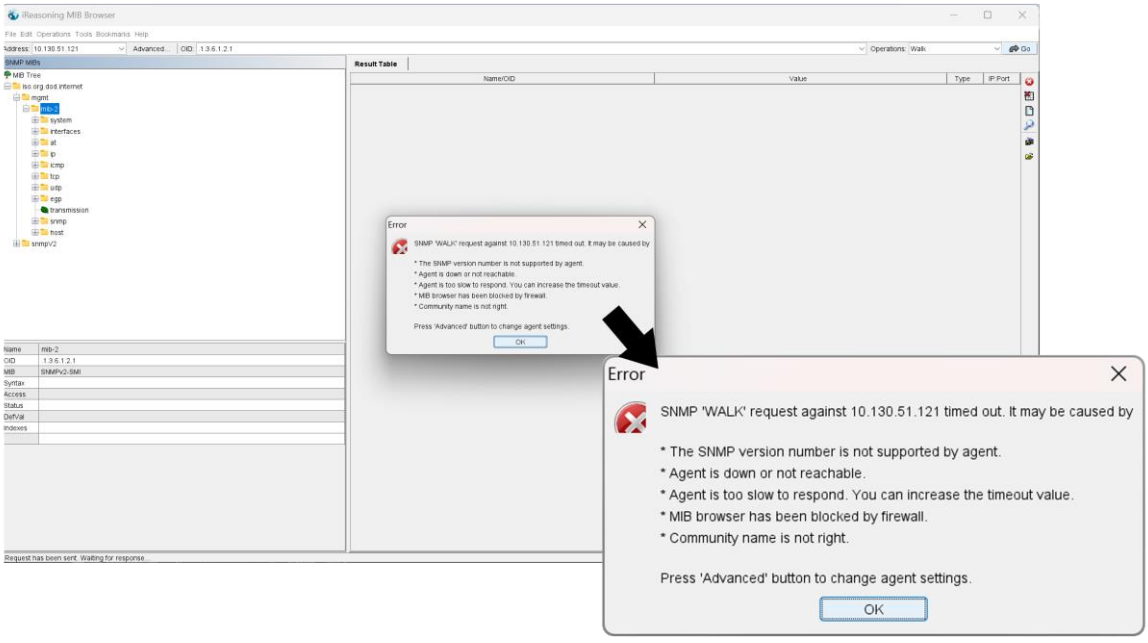
```
  Root ID    Priority    11243
             Address     0c71.6d5a.0000
             Cost        7
             Port        13 (GigabitEthernet3/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    35819  (priority 32768 sys-id-ext 3051)
             Address     0ce5.2746.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    P2p Edge
Gi0/1               Desg FWD 4         128.2    P2p Edge
Gi0/2               Desg FWD 4         128.3    P2p Edge
Gi0/3               Desg FWD 4         128.4    P2p Edge
Gi3/0               Root FWD 4         128.13   P2p
Gi3/1               Desg BLK 4         128.14   P2p
Gi3/2               Desg BLK 4         128.15   P2p

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
```

Billede 5.3.3.5.2: Gi3/0 på SW3-Production-L3 er nu i ROOT MODE

5.3.3.6 Test af SNMP

5.3.3.6.1 Første test

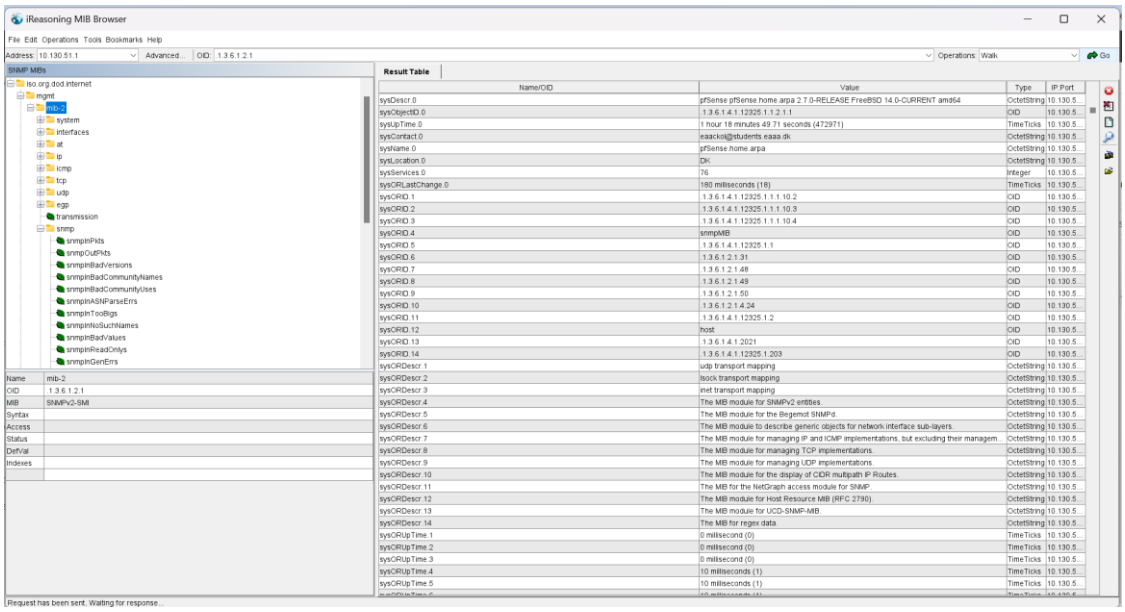
Ved den første test i MIB Browser, fremkom nedenstående fejlmeddelelse.



Billede 5.3.3.6.1.1: Fejlmeddelelse ved kørsel af MIB browser

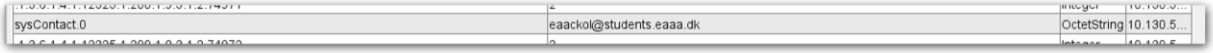
5.3.3.6.2 Anden test

Efter at have aktiveret SNMP-reglen i pfSense Firewall'en (se afsnit 5.4.1.1.5 SNMP) lykkedes det at trække OIDs ud med MIB Browseren. Dette ses på billede 5.3.3.6.2.1.



Billede 5.3.3.6.2.1: Succesfuld kørsel af MIB browser

Under syscontact ses den konfigurerede e-mail adresse, som bekræfter korrekt opsætning.



Billede 5.3.3.6.2.2: e-mail konfigureret i Cheatsheet ses i MIB browser

5.3.3.7 Test af VRRP

For at verificere at vrrp protokollen er oppe at køre som den skal, bruges kommandoen `show vrrp` på main switchen SW1-IT-L3. Som det ses nedenfor er konfigurationen aktiv på alle VLANs undtagen 3051 - LAN interfacet. For hvert VLAN er der angivet en master router og en prioritet. `priority 110` angiver at alle enheder har samme prioritet. SW1-IT-L3 fungerer som master i dette tilfælde.

Ved hjælp af kommandoen `track 1 ip route 0.0.0.0/0 reachability` som set i Bilag 6: Cheatsheet under sektionen L3-SW1, blev der oprettet et track, der har til formål at overvåge tilgængeligheden af en default route, nemlig (0.0.0.0/0).

Hvis default route bliver utilgængelig og gateway går ned, vil `track 1` kunne ændre sin tilstand. VRRP reducerer herefter `master priority` med det angivne point, det vil sige 20, og på den måde sikrer, at den mest tilgængelige enhed tager rollen som master, da denne nu har en lavere prioritet. 100 er default prioritet. Dette ses på billede 5.3.3.7.1.

```
SW1-IT-L3#sh vrrp
Vlan3053 - Group 53
  State is Master
  Virtual IP address is 10.130.53.1
  Virtual MAC address is 0000.5e00.0135
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 110
    Track object 1 state Up decrement 20
  Master Router is 10.130.53.121 (local), priority is 110
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.570 sec

Vlan3054 - Group 54
  State is Master
  Virtual IP address is 10.130.54.1
  Virtual MAC address is 0000.5e00.0136
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 110
    Track object 1 state Up decrement 20
  Master Router is 10.130.54.121 (local), priority is 110
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.570 sec

Vlan3059 - Group 59
  State is Master
  Virtual IP address is 10.130.59.1
  Virtual MAC address is 0000.5e00.013b
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 110
    Track object 1 state Up decrement 20
  Master Router is 10.130.59.121 (local), priority is 110
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.570 sec
```

Billede 5.3.3.7.1: VRRP konfiguration på SW1-IT-L3 set i konsollen

5.3.3.8 Test af etherchannel

Efter konfigurationen testes om etherchannel er sat korrekt op. Dette kan let gøres med kommandoerne:

- `sh int gi3/2`
- `sh int gi3/3`
- `sh int port-channel1`

Ved kørsel af kommandoerne kan det bekræftes, at der på interface Gi3/2 og Gi3/3 kun er en båndbredde på 1Gbit. Men at der på `port-channel1` interfacet er en sammenslutning af båndbredden fra 1000000 Kbit til 2000000Kbit.

```
SW1-IT-L3#sh int gi3/2
GigabitEthernet3/2 is up, line protocol is up (connected)
  Hardware is iGbE, address is 0c71.6d5a.000e (bia 0c71.6d5a.000e)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Billede 5.3.3.8.1: SW1-IT-L3 interface Gi3/2 har kun 1Kbit båndbredde

```
SW1-IT-L3#sh int gi3/3
GigabitEthernet3/3 is up, line protocol is up (connected)
  Hardware is iGbE, address is 0c71.6d5a.000f (bia 0c71.6d5a.000f)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Billede 5.3.3.8.2: SW1-IT-L3 interface Gi3/3 har kun 1Kbit båndbredde

```
SW1-IT-L3#sh int port-channel1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0c71.6d5a.000e (bia 0c71.6d5a.000e)
  Description: Trunk
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Billede 5.3.3.8.3: SW1-IT-L3 interface port-channel1 har 2Kbit båndbredde og en etherchannel er korret opsat

En ekstra kommando, der kan verificere hvor mange channel-groups, der kører samt hvor mange aggregationer, der findes - er `show etherchannel 1 summary`.

```
SW1-IT-L3#show etherchannel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -        Gi3/2(P)    Gi3/3(P)
```

Billede 5.3.3.8.4: Resultat ved kommandeo show etherchannel 1 summary på SW1-IT-L3

Her kan det konkluderes at der er én aktiv etherchannel group med 1 aggregering. Det konkluderes hermed at etherchannel er korrekt opsat.

5.4 Sikkerhed

Sikkerhed dækker over flere ting og findes i flere forskellige niveauer. De niveauer, som der er arbejdet med i dette projekt er:

- ➔ External Network (DMZ, VPN)
- ➔ Network Perimeter (Firewalls)
- ➔ Host (Authentication, Antivirus)

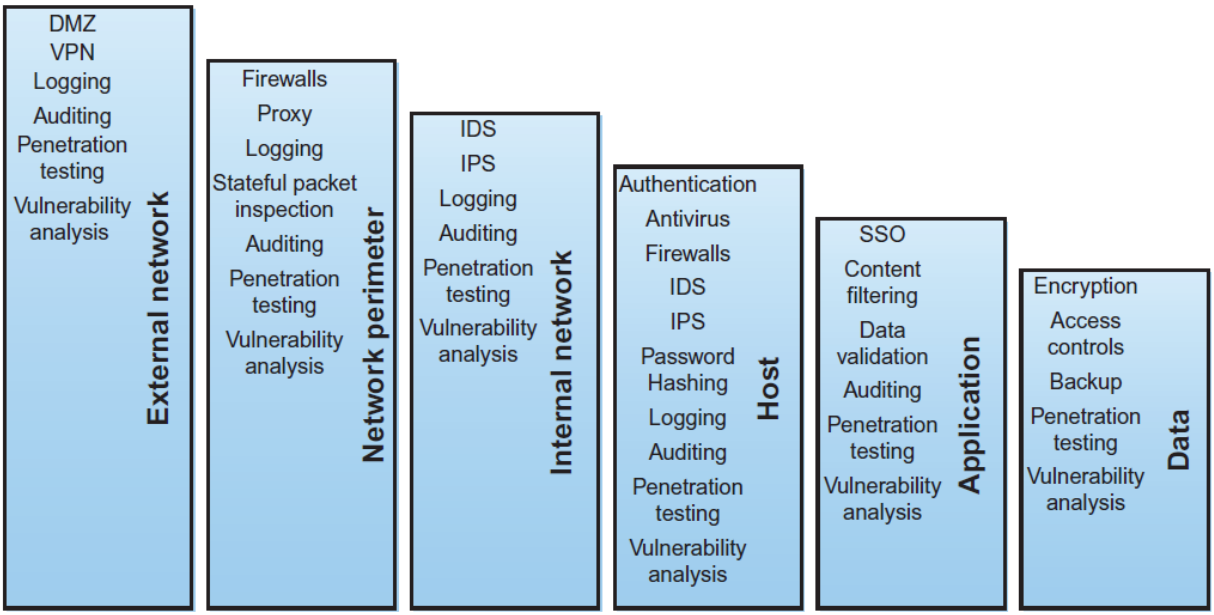


Diagram 5.4.1: Defense in each layer, s. 20 i "The Basics of Information Security" af Jason Andress

Sikring i Active Directory med bl.a. Security Groups og Permissions, som vil blive gennemgået senere i rapporten, kan man også argumentere for hører under Host.

I de følgende afsnit redegøres for, hvordan de forskellige sikkerhedsmæssige tiltag er forsøgt implementeret. Det var bl.a. et stort fokus at opnå en fungerende DMZ, hvor DNS server og Webserver ligger samt opsætte firewall'en således at trafik fra DMZ til LAN'et blokeres.

5.4.1 Firewall

Al trafik der går ind og ud af netværket skal passere igennem firewall'en, derfor opstilles en række regelsæt, så kun autoriseret trafik tillades. Dvs. at trafik fra DMZ og LAN skal gå gennem firewall

og ud til internettet - LAN må ikke gå gennem DMZ, ligesom det ikke skal være muligt at tilgå DMZ 10.130.52.1 fra pfSense Desktop'en, som er tilknyttet LAN'et. For at kunne oprette disse regelsæt opsættes først de nødvendige interfaces inde i selve pfSense.

Som tidligere beskrevet i afsnit 5.2.2.4 pfSense Server blev serveren installeret og opsat på ESXi 10.100.0.40. Ved første opstart havde pfSense registreret tre netværk, som skulle sættes op. Disse tre skulle hver tildeles et interface og en IP-adresse.

```
VMware Virtual Machine - Netgate Device ID: 1ab8cd9c0e3ff294ab54

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4: 87.116.5.215/28
 LAN (lan)       -> vmx1       -> v4: 10.130.51.1/24
 OPT1 (opt1)     -> vmx2       -> v4: 10.130.52.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell
```

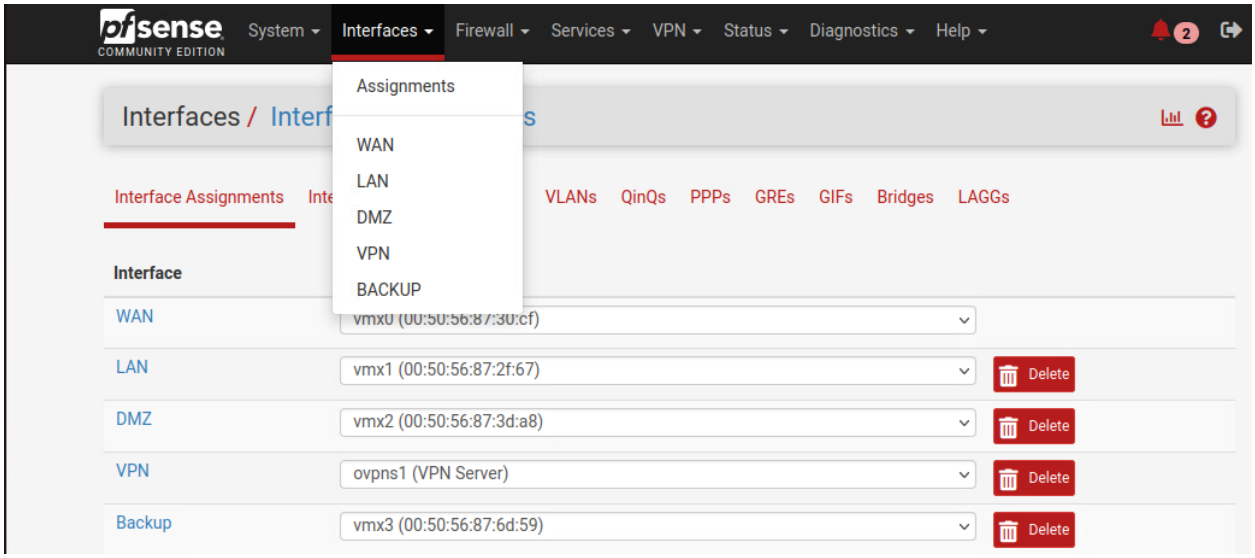
Billede 5.4.1.1: Network interfaces i pfSense serveren

Som processen skred frem og flere netværk kom til så pfSense interfaces således ud:

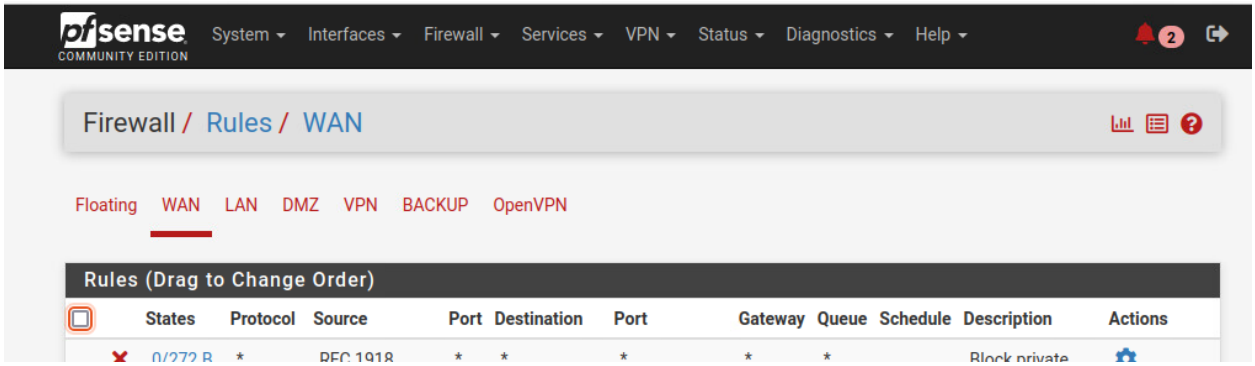
```
VMware Virtual Machine - Netgate Device ID: 94a1b631e29c298b4385

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4: 87.116.5.215/28
 LAN (lan)       -> vmx1       -> v4: 10.130.51.1/24
 DMZ (opt1)      -> vmx2       -> v4: 10.130.52.1/24
 VPN (opt2)      -> ovpns1     -> v4: 10.11.12.1/24
 BACKUP (opt3)   -> vmx3       ->
```

Billede 5.4.1.2: Den endelige konfiguration af network interfaces i pfSense serveren

Billede 5.4.1.2 med udsnit fra konsollen giver et overblik over, hvilke IP-adresser de forskellige interfaces har fået tildelt. Det er disse interfaces, som man kan tilføje regler til, når man tilgår firewall'en gennem pfSense Desktop GUI'en.

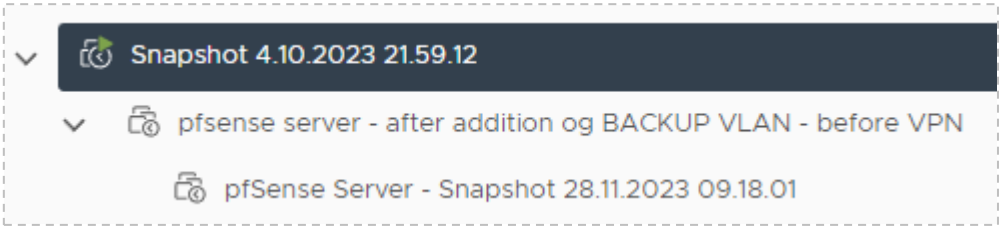


Billede 5.4.1.3: De opsatte interfaces ses i pfSense firewall'ens GUI



Billede 5.4.1.4: De opsatte interfaces ses her under fanen Firewall ▸ Rules

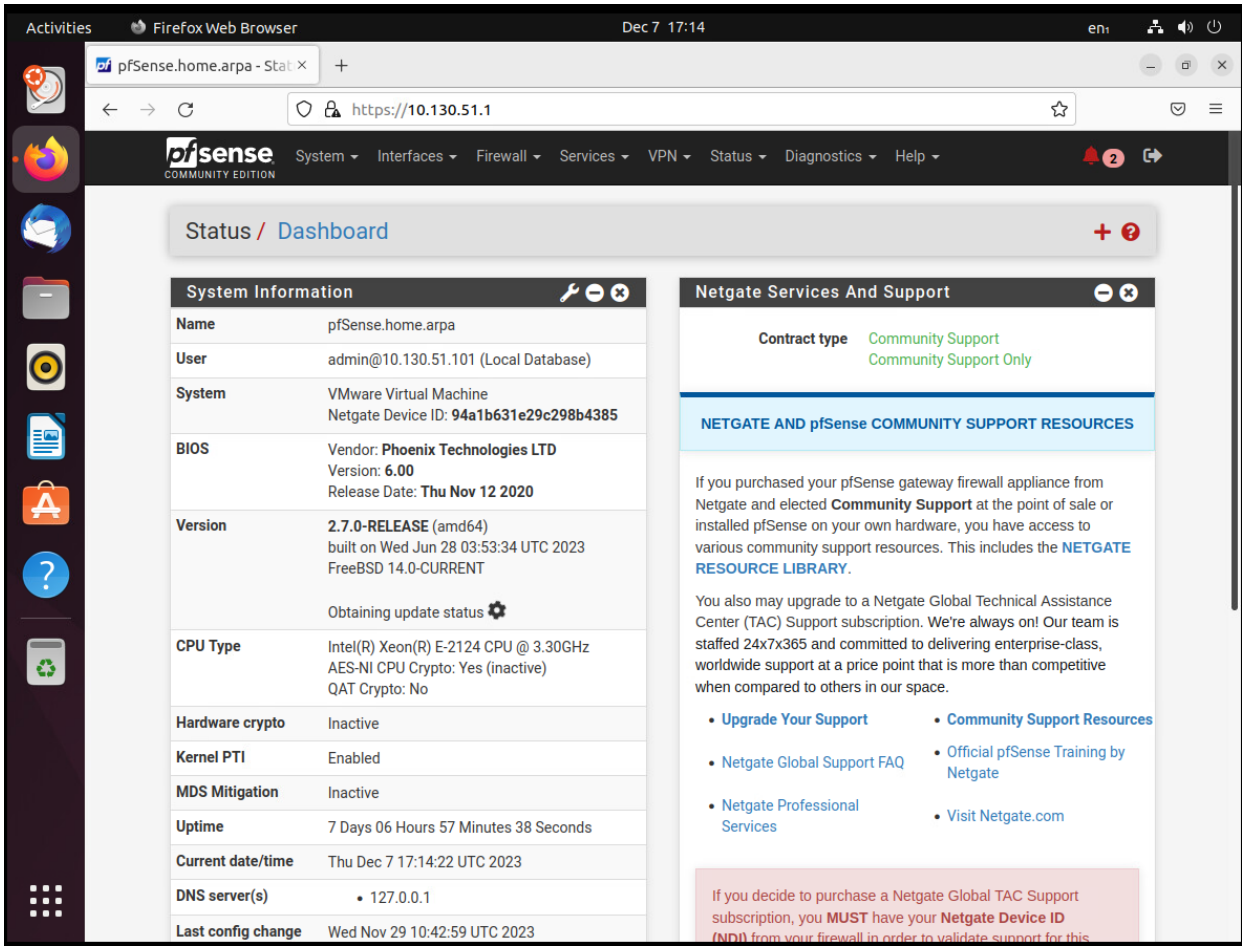
Slutteligt blev der installeret et selv-genereret SSL certifikat, der opgraderede vores HTTP til HTTPS. Efter endt opsætning af regelsæt blev, der taget et snapshot i vCenter.



Billede 5.4.1.5: Snapshots af pfSense serveren, set i vCenter

5.4.1.1 Opsætning af interface regler via Ubuntu Desktop GUI

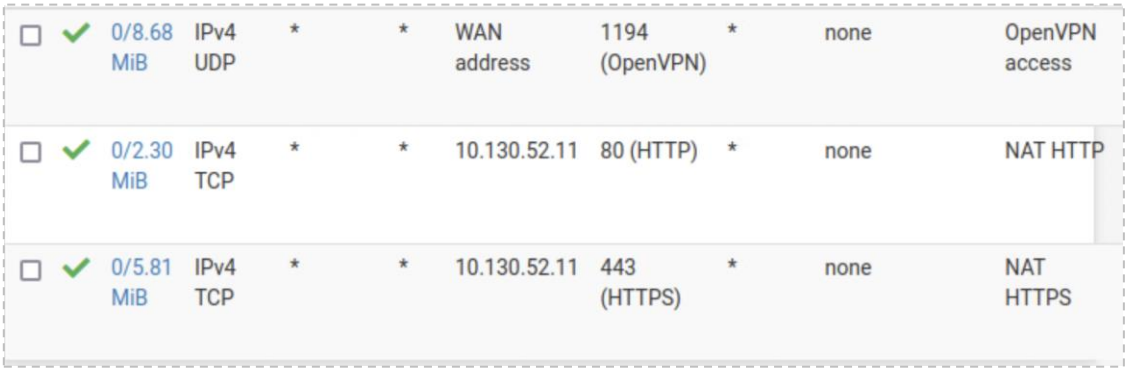
Regler bliver opsat direkte i firewall'ens GUI som tilgås fra en browser: 10.130.51.1.



Billede 5.4.1.1.1: GUI interface DASHBOARD i pfSense firewall'en

5.4.1.1.1 WAN

HTTP og HTTPS tillades fra alle udefrakommende kilder. Ligeledes tillades VPN trafik på WAN interfacet.



0/8.68 MiB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN access
0/2.30 MiB	IPv4 TCP	*	*	10.130.52.11	80 (HTTP)	*	none	NAT HTTP
0/5.81 MiB	IPv4 TCP	*	*	10.130.52.11	443 (HTTPS)	*	none	NAT HTTPS

Billede 5.4.1.1.1.1: Regler for WAN trafik opsat i pfSense firewall

5.4.1.1.2 LAN

På LAN interfacet tillades trafik fra de tre VLANS 3059, 3054 og 3053 at gå til firewall'en. Ligeledes tillades trafik fra SW1-IT-L3 (med Ip 10.130.51.121) at nå firewall'en. Inde i selve LAN'et tillades al trafik, hvilket også er årsag til at de forskellige enheder kan pinge hinanden på tværs af VLANs.

0/0 B	IPv4 *	10.130.59.0/24	*	*	*	*	none	VLAN Guest to firewall
0/881.14 MiB	IPv4 *	10.130.54.0/24	*	*	*	*	none	VLAN Production to firewall
0/97.94 MiB	IPv4 *	10.130.53.0/24	*	*	*	*	none	VLAN Office to firewall
0/0 B	IPv4 *	10.130.51.121	*	This Firewall	*	*	none	VLAN LAN to firewall
5/1.57 GiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule

Billede 5.4.1.1.2.1: Regler for LAN trafik opsat i pfSense firewall

5.4.1.1.3 DMZ (Demilitarized Zone) (DONE)

Serveren skal være i stand til at reagere på de forespørgsler, der kommer ind via HTTPS samt kunne håndtere trafikken, der bevæger sig ud af DMZ, bl.a. HTTPS forespørgsler samt for at udføre opdateringer. Reglerne på billede 5.4.1.1.3.1 er blevet oprettet på DMZ interfacet i firewall'en for at tillade, at disse kriterier kan opfyldes.

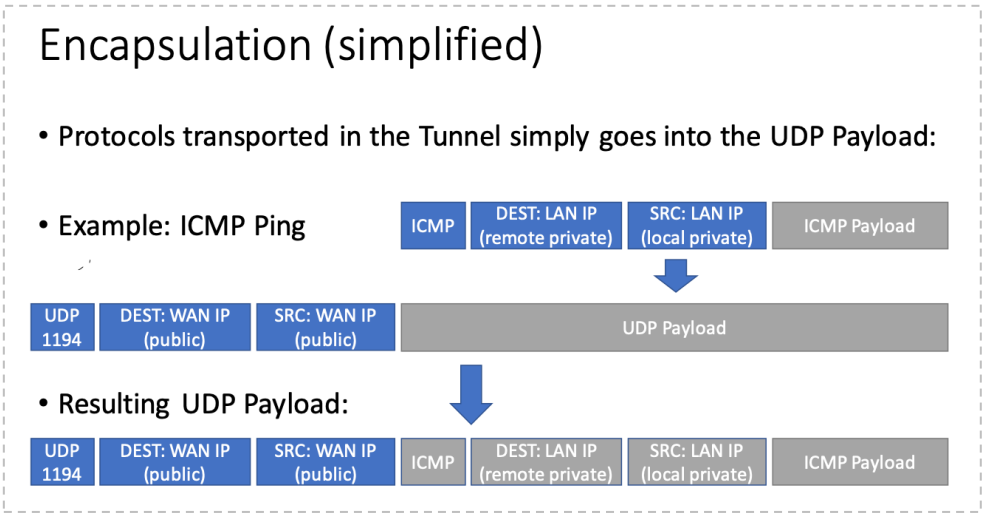
0/2.49 MiB	IPv4 TCP	DMZ net	*	! LAN net	443 (HTTPS)	*	none	HTTPS
0/45 KiB	IPv4 UDP	DMZ net	*	! LAN net	123 (NTP)	*	none	NTP
0/36 KiB	IPv4 UDP	DMZ net	*	! LAN net	53 (DNS)	*	none	DNS

Billede 5.4.1.1.3.1: Regler for trafik gennem DMZ opsat i pfSense firewall

En anden ting værd at nævne er, at DMZ skulle isoleres fra LAN netværket, for at sikre mod indtrængning fra uønskede enheder eller i tilfælde af at DMZ skulle gå ned eller der på anden vis skulle forekomme et sikkerhedsbrud. Derfor konfigureres DMZ reglerne således at trafik, der går fra DMZ til alle destinationer undtagen LAN tillades.

5.4.1.1.4 VPN

Formålet med VPN er at transportere protokoller fra et netværk til et andet. VPN-tunnelmetoden bruger encapsulation og kryptering til sikkert at føre datatrafik gennem et usikkert miljø såsom internettet. Encapsulation isolerer datapakken mens kryptering gør data "usynlige". Dette illustreres nedenfor i billede 5.4.1.1.4 fra artiklen "Ultimate guide to VPN tunneling af vpnmentor.com.



Billede 5.4.1.1.4.1: Simplificeret indkapsling af VPN transport.
Kilde: "Ultimate guide to VPN tunneling" af vpnmentor.com

Konfigurering af VPN-regler i firewall er vigtig for at sikre, at forbindelsen fungere korrekt og tillader sikker udveksling af data. For at oprette VPN-regel i firewall, skal der oprettes en regel i OPT2, der opfører sig som gruppens VPN-interface. Deraf skulle reglen kunne tillade alle protokoller at transportere. Reglen kan ses på billede 5.4.1.1.4.2.

Billede 5.4.1.1.4.2: Regel opsat for VPN i pfSense Firewall ▸ Rules ▸ OPT2

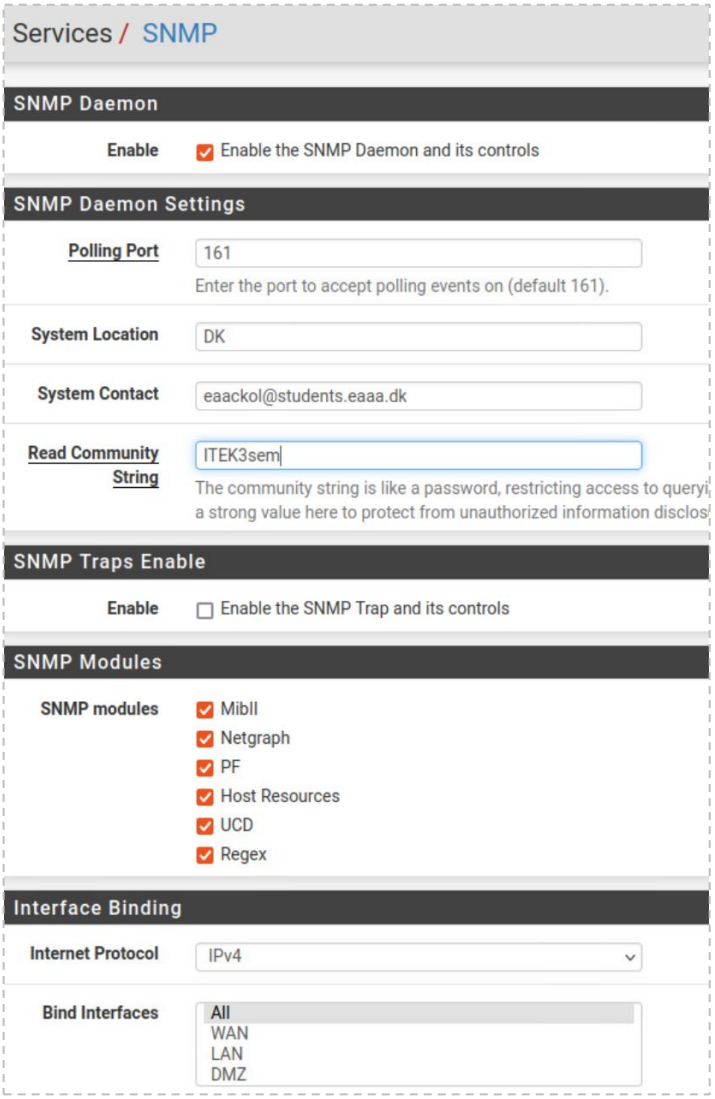
5.4.1.1.5 SNMP

For at tillade indhentning af statistiske data fra netværkets enheder, måtte SNMP først aktiveres under Services.

Hertil blev følgende opsat:

- ➔ Polling Port på 161
- ➔ System location: DK
- ➔ System Contact: eaackol@students.eaaa.dk
- ➔ System Community: ITEK3sem
- ➔ SNMP Modules: Enable all
- ➔ Internet protocol: IPv4
- ➔ Bind interfaces: All

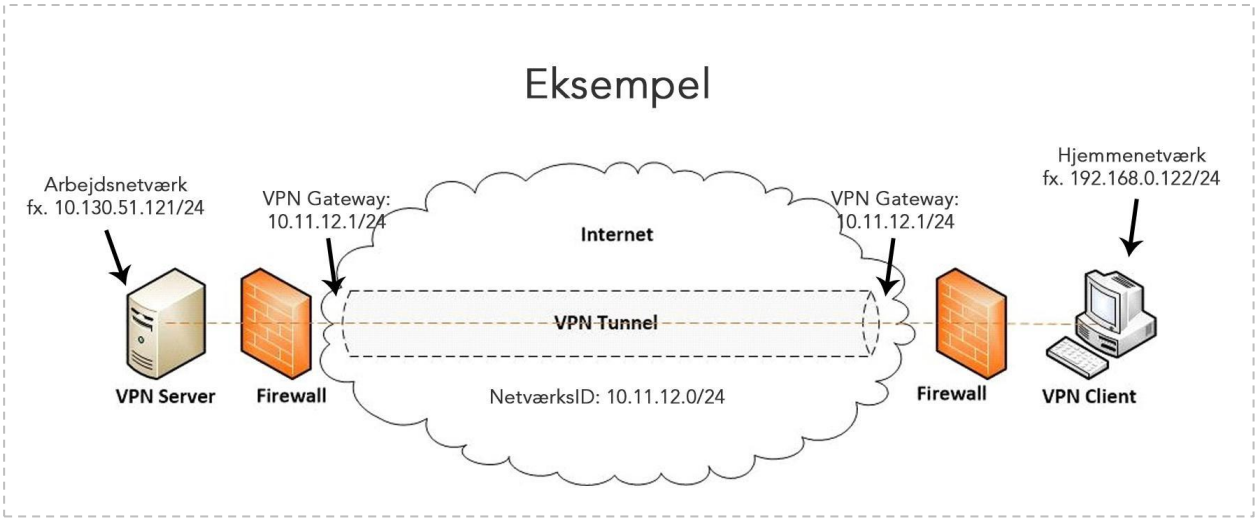
Tests fra afsnit 5.3.3.6 Test af SNMP, dokumenterer at SNMP er korrekt opsat og fuldt funktionelt.



Billede 5.4.1.1.5.1: Opsætning af SNMP Service i pfSense firewall

5.4.2 VPN

Ved brug af VPN oprettes en netværkstunnel - en protokol med et UDP payload, der kan transportere andre protokoller. Det bruges til at oprette forbindelse fx fra ens hjemmenetværk i privatboligen til firmanetværket. Tunnelen kan illustreres som nedenfor i billede 5.4.2.1.



Billede 5.4.2.1: Illustration a fen VPN tunnel. Kilde: https://www.vpnmentor.com/blog/ultimate-guide-to-vpn-tunneling/

VPN klienten forbinder via firewall til OpenVPN's gateway 10.11.12.1. For at kunne nå igennem firewall'en opsættes der regler for VPN, denne er beskrevet i afsnit 5.4.1.1.4 VPN.

Da brugen af VPN på skolens netværk krævede certifikater, som kun underviseren havde tilladelser til at konfigurere, er der brugt en ip-adresse udleveret af skolen: 87.116.5.216. Men billede 5.4.2.1 viser, hvordan det *kunne* have set ud.

Til denne service installeres en OpenVPN server. Trafikken skal sikres med et CA (Certificate Authentication), kryptering og hashing - dette er ligeledes sat op i pfSense Firewall'en.

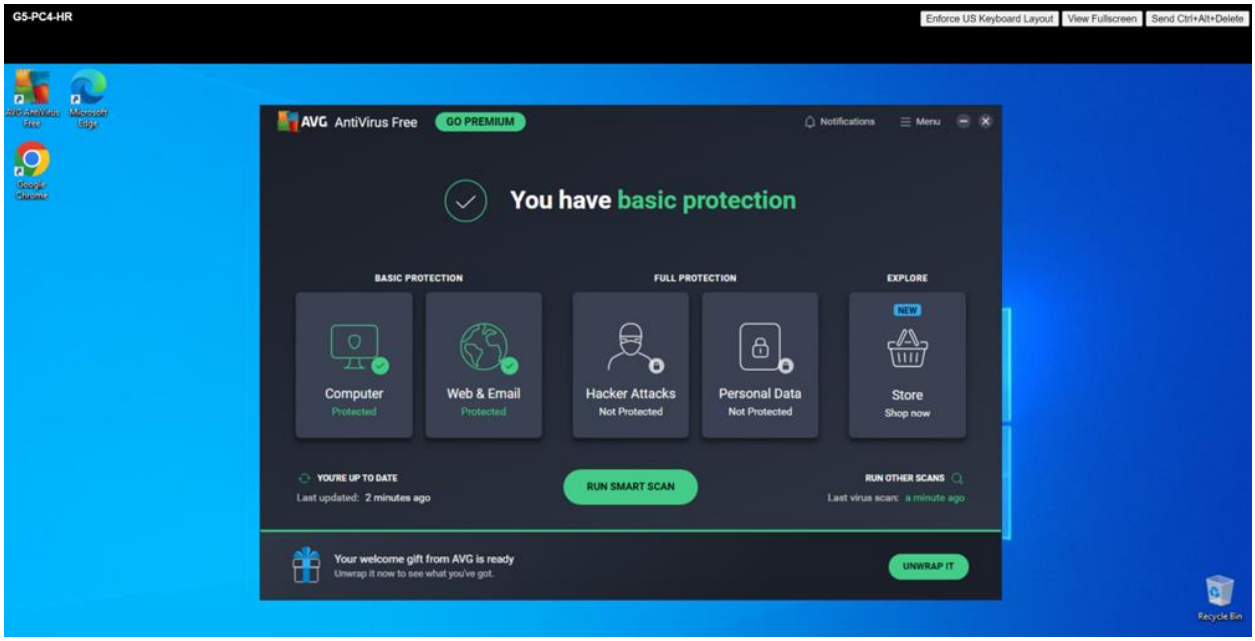
5.4.2.1 Test af VPN forbindelse

Testen foretaget i afsnit 5.2.2.3.2 Test af RDP (Remote Desktop Protocol) omhandler også funktionaliteten af OpenVPN. Uden tilkobling til `G5-Remote-User-Group` opstod der fejlmeddelelse om at domænet ikke kunne nås. Denne test bekræfter herfor også at OpenVPN er opsat korrekt og behøver ikke yderligere demonstration.

5.4.3 AVG Antivirus

Jf. de opstillede krav i afsnit 4. Krav udgør antivirus en del af den samlede beskyttelse.

Til projektet blev der valgt et gratis antivirusprogram for demonstration. AVG Antivirus installeres på alle PC'er og konfigureres til at scanne på daglig basis. En gratis version yder dog kun grundlæggende service, så en betalt version anbefales. Et gratis alternativ er Avast Antivirus. Her havde det ligeledes været optimalt, hvis der havde været tidsmæssige ressourcer til at opsætte Group Policies vedrørende Computer Settings. Så ville alle fremtidige PC'er kunne installeres let og centralt med alle programmer fra start, således at al software ikke skal installeres individuelt hver gang.



Billede 5.4.3.1: AVG Antivirus Dashboard på den virtuelle computer G5-PC4-HR

5.4.4 Andre tiltag

Af andre sikkerhedsmæssige tiltag er det værd at nævne Password Managers, som fx Dashlane eller BitDefender. De kan med én master-kode holde styr på hele virksomhedens password arkiv, ligeledes med at den har en generator og krypteringsfunktion. BitDefender tilbyder også udvidet Firewall, Antivirus, Anti Malware, Anti Ransomware, SpamBot, Safety Wallet, VPN og SafePay blot for at nævne nogle af funktionerne. Et produkt som dette kan anbefales til den samlede løsning.

Yderligere er det værd at bringe en nærmere konfiguration af Windows Defender på banen, men denne har vi beklageligvis ikke haft de tidsmæssige ressourcer til at beskæftige os med i projektet.

5.5 Active Directory Domain Services

Active Directory Domain Services (AD DS) er en afgørende komponent i Microsofts Windows Server-operativsystem, designet til at administrere og organisere et netværk af computere inden for et domæne. AD DS muliggør oprettelsen af fælles ressourcer, der kan tilgås af autoriserede brugere og grupper.

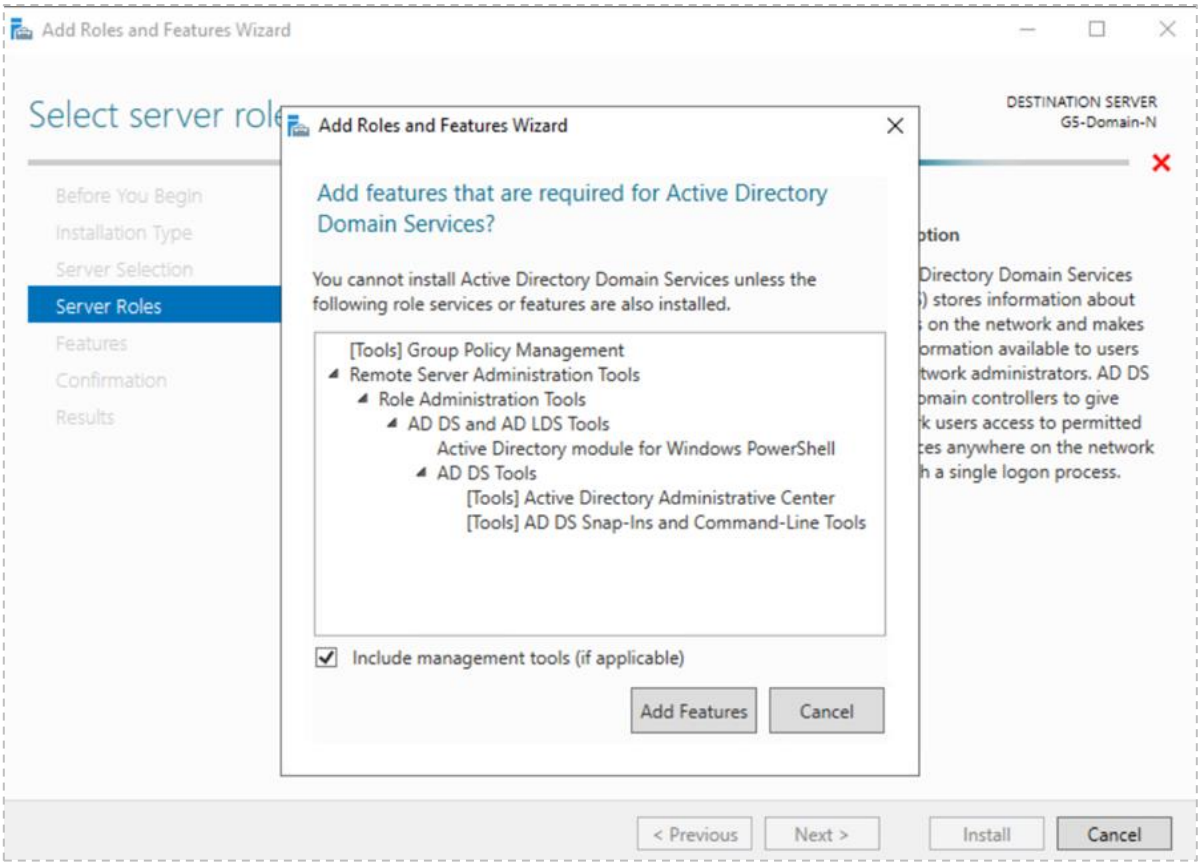
Delinger og fælles mapper er værdifulde redskaber til samarbejde inden for et domæne netværk. Fælles mapper bruges typisk til at opbevare og organisere filer, så brugere kan samarbejde om dokumenter, projekter og andre data.

Ved at udnytte AD DS kan administratorer nemt styre adgangen til fælles ressourcer og sikre, at kun autoriserede brugere og grupper har de nødvendige tilladelser. Denne centraliserede tilgang forenkler sikkerhedsstyring og forbedrer dataintegriteten inden for G5-domænet.

De følgende afsnit omhandler opsætningen af domain server samt oprettelsen af brugergrupper, domæne-medlemmer, shares og tilladelser. Slutteligt afsluttes sektionen med et testafsnit, hvor funktionaliteten af shares og tilladelser dokumenteres.

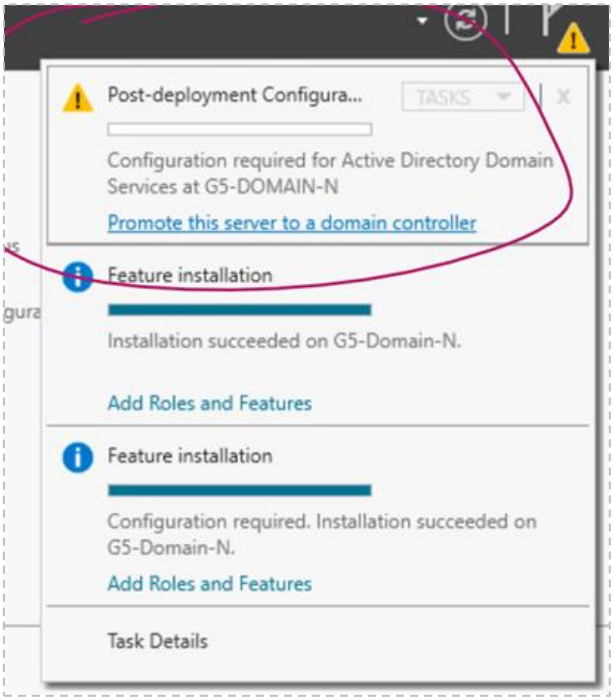
5.5.1 Opsætning af AD DS

For at implementere Active Directory Domain Services er det først nødvendigt at foretage installationen af Active Directory (AD).På nedenstående skærmbilleder af konfigurationerne detaljeret og trinvis proces for installationen, hvori der skabes en ny forest ved navn G5-local. Dette omfatter også konfigurationen af den nye forest G5-local samt opsætningen af yderligere konfigurationer for G5-domænet. Billede 5.5.1.2 viser en del af installationsprocessen af Active Directory Domain Services, som skal foretages i Server Manageren ▸ Add Roles and Features.



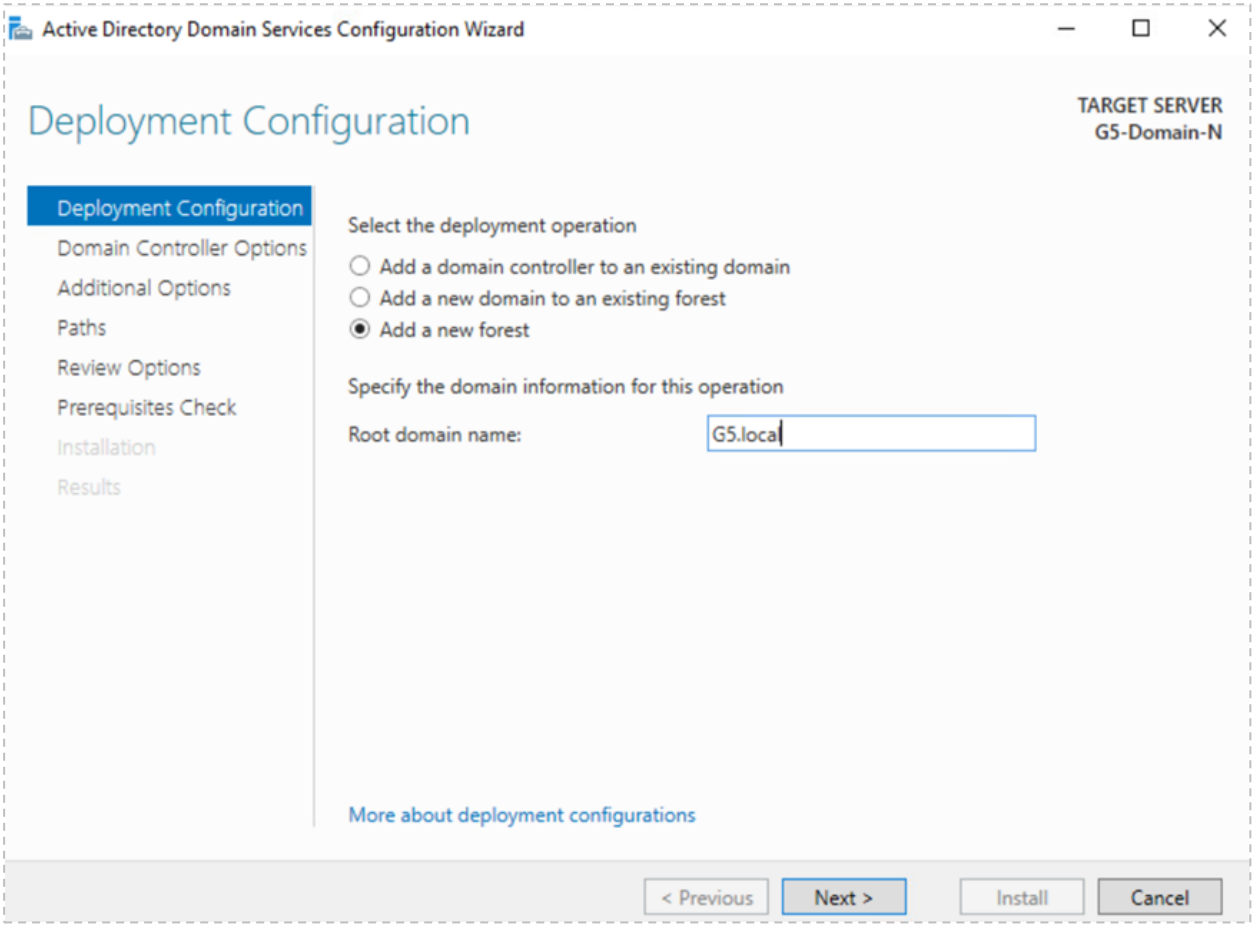
Billede 5.5.1.1: Installation af Active Directory Domain Services på Domain serveren, via Server Manager

Herefter promotes DNS serveren til en DOMAIN server.



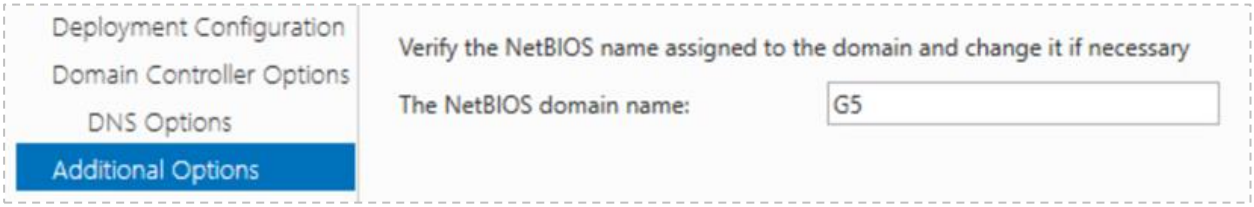
Billede 5.5.1.2: DNS serveren promotes til Domain server

Næste skridt er at konfigurere en ny skov, som domænemedlemmerne kan blive en del af.



Billede 5.5.1.3: Forest oprettes for G5 domæne: G5.local

Domænet oprettes herefter med navnet G5.



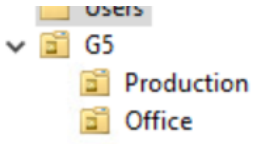
Billede 5.5.1.4: Domænenetværk navngives "G5"

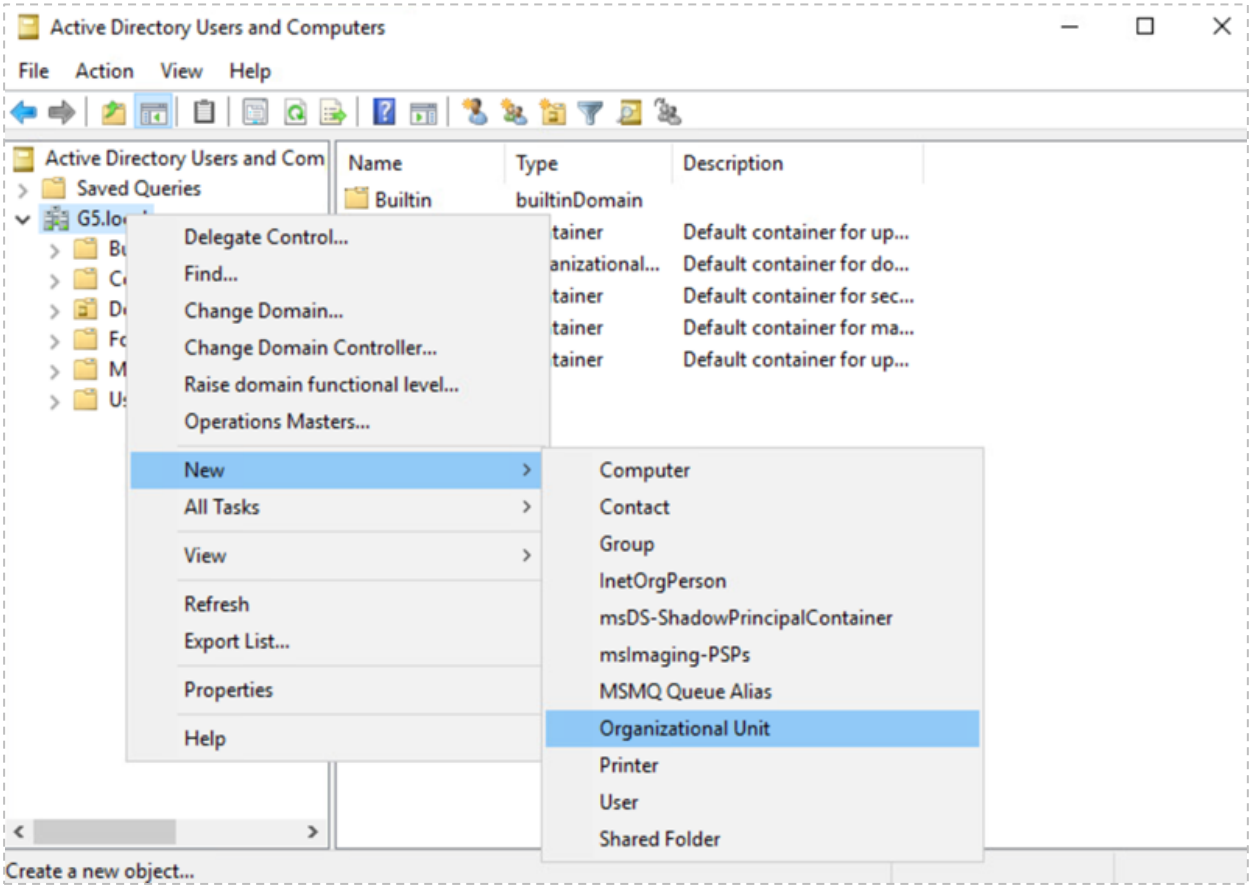
Efter domænenetværket er oprettet, skal der oprettes nogle Organizational Units samt Administratorer.

5.5.2 Oprettelse af Organizational Units & Administrators

5.5.2.1 Organizational Units (OUs)

Organizational units i AD er en metode til at organisere og administrere objekter som computers, users and groups. Dette hierarki letter administration og delegation af opgaver inden for et domæne miljø. For at oprette OU-hierarki skal man som administrator oprette OU's baseret på organisatoriske kriterier for afdelinger. På nedenstående billeder ses hvordan der bliver oprettet OU's for *Production* og *Office*.[11]





Billede 5.5.2.1.1: Oprettelse af Organizational Unit OU i Server Manageren på Domain serveren

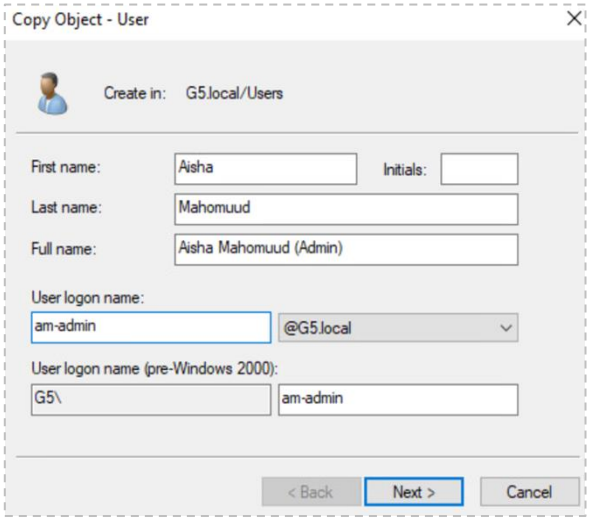
Administratorer kan tildeles specifikke rettigheder inden for hver OU. Dette muliggør at administratorer kan administrere objekter inden for deres ansvarsområde uden fuld adgang til hele domænet.

[11] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/delegating-administration-of-account-ous-and-resource-ous

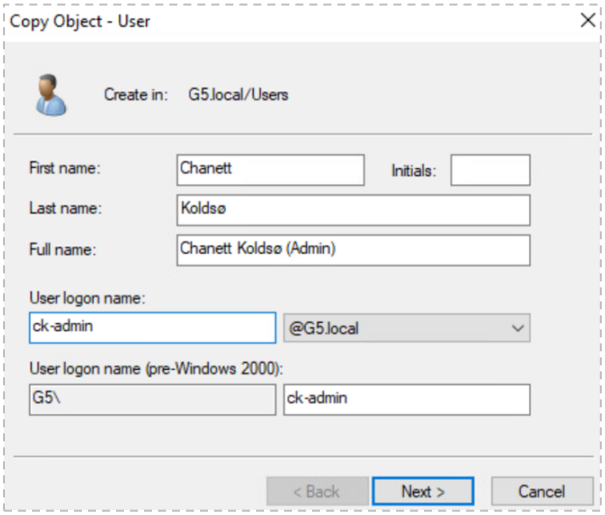
5.5.2.2 *Administrators*

Administratorer i AD har forskellige niveauer af adgangsrettigheder baseret på deres rolle. Grupper som *Domain admin* har omfattende kontrol over hele domænet og det anbefales ikke at gøre brug af denne bruger, da den er indbygget i AD og dermed for kendt til at være sikker. I stedet blev administrator-brugeren kopieret tre gange for at oprette tre særskilte administratorer med den indbyggede admin tilladelser. Der blev oprettet følgende administratorer:

- ck-admin
- am-admin
- IT-admin

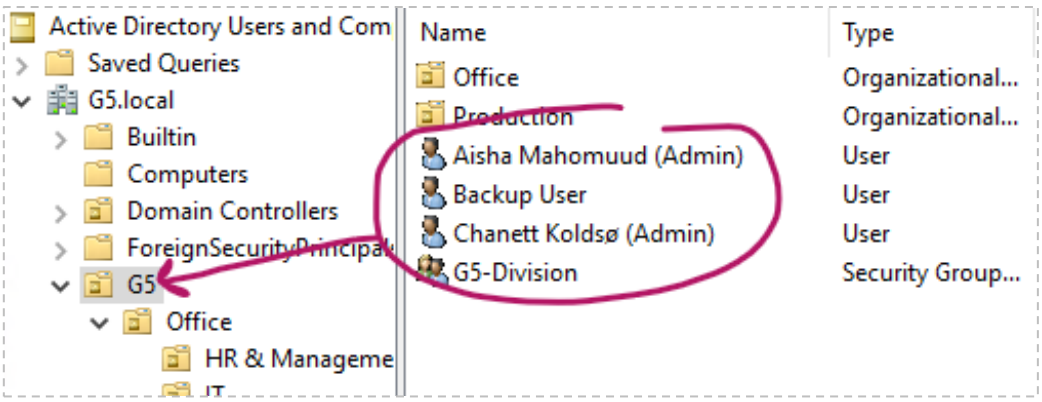


Billede 5.5.2.2.1: am-admin oprettes som administrator

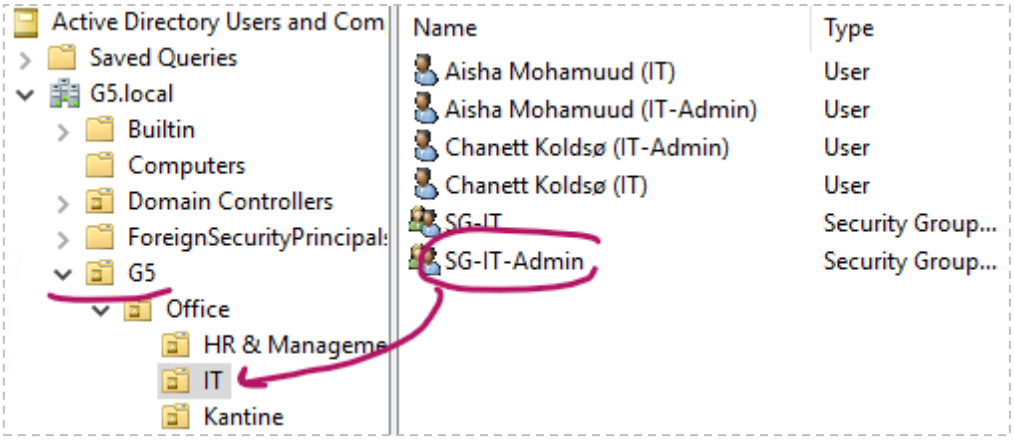


Billede 5.5.2.2.2: ck-admin oprettes som administrator

Efter de to administrator-brugere blev oprettet, blev de flyttet over i de ønskede OUs som det fremgår af billede 5.5.2.2.3 og billede 5.5.2.2.4.



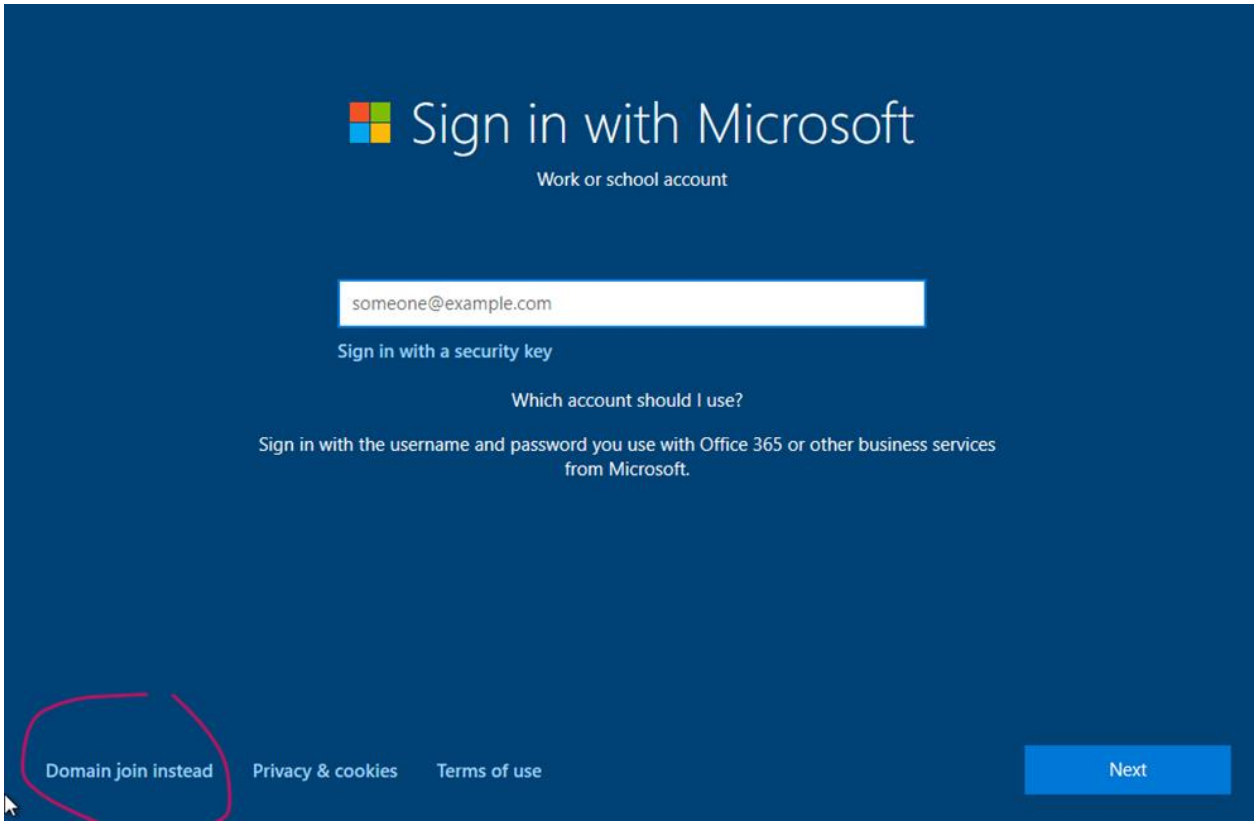
Billede 5.5.2.2.3: am-admin og ck-admin flyttes til hovedmappe G5



Billede 5.5.2.2.4: SG-IT-Admin Security Group flyttes til G5 ▸ Office ▸ IT

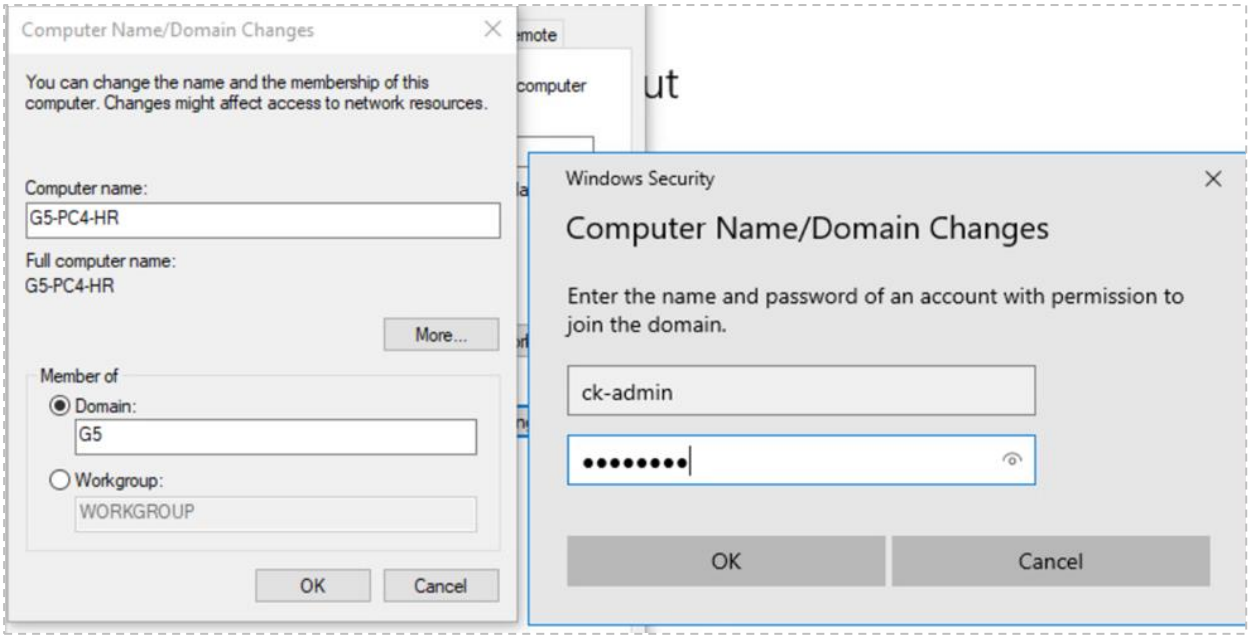
5.5.3 Oprettelse af domæne medlemmer

For at computere kan deltage i G5-domænet, skal disse konfigureres som domæne medlemmer. Det gøres efter installationen, hvor "join to domain" vælges frem for en almindelig login proces.



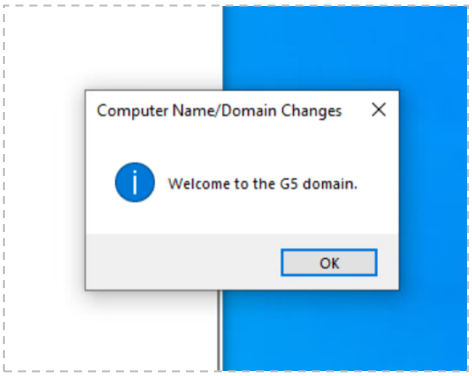
Billede 5.5.3.1: Domain join instead, skulle bruges for at opsætte PC'en som domænemedlem

Efterfølgende tilsluttes PC'en til domænet ved at tilgå "Advanced System Setting" og ændre "Member of" indstillingerne fra WORKGROUP til Domain: G5.



Billede 5.5.3.2: Ændring af membership fra WORKGROUP til Domain: G5

Herefter ville - hvis join var succesfuldt fremkomme en lille besked herom.



Billede 5.5.3.3: Succesmeddelelse

Når de er tilsluttet, simplificeres vedligeholdet af computere, da der gøres brug af centraliseret styring, godkendelse og autorisation leveret af AD DS. Dette tillader et forenet login system, hvor brugere kan få adgang til ressourcer på tværs af netværket ved hjælp af en enkelt sæt legitimationsoplysninger. Dette forudsætter dog opsætning af GPOs (Group Policy Object), som gruppen grundet tidspres beklageligvis ikke nåede at sætte op. Men her var det ønskeligt, at alle brugere havde adgang til samme PC-opsætning med antivirus, VMware Tools og andre programmer, som kunden bruger i hverdagen. Dette går under kategorien Computer Configuration settings.

5.5.4 Oprettelse af Security Groups & Users

Security Groups (SG's) og users (brugere) i Active Directory er essentielle elementer. men SG's muliggør effektiv nedarvning og gruppebaseret adgangskontrol, hvor de enkelte brugere kan få individuel rettighedstildeling. Begge spiller en central rolle i at opretholde sikkerhed og effektiv administration.

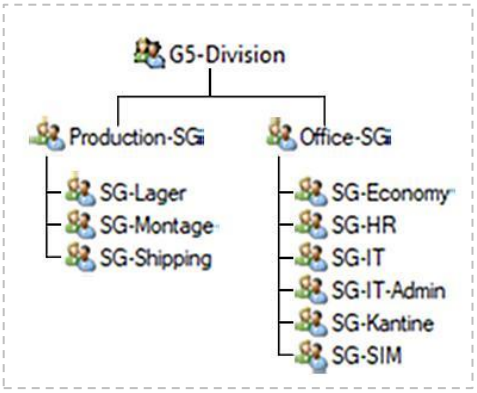
5.5.4.1 Security Groups & Users

Det er afgørende at implementere Security Groups (SGs) i AD, på grund af to ting:

- ➔ Nedarvninger af rettigheder
- ➔ Effektiv tildeling af adgang

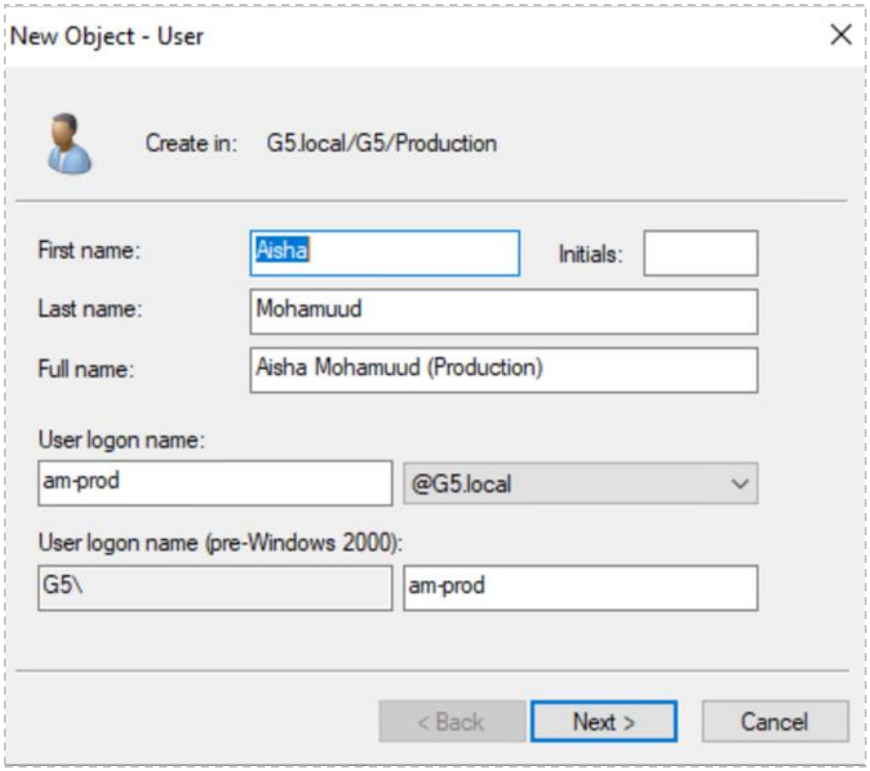
SGs muliggør en struktureret nedarvning af brugerrettigheder startende fra toppen. De tilladelser, der gives i G5-Division, går igennem hele vejen ned til det nederste niveau af SGs. Hertil kan de individuelle SGs og brugere få tildelt eller frataget sig særlige tilladelser. De tilladelser, som der er arbejdet med i projektet, er NTFS-tilladelser og gennemgås i afsnit 5.5.6 Tilladelser.

Hierarkiet forenkler administrationen og sikrer adgangskontrol på effektiv vis. Billede 5.5.4.1.1 illustrerer fint hierarkiet af Security Groups i G5-domænet.



Billede 5.5.4.1.1: Hierarkisk struktur for Security Groups I G5-domænenetværket. Illustration af Chanett Koldsø

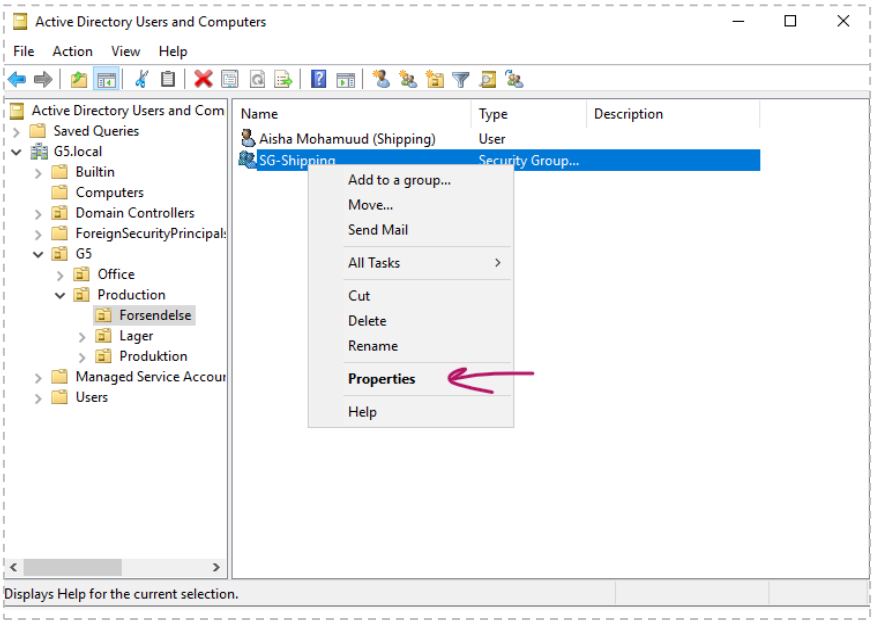
Alle oprettede users i en virksomhed bør være medlem af en Security Group, så der er helt styr på tilladelser og begrænsninger hos de enkelte brugere. Når en bruger oprettes - i hvert fald i dette projekt - angives for- og efternavn, display navn (Full name), brugerlogin og password, som vist i billede 5.5.4.1.2.



Billede 5.5.4.1.2: Oprettelse af alm. bruger

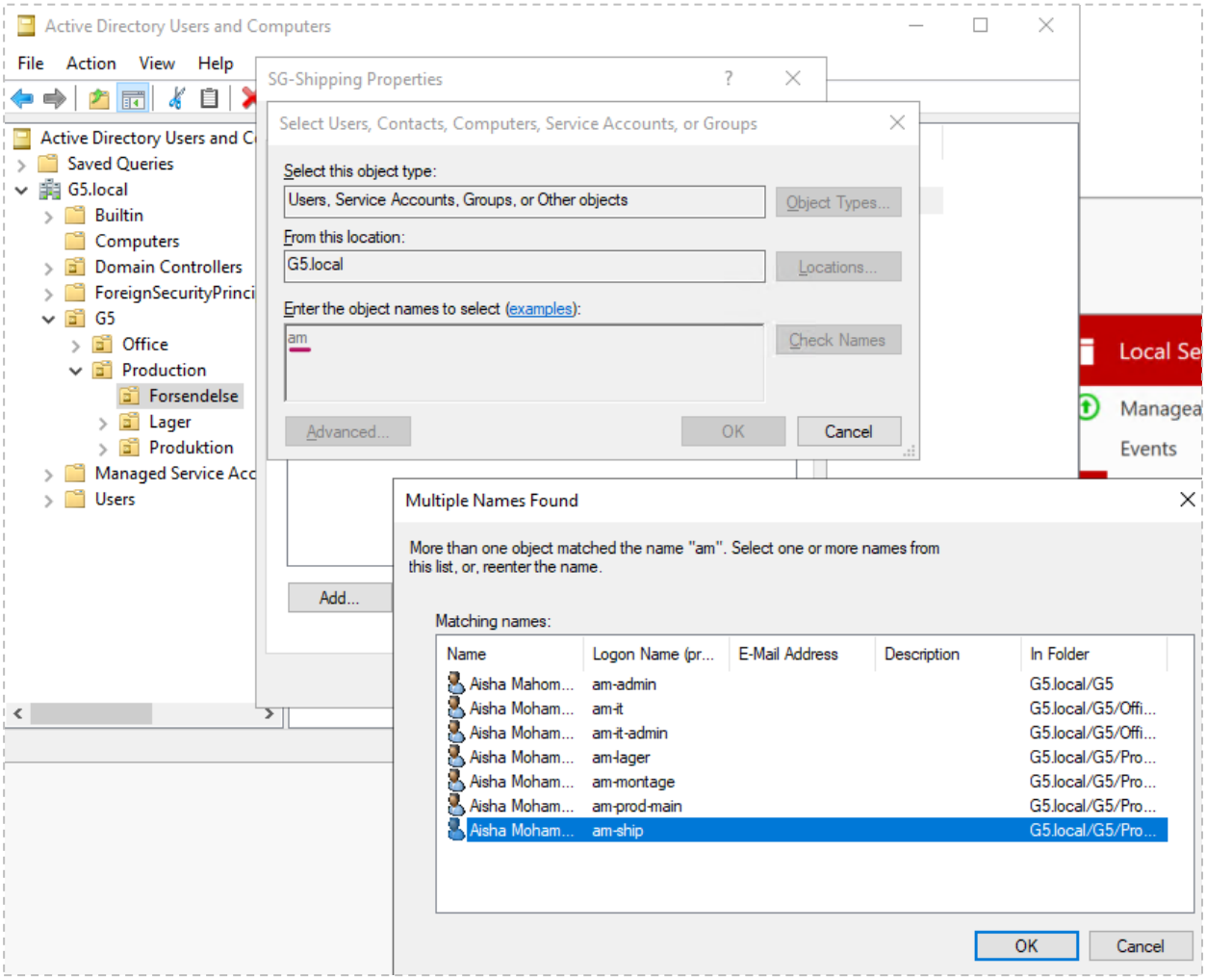
5.5.4.1.1 Tilknytning af users til Security Groups

Brugerne blev herefter tilføjet til en ønsket Security Group. Enten går man ind i en SGs egenskaber og vælger "Members" og tilføjer brugeren dér (som vist på nedenstående billeder) eller også tilgår man brugerens egenskaber og vælger "Members of" og tilføjer en Security Group dér. Sidstnævnte giver mest mening, hvis det er enkelte brugere, der oprettes og skal tilføjes. Hvis man har en større mængde brugere, kan man tilføje flere brugere på én gang, hvis man tilføjer dem fra SGs "Members" panel.



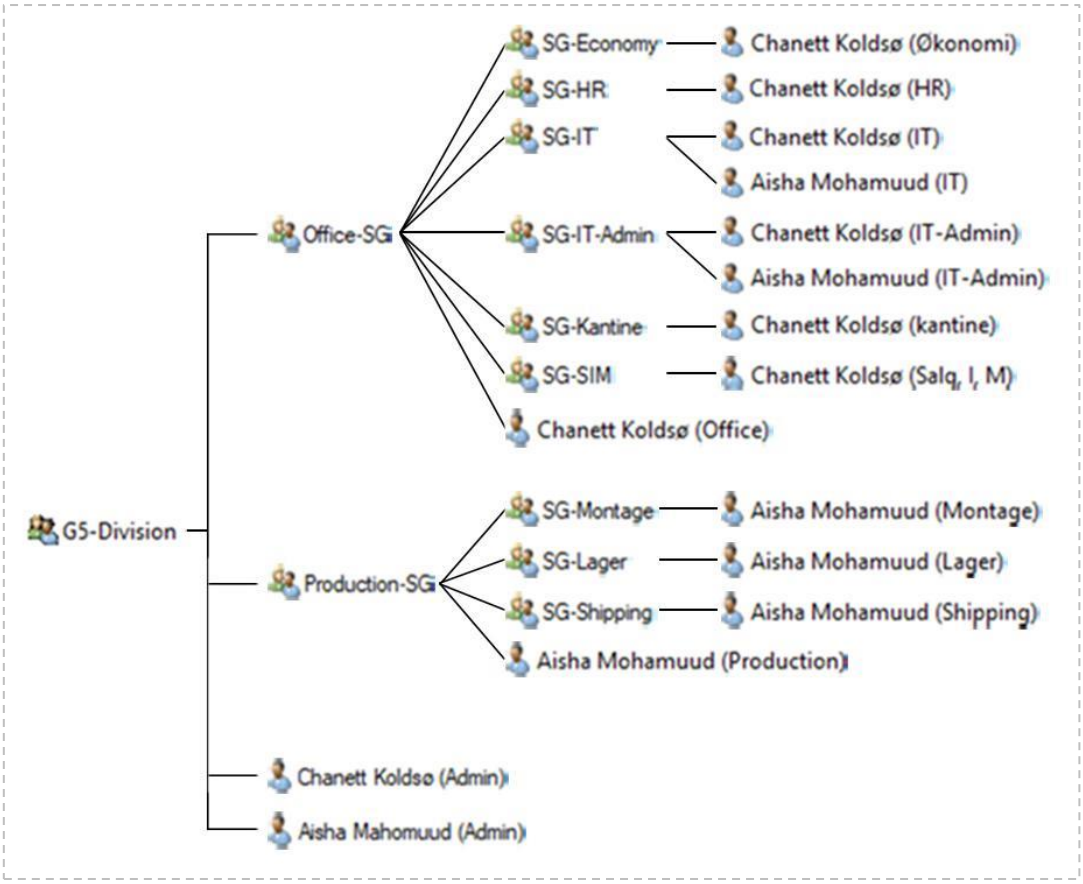
Billede 5.5.4.1.1.1: Ændring af medlemsskab gøres under "Egenskaber"

På billede 5.5.4.1.1.2 fremgår det, at der er blevet søgt efter alle brugere startende med am, hvor man fra en liste kan vælge dén bruger, man ønsker at tilføje. I dette tilfælde tilføjes am-ship til SG-Shipping.



Billede 5.5.4.1.1.2: am-ship vælges fra brugerliste

På billede 5.5.4.1.1.3 fremgår det, hvordan medlemskaber mellem Security Groups er struktureret samt hvilke brugere, der er medlemmer af de enkelte Security Groups. Denne opdeling er en del af strukturingen af tilladelser, hvilket gennemgås i afsnit 5.5.6 Tilladelser.

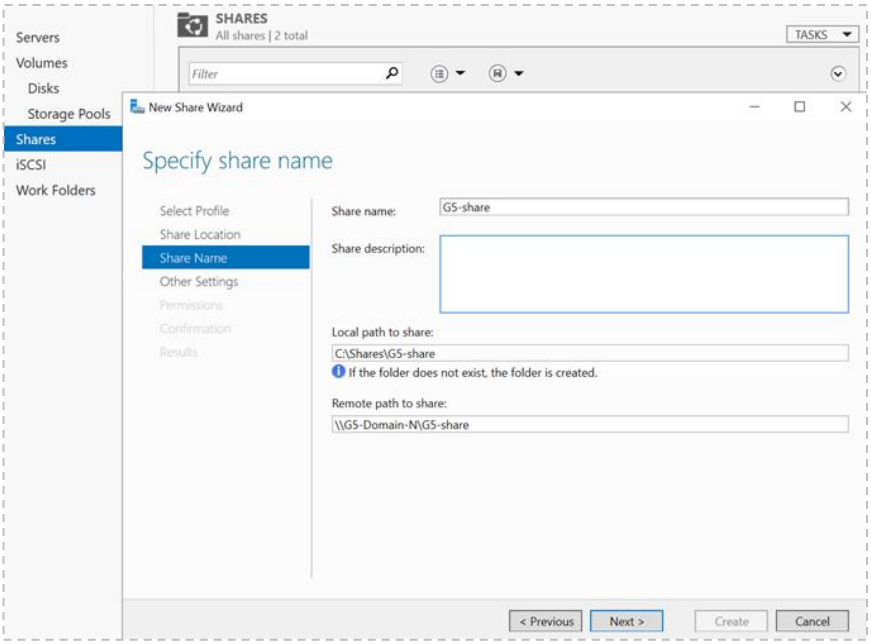


Billede 5.5.4.1.1.3: Oversigt over hierarkiet af Security Groups & Members.
Illustration af Chanett Koldsø

5.5.5 Shares

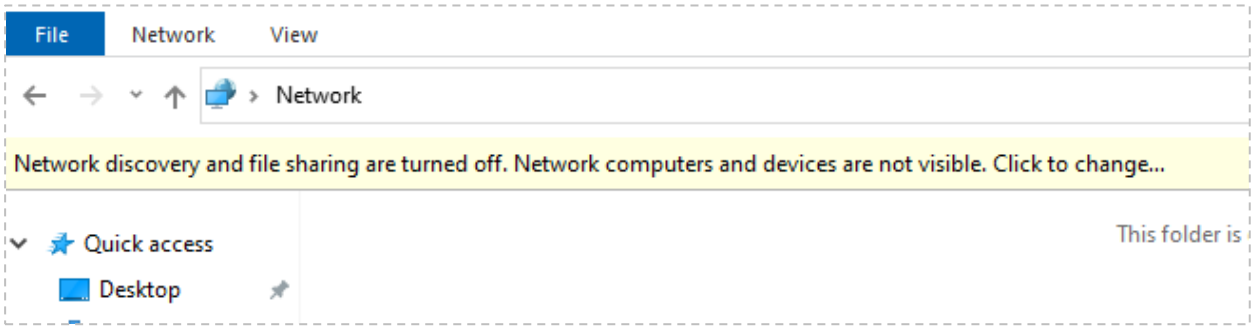
Efter fordelingen af brugere i Security Groups, blev der opsat et Share. Dette blev foretaget fra Server Manager på G5-Domain-N serveren.

Det oprettede Share vil herefter kunne tilgås fra et hvert domæne-medlem ved at navigere til "Netværk".



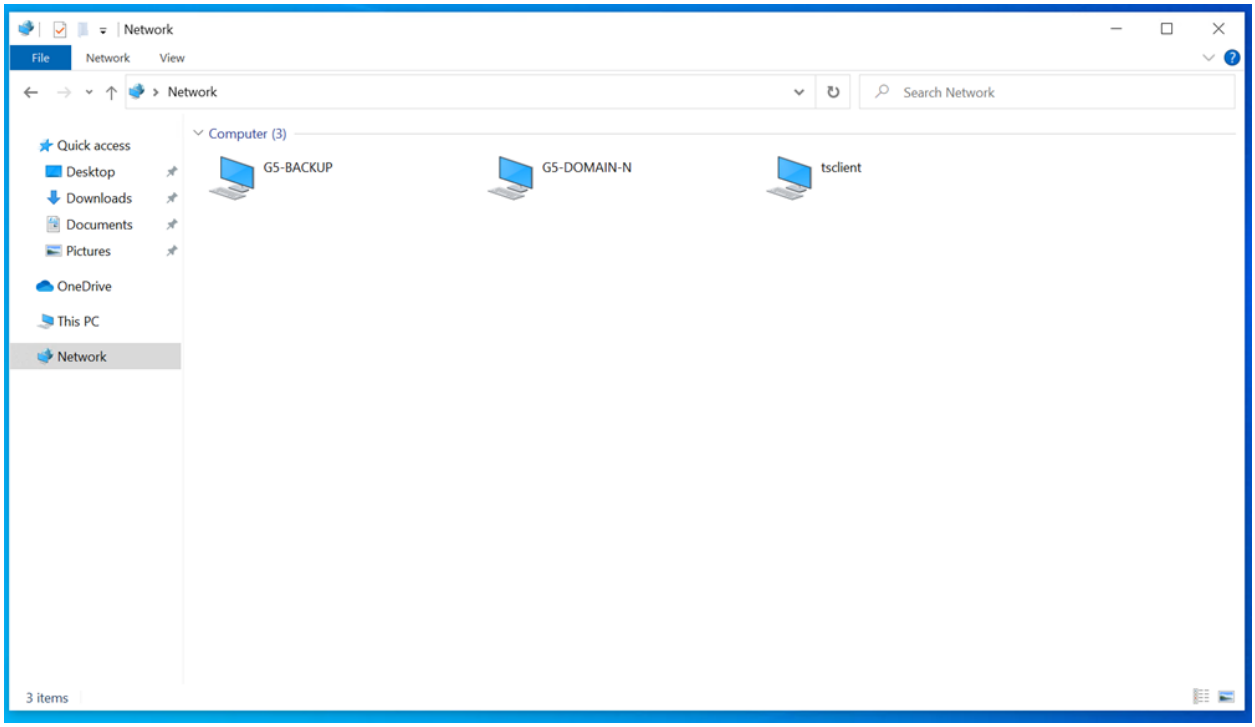
Billede 5.5.5.1: Oprettelse af Share på Domain-serveren

Aktivering af "Network discovery and file sharing" på private netværk kan være nødvendigt for at kunne finde domæne-netværket ligesom det var nødvendigt i eksemplet nedenfor.



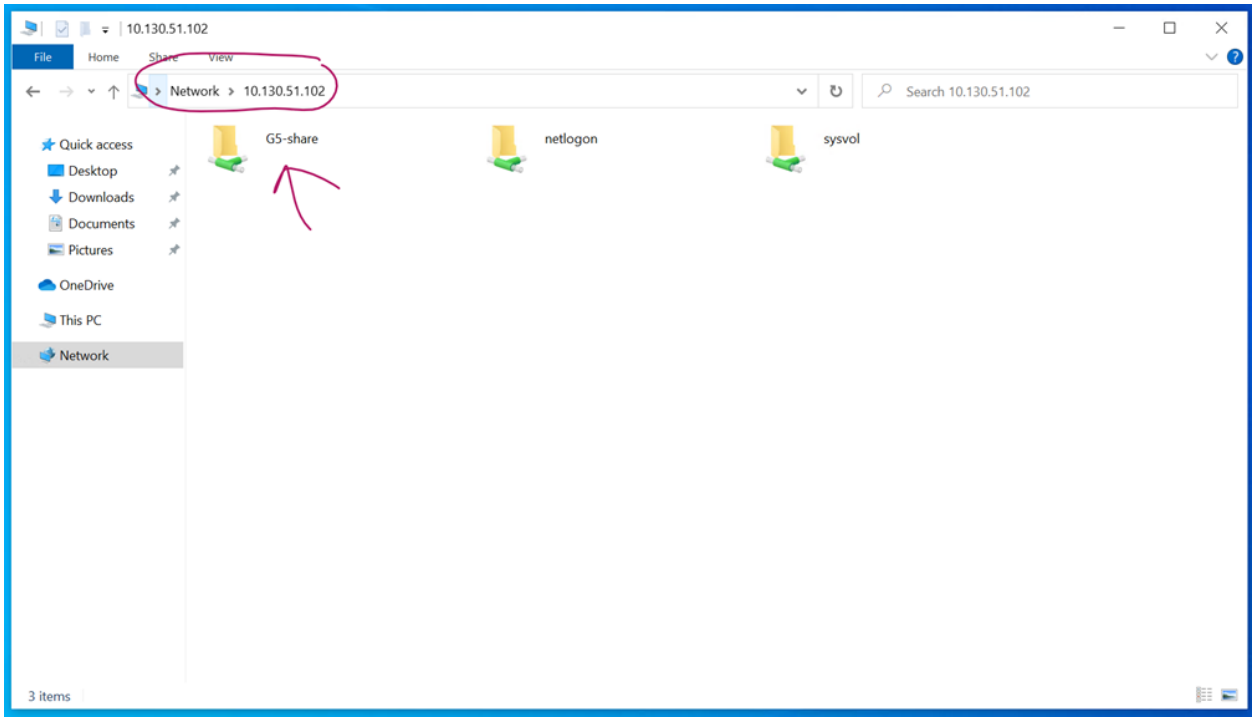
Billede 5.5.5.2: Fane vist første gang man fra Windows tilgår sektionen NETVÆRK

Efter aktivering af Network Discovery, kunne man fra Network i mappe-panelet tilgå domænenetværket, som vist på billede 5.5.5.3.



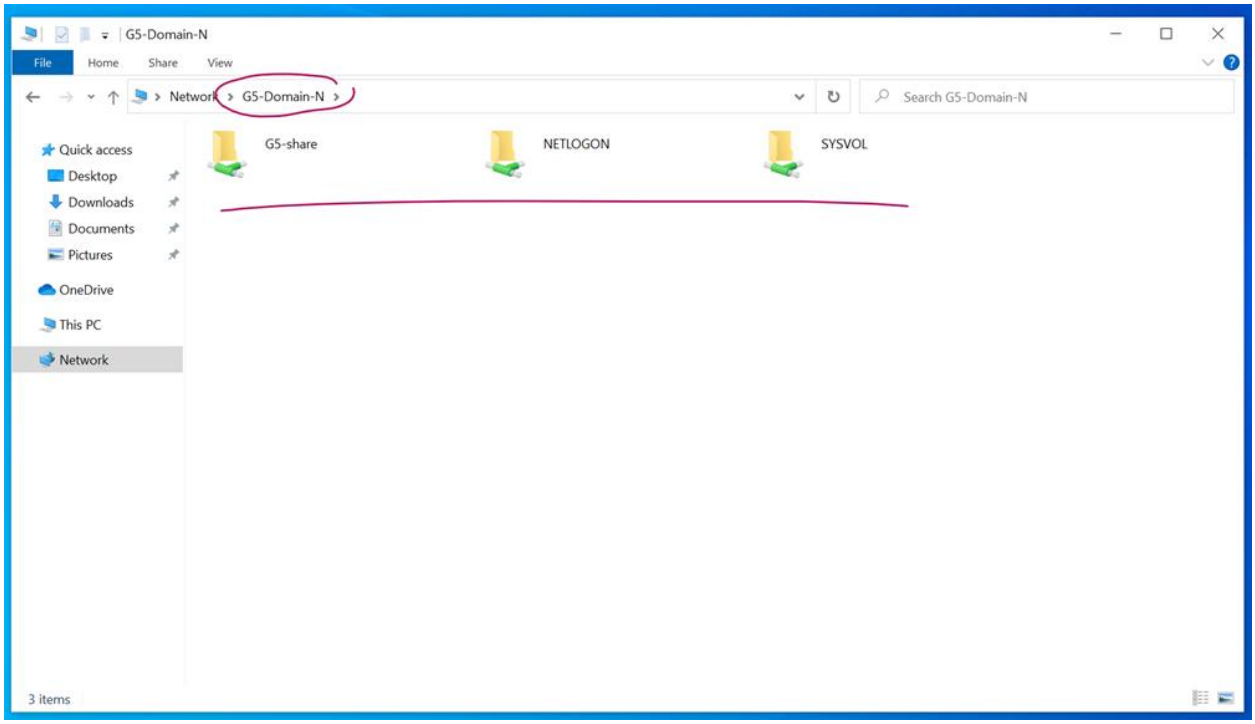
Billede 5.5.5.3: Domænenetværket er tilgængeligt på Windows PC og Server

Billede 5.5.5.4 viser adgang til det oprettede share via ip adresse \\10.130.51.102.



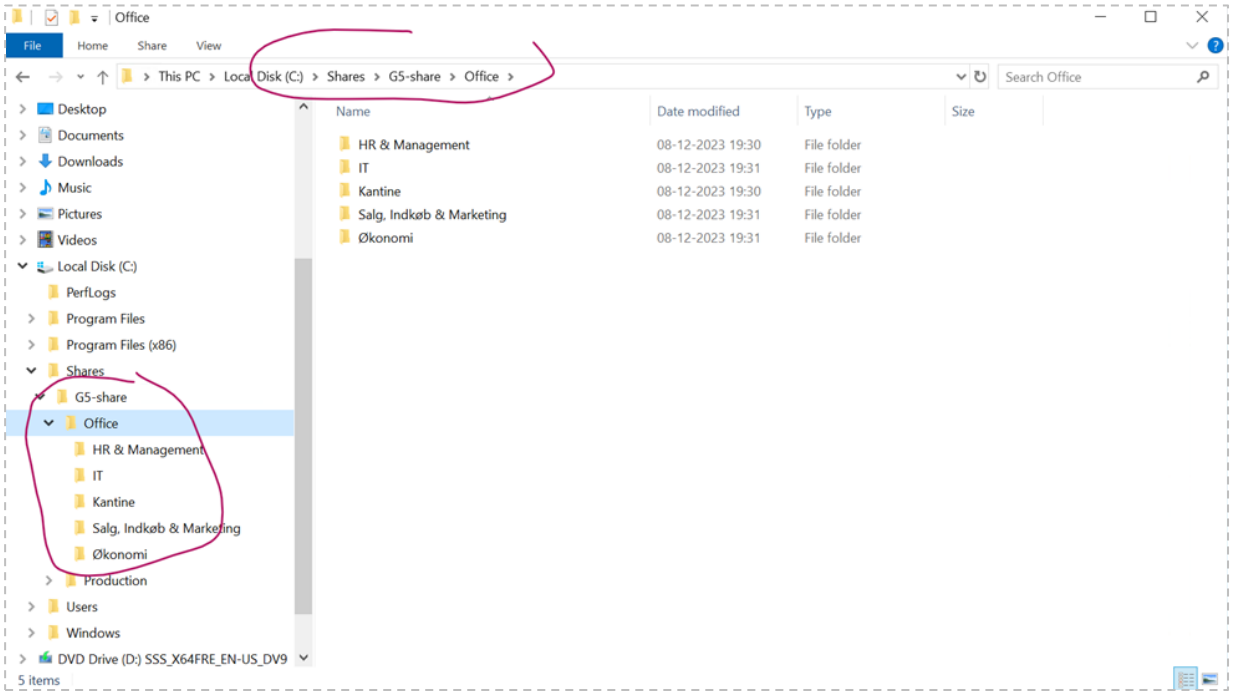
Billede 5.5.5.4: Domænenetværket kan tilgås via ip: \\10.130.51.102

Ligeledes er det muligt at få adgang til det oprettede Share via domænenavn G5-Domain-N.



Billede 5.5.5.4: Domænenetværket kan tilgås via domænenavn:G5-Domain-N

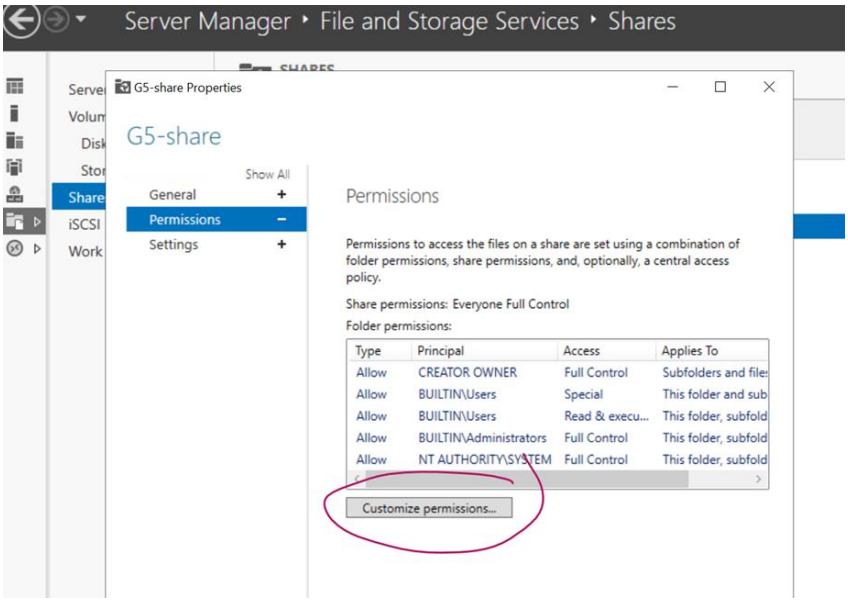
Efter verifikation af at et Share blev oprettet skulle der oprettes nogle mapper, som brugerne kan benytte. Dette gøres på Domain serveren i Windows' mappepanel.



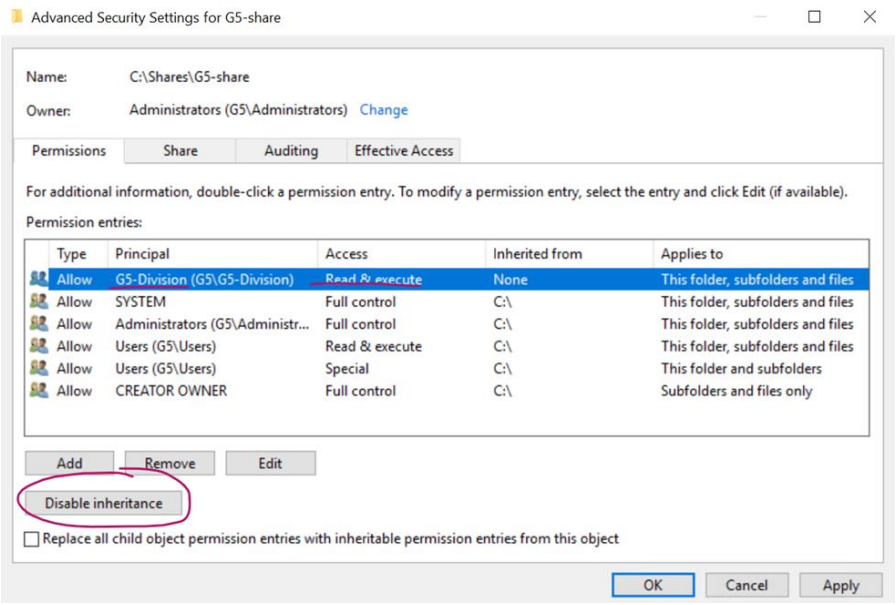
Billede 5.5.5.5: Mapper oprettes i Windows mappesystem

5.5.6 Tilladelser

Første skridt til at opsætte tilladelser for domænets medlemmer var at deaktivere nedarvning fra Server Manager ▸ Shares ▸ Permissions ▸ Customize Permissions ▸ G5-Division.



Billede 5.5.6.1: Permissions panel for G5-share, Server Manager, Domain server.



Billede 5.5.6.2: Her vælges "Disable inheritance" fra Permissions tab in Advanced Security Settings for G5-share

Efterfølgende blev der sat NTFS tilladelser op baseret på både de oprettede Security Groups, men også for nogle af de enkelte brugere. Dette kunne med lethed kombineres. Alle `allow` tilladelser kan overskrives af `deny` tilladelser - med dét in mente oprettedes følgende reglerne som vist i nedenstående tabeller.

TABEL 5.5.6.1: TILLADELSER FOR "G.5-SHARE" UNDERMAPPER (NTFS)

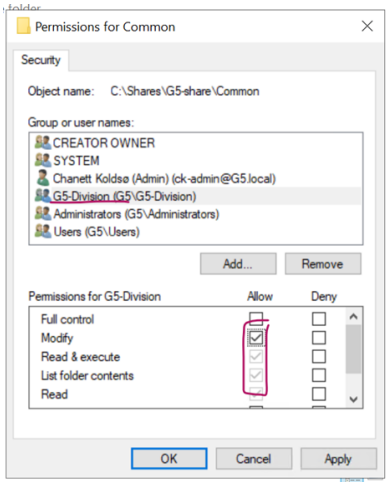
	COMMON	OFFICE	PRODUCTION
Full Control	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin
Modify	SG-G5-Division	SG-IT	SG-IT
Read & Execute			
Read		Office-SG	Production-SG
Write			
Deny		Production-SG (all)	Office-SG (all)

TABEL 5.5.6.2: TILLADELSER FOR "PRODUCTION" UNDERMAPPER (NTFS)			
	FORSENDELSE	**LAGER**	**PRODUKTION**
Full Control	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin
Modify	SG-IT	SG-IT	SG-IT
Read & Execute	SG-Shipping	SG-Lager	SG-Montage
Read	SG-Lager	SG_Shipping	SG-Lager SG_Shipping
Write			
Deny	SG-Lager (write) SG-Montage (all)	SG_Shipping (write) SG-Montage (all)	SG-Lager (write) SG_Shipping (write)

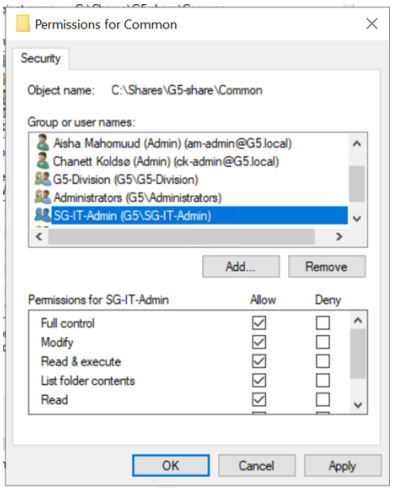
TABEL 5.5.6.3: TILLADELSER FOR "OFFICE" UNDERMAPPER					
	HR / MANAGEMENT	**IT**	**Kantine**	**SALG, INDKØB & MARKETING**	**Økonomi**
Full Control	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin	SG-IT-admin am-admin ck-admin
Modify	SG-IT	SG-IT	SG-IT	SG-IT	SG-IT
Read & Execute	SG-HR		SG-Kantine	SG-SIM	SG-Economy
Read					
Write					
Deny	SG-Economy (all) SG-Kantine (all) SG-SIM (all)	SG-Economy (all) SG-HR (all) SG-Kantine (all) SG-SIM (all)	SG-Economy (all) SG-HR (all) SG-SIM (all)	SG-Economy (all) SG-HR (all) SG-Kantine (all)	SG-HR (all) SG-Kantine (all) SG-SIM (all)

Nedenfor listes en række eksempler på, hvordan tildelingen af regler så ud i praksis - bemærk dels at der kun er tale om et udsnit og dels at der er tildelt regler til Security Groups og brugere i nogle eksemplerne.

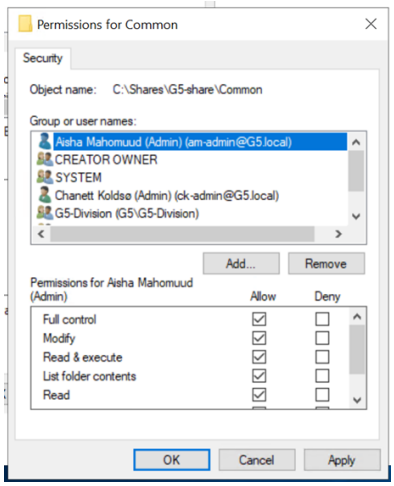
Common mappe:
G5-Division SG tilladelser



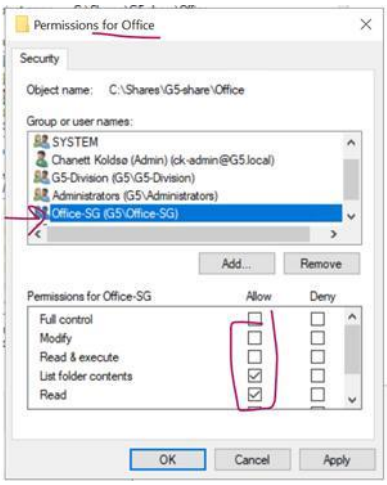
Common mappe:
SG-IT-Admin tilladelser



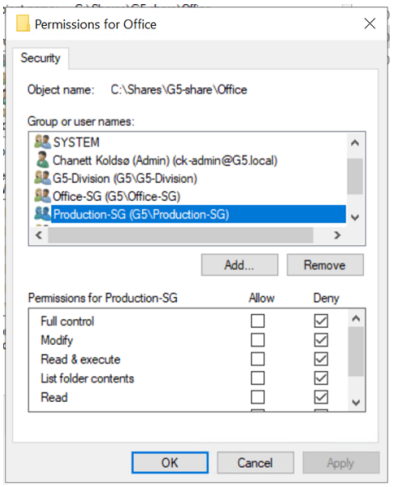
Common mappe:
am-admin brugertilladelser



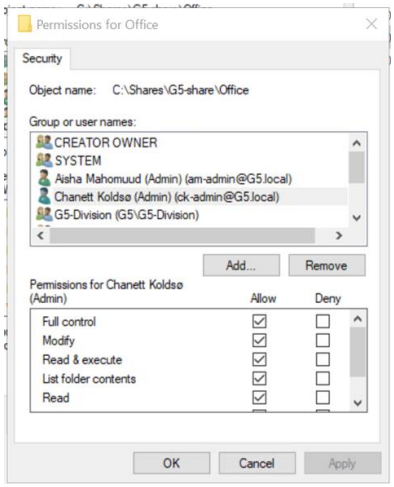
Office mappe:
G5-Division SG tilladelser



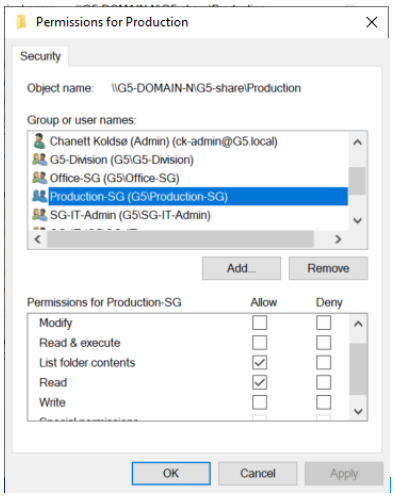
Office mappe:
Production-SG tilladelser



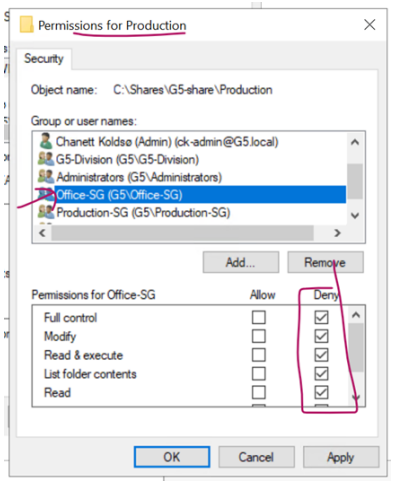
Office mappe:
ck-admin brugertilladelser



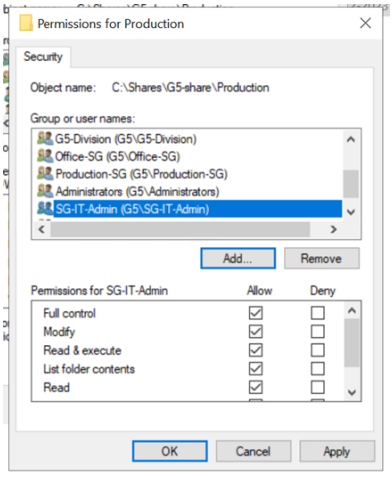
Production mappe:
Production-SG tilladelser



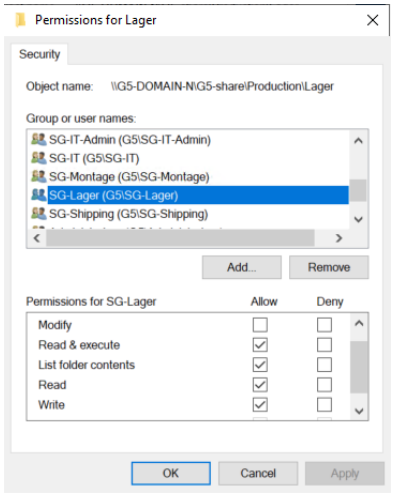
Production mappe:
Office-SG tilladelser



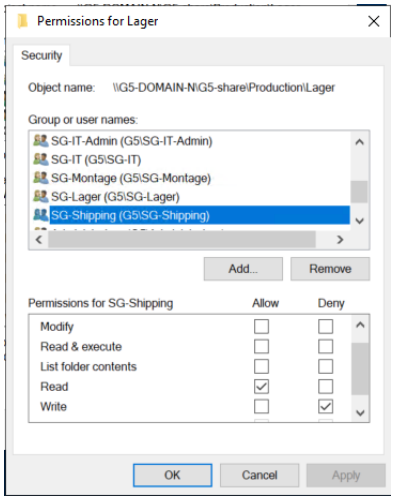
Production mappe:
SG-IT-Admin tilladelser



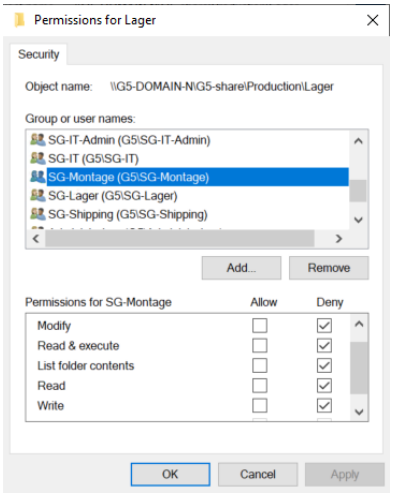
Lager mappe:
SG-Lager tilladelser



Lager mappe:
SG-Shipping tilladelser



Lager mappe:
SG-Montage tilladelser

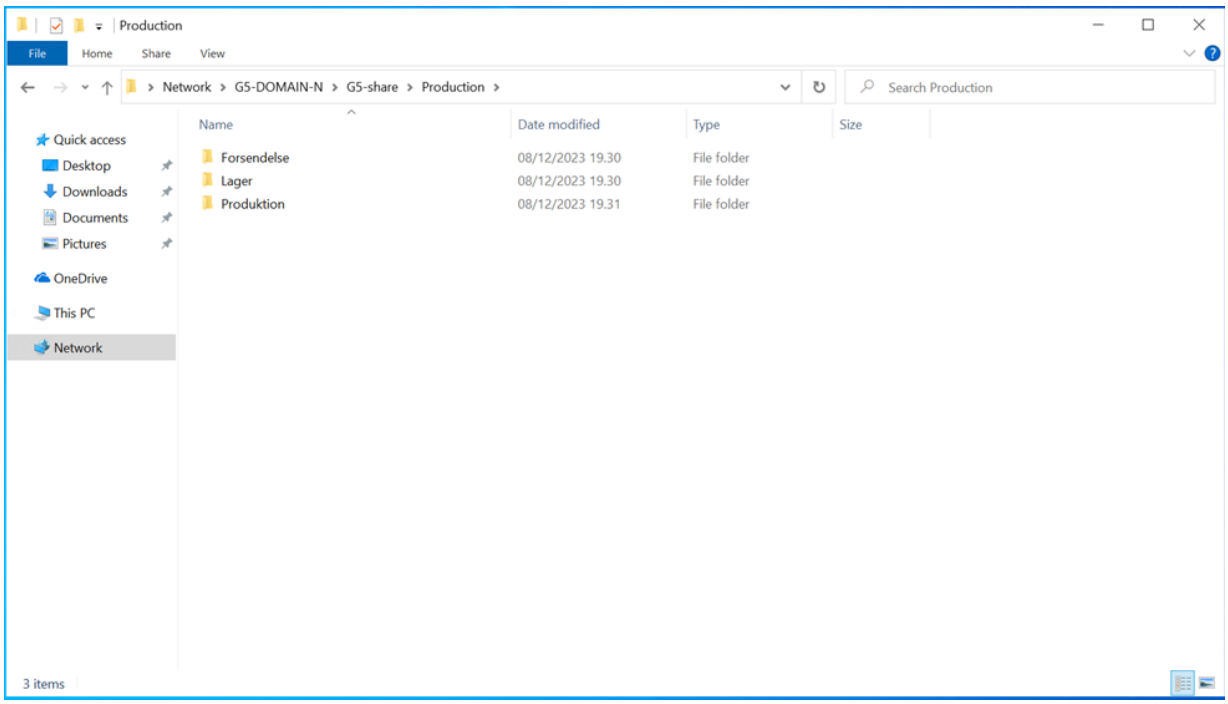


Med reglerne på plads blev det testet i praksis.

5.5.7 Tests af tilladelser

5.5.7.1 Test af Share-tilgængelighed på PC

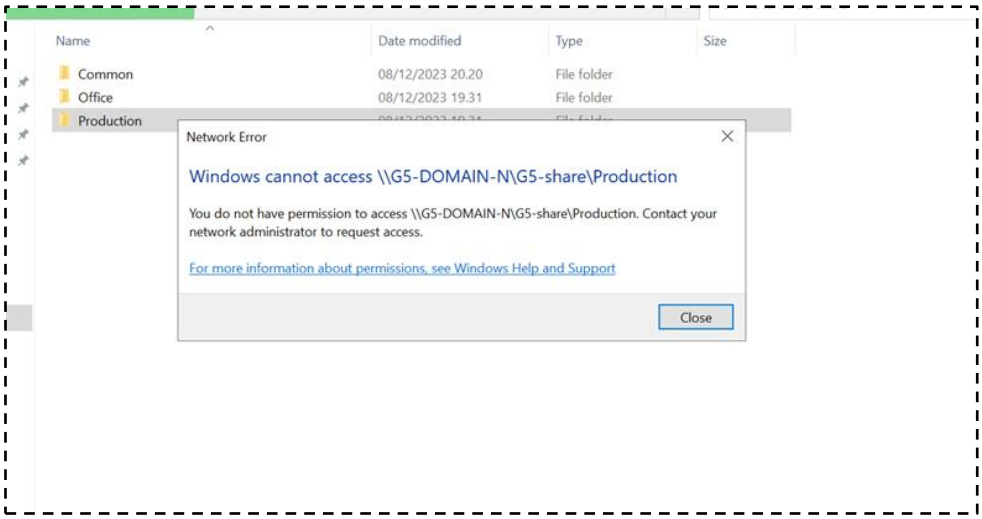
På billede 5.5.7.1.1 har bruger `ck-hr` adgang til G5-share ▸ Production. Herved bekræftes det at Shared kan tilgås af domænemedlemmer. Det bekræftes også, at der ikke er opsat permissions endnu, eftersom en bruger fra Office-SG kan tilgå mapper, som oprindeligt kun skulle kunne tilgås fra Produktion-SG jf. de opstillede krav om brugertilladelser i afsnit 4. Krav.



Billede 5.5.7.1.1: Delte mapper set fra bruger "ck-hr" i Office-SG

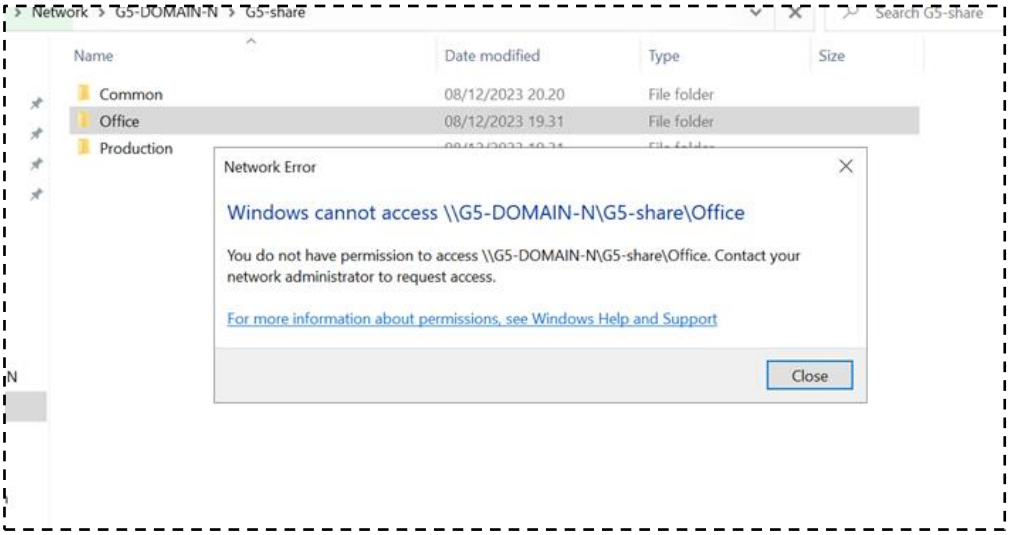
5.5.7.2 Opfølgende test på Share-tilgængelig til anden afdeling

Af testen i afsnit 5.5.7.1 Test af Share-tilgængelighed på PC blev det bekræftet at en bruger fra Office afdelingen kunne tilgå Production afdelingens delte mapper, hvilket ikke var ønskeligt. Efter at have sat Office-SG til "deny all" i Production hovedmappen blev tilgængeligheden testet igen - og bekræftet at Office nu får adgang nægtet.



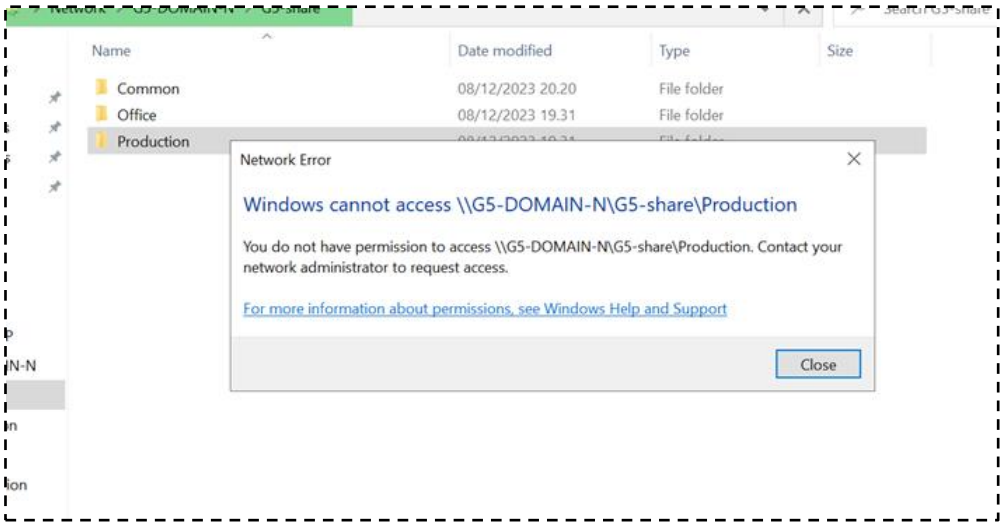
Billede 5.5.7.2.1: Office afdeling kan ikke tilgå Production afdeling

Det blev ligeledes bekræftet at brugeren am-lager fra SG-Lager ikke kunne tilgå Office mappen.



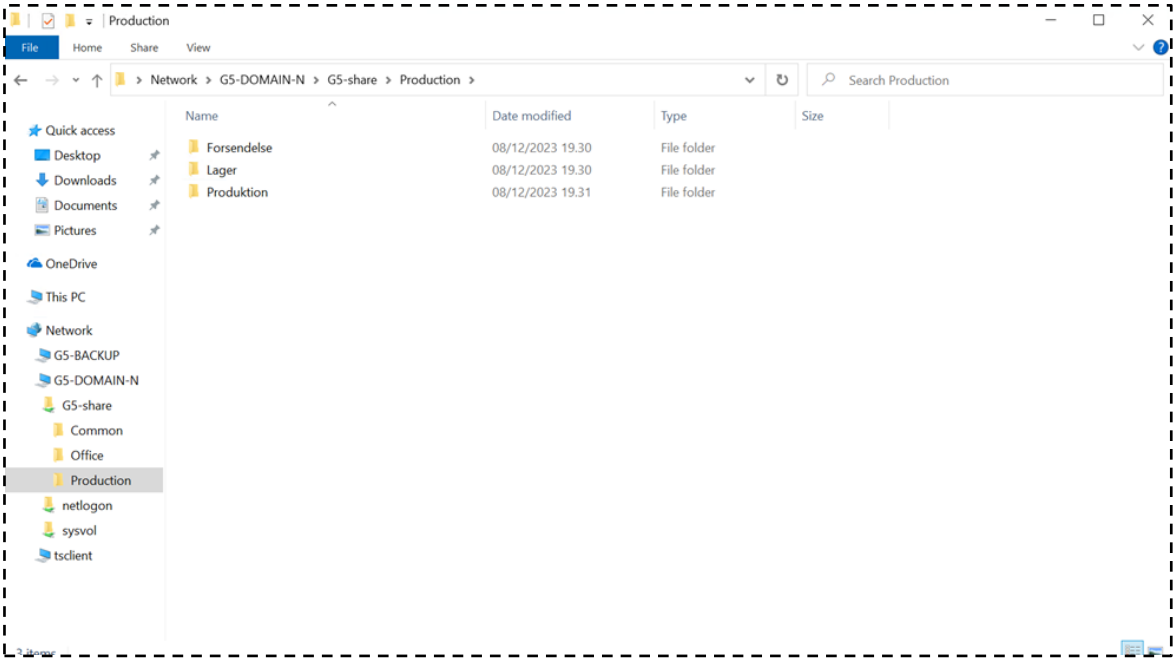
Billede 5.5.7.2.2: Lager afdeling kan ikke tilgå Office afdeling

Men det blev også bekræftet, at brugeren am-lager heller ikke kunne tilgå sin egen mappe, hvilket måtte skyldes en fejl i tildelingen af tilladelser.



Billede 5.5.7.2.3: Der findes fejl i tilladelser

Ved gennemsyn af reglerne for mappen Lager, blev det opdaget at G5-Division (en SG der dækker alle AVK-afdelinger) var sat til "deny all". Efter denne regel blev fjernet, virkede det efter hensigten og am-lager kunne tilgå mappens indhold.

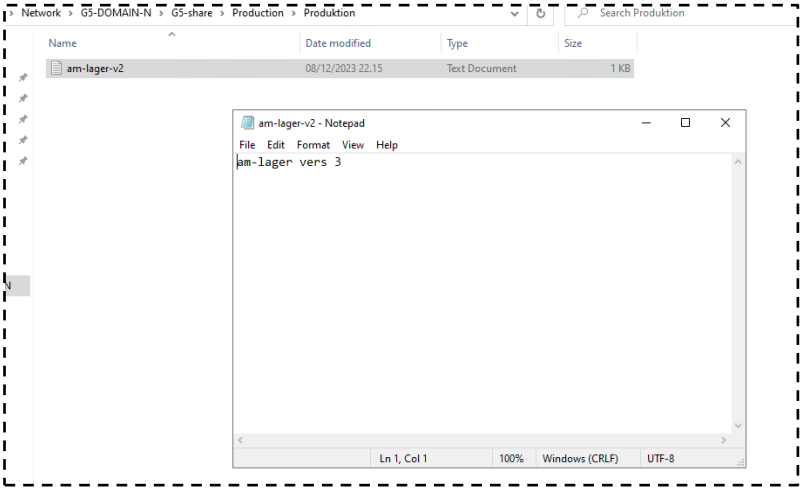


Billede 5.5.7.2.4: Fejlen i tilladelser blev rette og der er opnået adgang til mappen

5.5.7.3 Test af fil-tilladelser

I denne test undersøges det om brugeren am-lager kan ændre filer i mappen Produktion. Som det er tiltænkt, vil brugeren kunne læse (read) filer i mappen, men vil hverken kunne skrive (write)

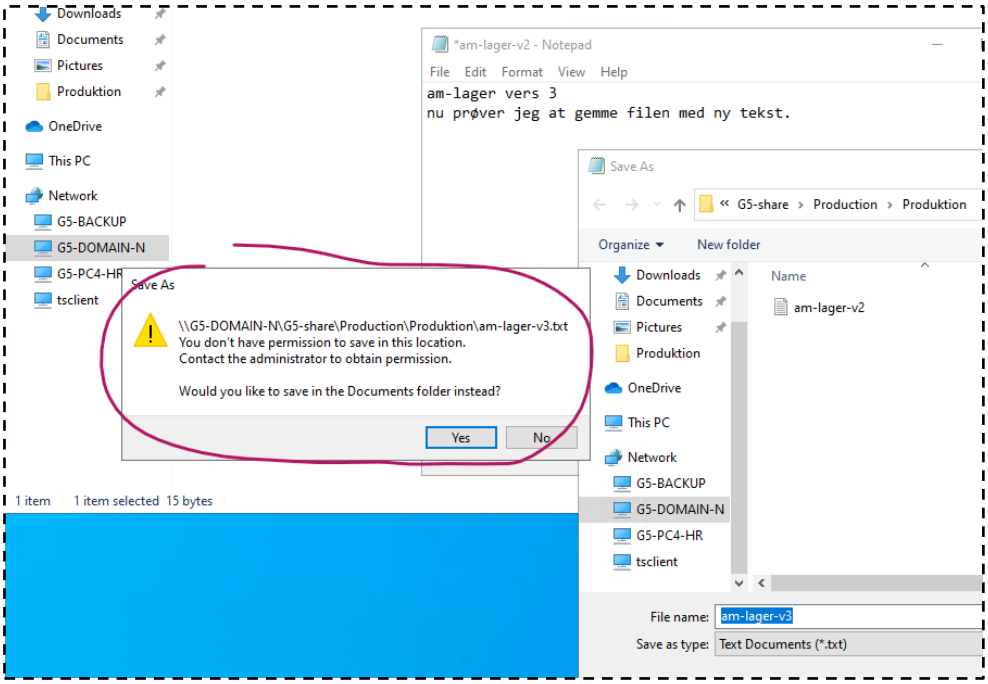
eller på anden måde ændre dem (read & execute, modify). På billede 5.5.7.3.1 bekræftes det, at brugeren kan læse filer.



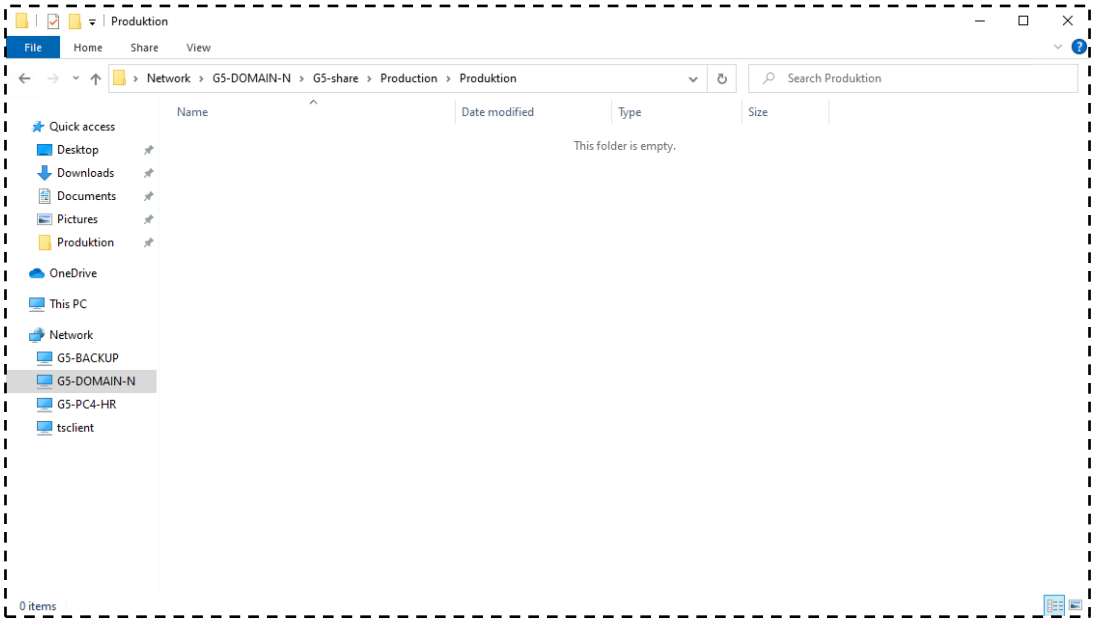
Billede 5.5.7.3.1: Brugeren kan læse filer

På billede 5.5.7.3.2, bekræftes det at brugeren am-lager - som planlagt - ikke kan modificere filen. Til gengæld var det muligt for brugeren at slette filen - som det fremgår af billede 5.5.7.3.3 - hvilket ikke er et ønskeligt scenarie.

Det er beklageligvis en sag, som må nedprioriteres til fordel for opsætning af Backup og derfor gøres der ikke mere ved det nu, men en årsag kan måske ligge i en overordnet regel, der er nedarvet og som er blevet overset.



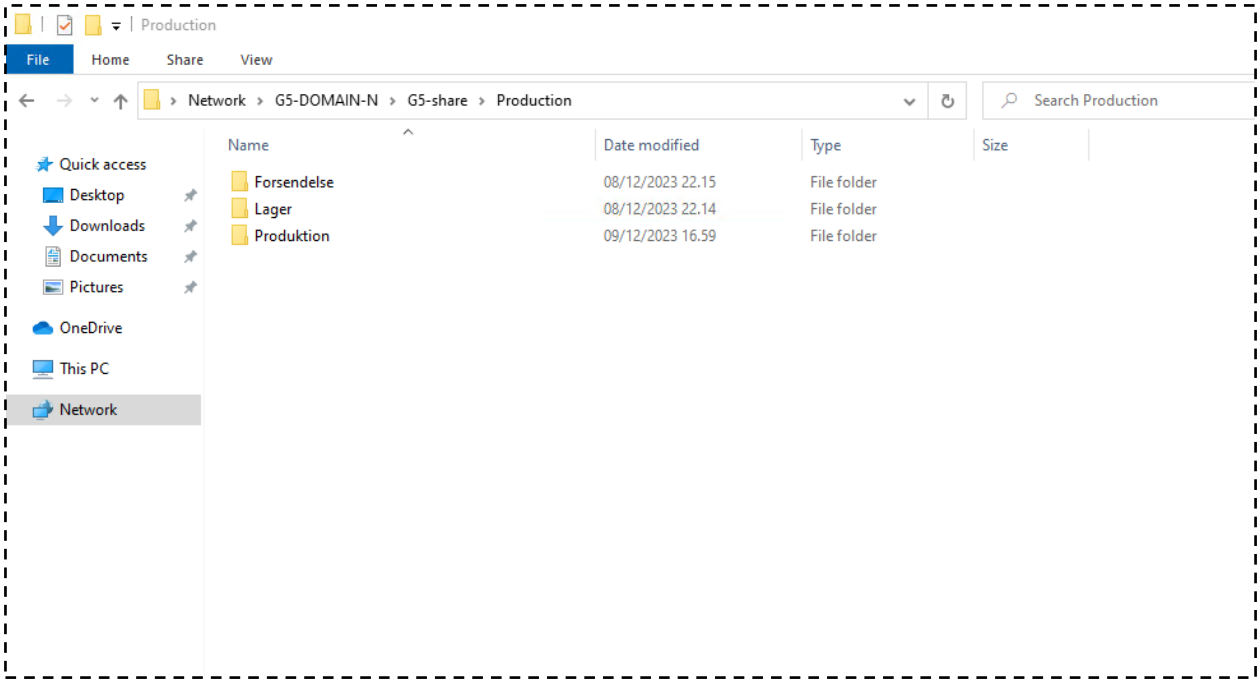
Billede 5.5.7.3.2: Bruger kan ikke skrive eller modificere fil



Billede 5.5.7.3.3: Bruger kan slette en fil - det er en fejl i tilladelsen

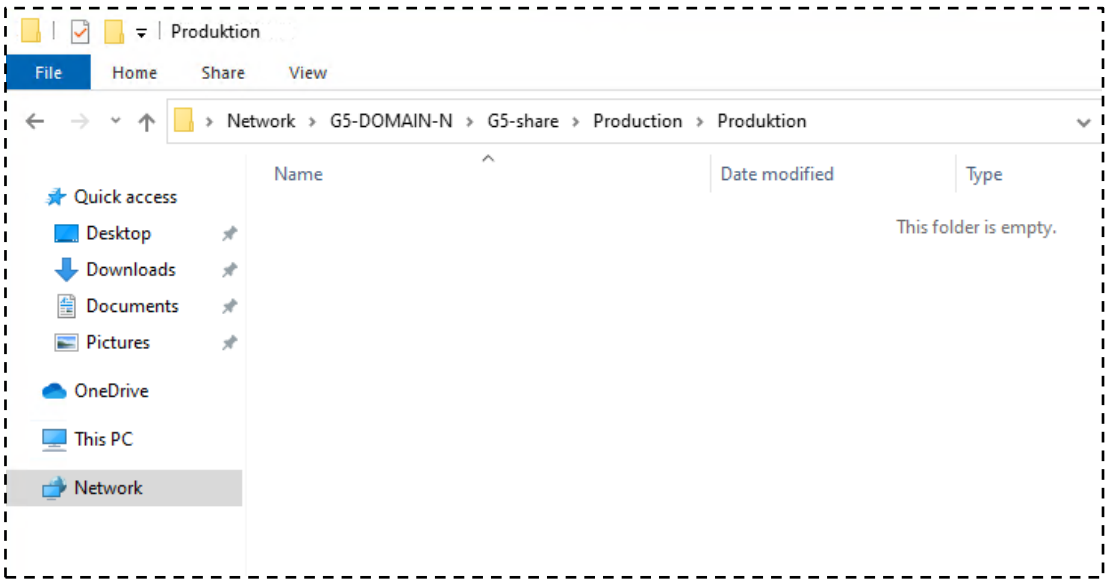
Nu testes det, om brugeren am-montage fra produktionen kan tilgå mapper eller filer fra lager. Som vist i afsnittet om tilladelser er SG-Montage sat til "deny all". Så det burde ikke kunne lade sig gøre.

Brugeren kan - som tiltænkt - tilgå hovedmappen "Production".



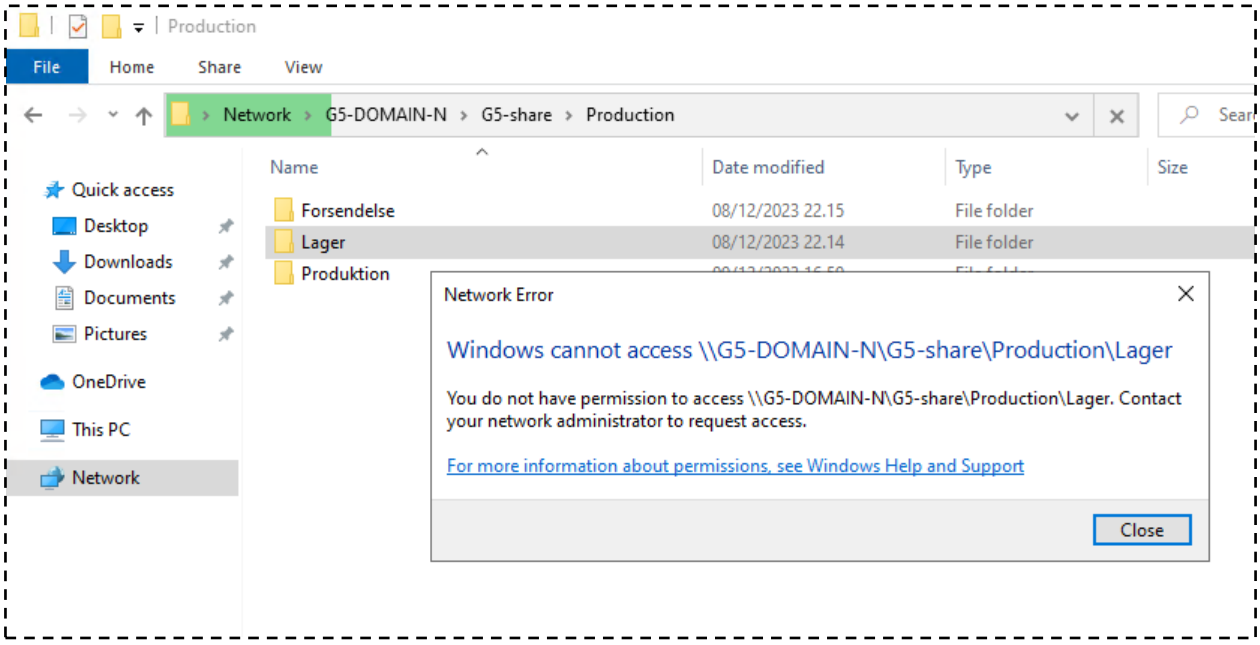
Billede 5.5.7.3.4: Brugeren kan tilgå hovedmappen "Production"

Adgang til undermappen "Produktion" er også givet, så det er fortsat som planlagt og nu ved vi at brugeren har adgang til minimum én undermappe.



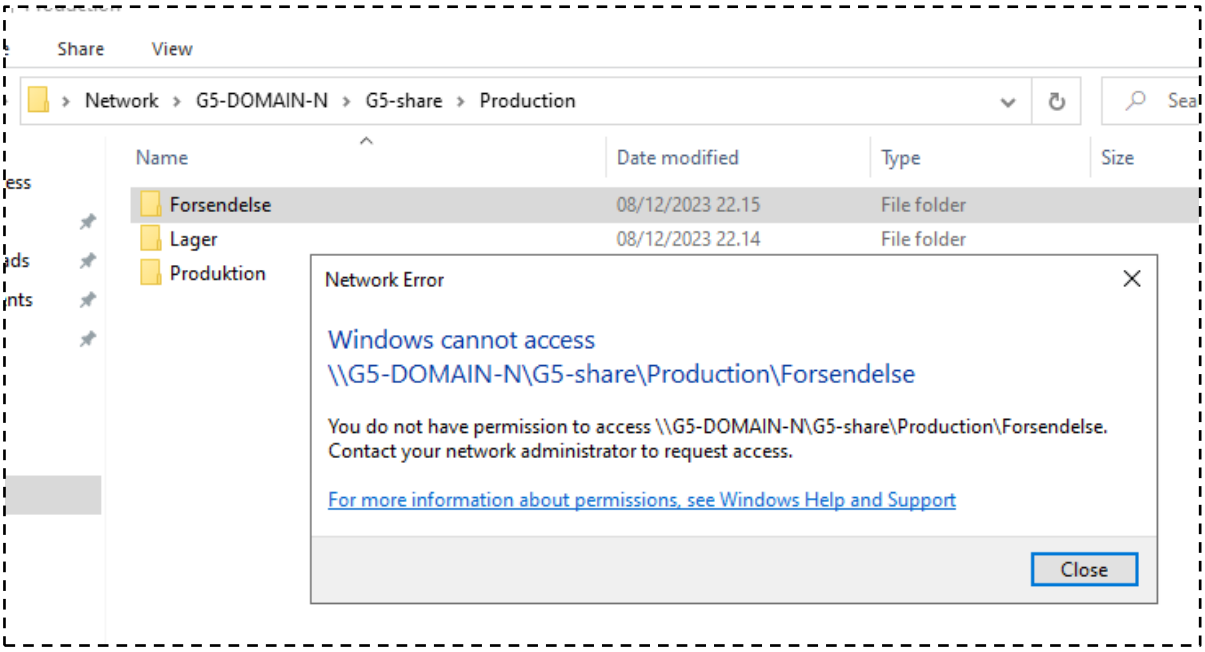
Billede 5.5.7.3.5: Brugeren har adgang til minimum én undermappe

Adgang til mappen "Lager" er nægtet, som forventet.



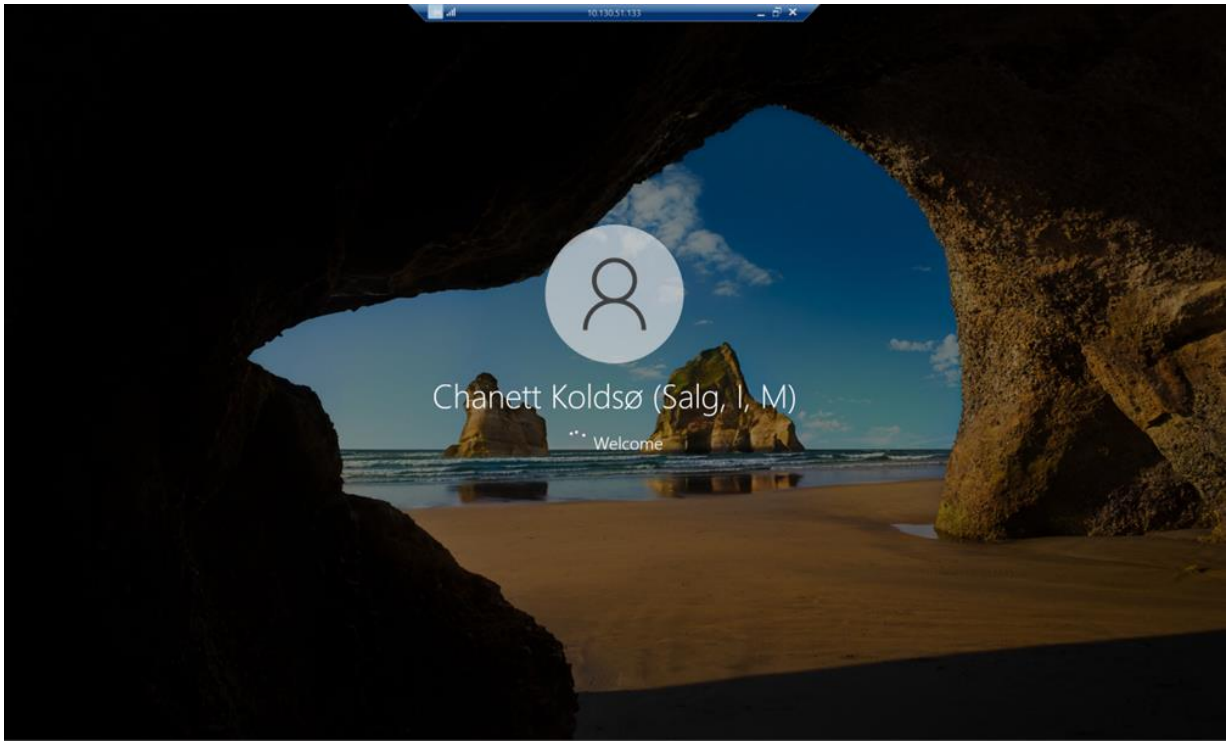
Billede 5.5.7.3.6: Montage-bruger har ikke adgang til lager-mappen

Så testes adgangen til mappen "Forsendelse".



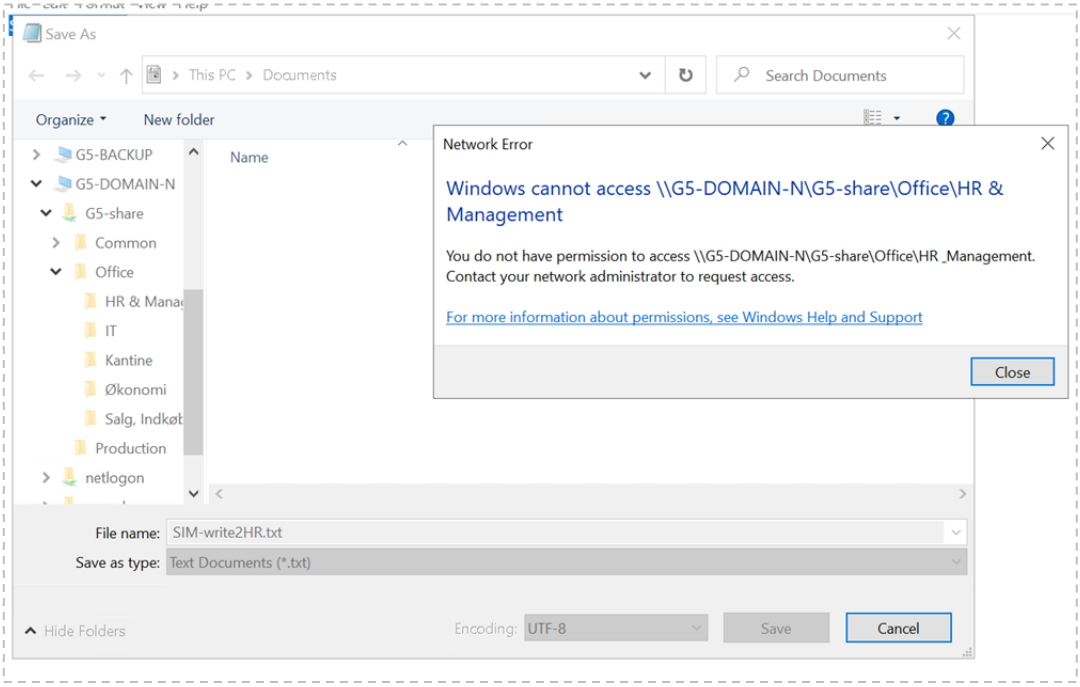
Billede 5.5.7.3.7: Montage-bruger har heller ikke adgang til mappen Forsendelse

Her nægtes ligeledes adgang, så tilladelserne er korrekte. En yderligere test blev foretaget med brugeren ck-sim (salg, indkøb og marketing).



Billede 5.5.7.3.8: SIM-bruger login-page

En test viste at brugeren ikke kunne tilgå andre undermapper end sin egen. Ved fx HR & Management, blev adgang nægtet ligesom det blev, da vi forsøgte adgang til de andre mapper.



Billede 5.5.7.3.9: SIM-bruger har ikke adgang til HR mappen

Herefter foretog vi test af filtilladelser og fandt at:

- ➔ SIM kan skrive til common, Office mappen og egen mappe.
- ➔ SIM kan omdøbe, kopiere og slette i common, egen mappe samt OFFICE mappe
- ➔ SIM kan oprette mapper i Common, OFFICE og egen mappe

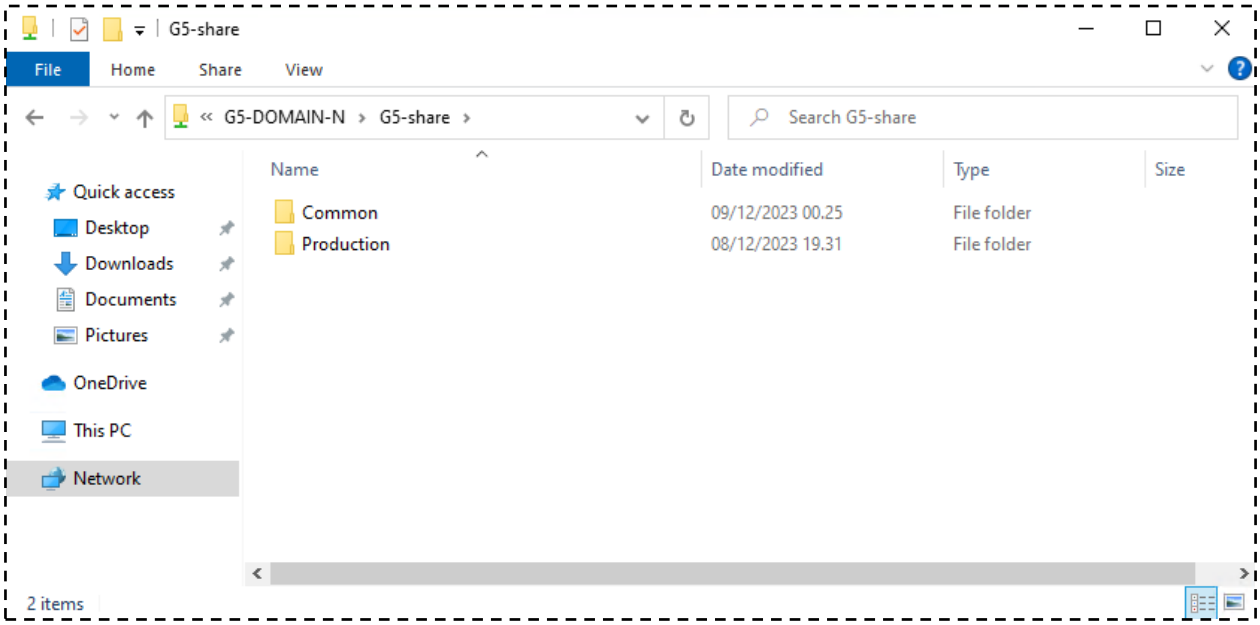
5.5.7.4 Test af modifikationstilladelser

Til udførelsen af denne test logges ind på brugeren am-it, der tilhører SG-IT. SG-IT har MODIFY aktiveret for alle mapper. Der blev foretaget forskellige tests såsom;

- ➔ oprettelse samt omdøbning af filer og mapper
- ➔ læsning og skrivning af filer
- ➔ sletning af filer

Slutteligt blev det undersøgt om brugeren kunne slette en hovedmappe. Yep! Kan det hele. Dum nok som jeg var - kl. 2.00 om natten, tog jeg ikke en kopi eller snapshot og slettede OFFICE

mappen (med de mange tilladelser i) blot for at finde ud af, at mappen ikke kunne gendannes. Så vi mistede en stor mængde arbejde, der lå i at oprette de tilladelser tilknyttet dén og alle undermapper. Så nu ser G5-share således ud:



Billede 5.5.7.4.1: Tragisk udseende Share med en manglende mappe efter uønsket sletning

For fortsat at have en succesfuld test for nægtet adgang - eftersom den ene afdeling beklageligvis var blevet slettet fra jordens overflade, blev det i stedet gjort således at afdelingen Montage ikke skulle have adgang til Lager og Forsendelse, hvilket sådan set giver god nok mening. Dog kunne vi se meningen i fortsat at lade Lager og Forsendelse kunne tilgå filer fra produktionen, blot ikke at skrive i dem.

Konklusionen er at Modify er en tilladelse, man skal give med varsomhed - og i hvert fald ikke til et træt gruppemedlem kl. 2.00 om natten - og husk nu altid at lave backup. Hvilket bringer os til næste punkt i processen. Det kunne dog være rart at backup-delen faktisk var implementeret før OFFICE mappen blev slettet, så vi kunne teste om den kunne restore dén - det havde været praktisk. Men det er jo bare en lektion lært.

5.6 Backup med Veeam

Som sidste led i projektarbejdet var målet at implementere en backup løsning, der muliggjorde backups af filer og data. At føre backups af vigtige data er en vigtig og uundværlig del af netværksstrukturen, og uden ordentlig backups kan virksomheder stå til at gå konkurs, hvis alle

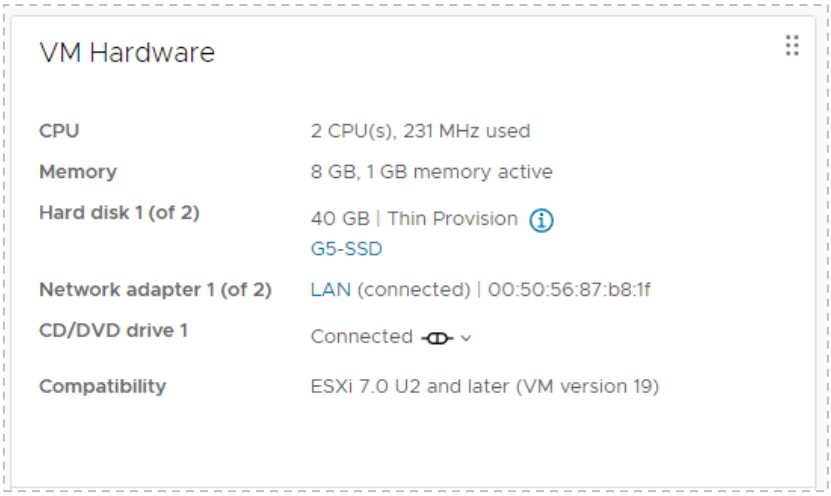
deres data bliver utilgængelige. Det kan fx ske i forbindelse med ransomware angreb, som denne case bl.a. er baseret på.

Til integrering af backup funktionalitet, integreres en Backup server, hvorpå software Veeam Backup & Replication 11 installeres. Med en mere dybdegående opsætning er det også muligt at få Veeam til at lave backup af virtuelle maskiner. Dette er der dog ikke blevet arbejdet med i projektet - i stedet er der lavet snapshots, templates og clones baseret på de virtuelle maskiner. Her vil det være praktisk, hvis disse skabeloner og gendannelsespunkter kunne gemmes i ekstern backup repository ved fx Veeam.

5.6.1 Implementering

Først blev en server opsat - denne blev døbt G5-Backup og har følgende specifikationer:

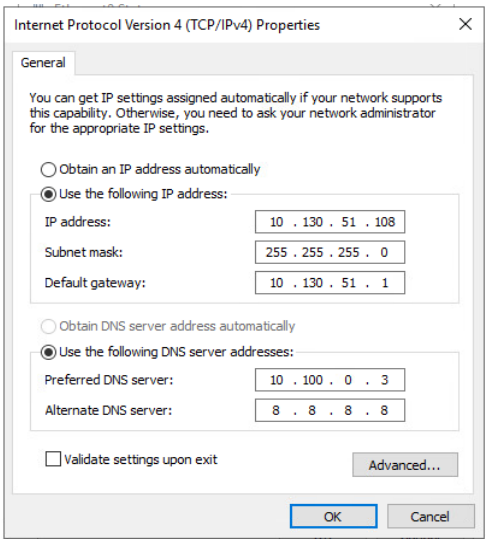
- 2 CPU'er
- 8GB RAM
- 40GB harddisk, thin provision
- Network adapter: LAN
- OS: Windows Server 2019 (64-bit)



Billede 5.6.1.1: Specifikationer for Backup server i vCenter

Herefter blev en Windows 2019 Server OS installeret. For at kunne opdatere styresystemet blev en statisk IP, Default Gateway og DNS sat til følgende:

- IP: 10.130.51.108/24
- Default Gateway: 10.130.51.1
- DNS: 10.100.0.3/8.8.8.8



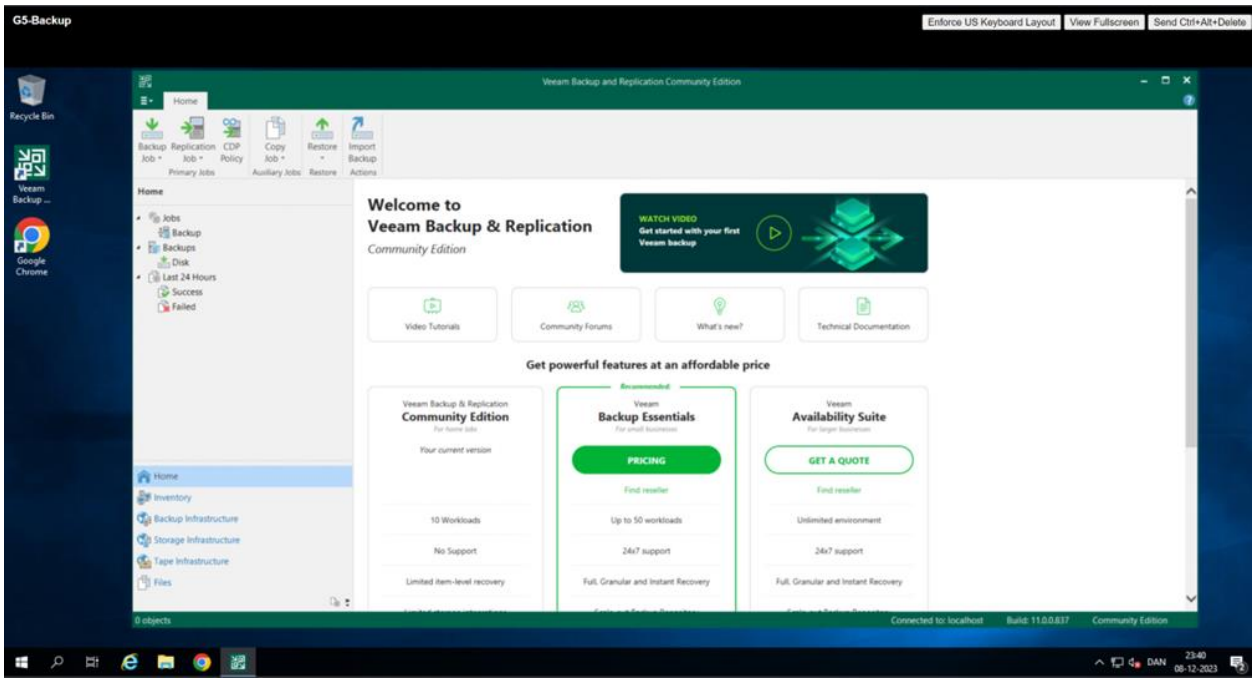
Billede 5.6.1.2: IP konfigurationer

Efter forbindelse til Google blev bekræftet med ICMP pings, kunne systemet opdateres.

```
C:\Users\Administrator>ping google.com

Pinging google.com [172.217.16.78] with 32 bytes of data:
Reply from 172.217.16.78: bytes=32 time=6ms TTL=54
Reply from 172.217.16.78: bytes=32 time=6ms TTL=54
Reply from 172.217.16.78: bytes=32 time=6ms TTL=54
Reply from 172.217.16.78: bytes=32 time=6ms TTL=54

Ping statistics for 172.217.16.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

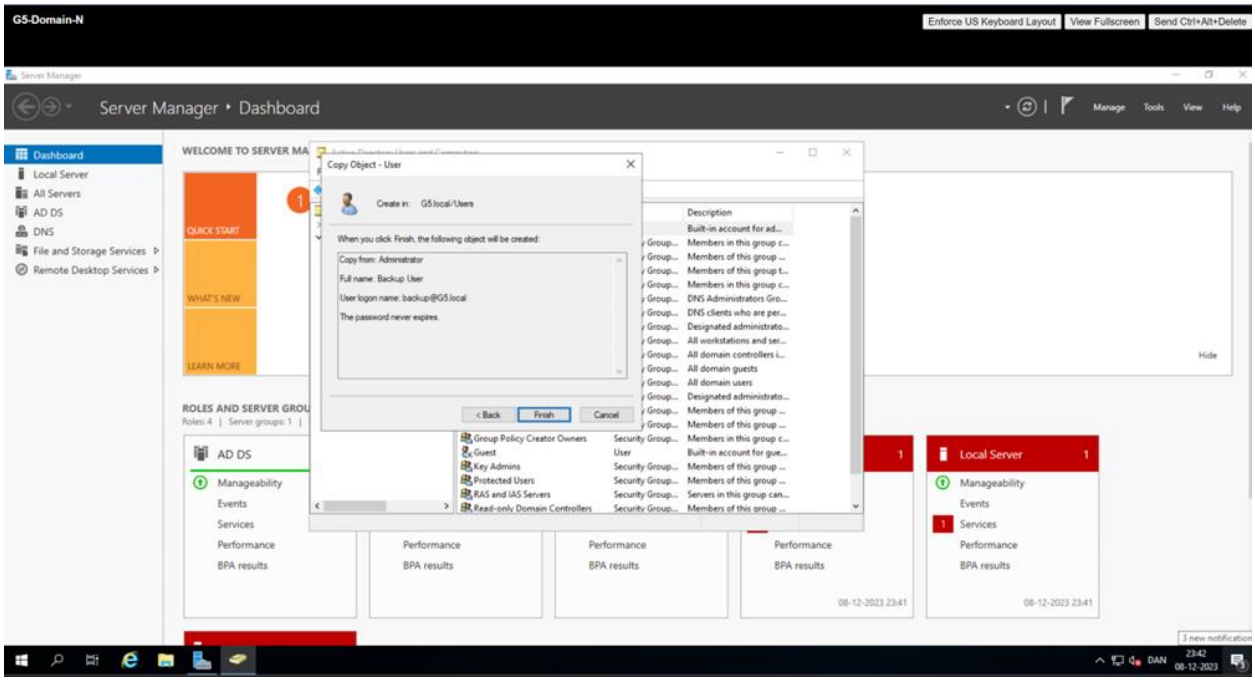
Billede 5.6.1.3: Forbindelse til Google bekræftet.

Efter endt opdatering blev Veeam Backup & Replication 11 services installeret.



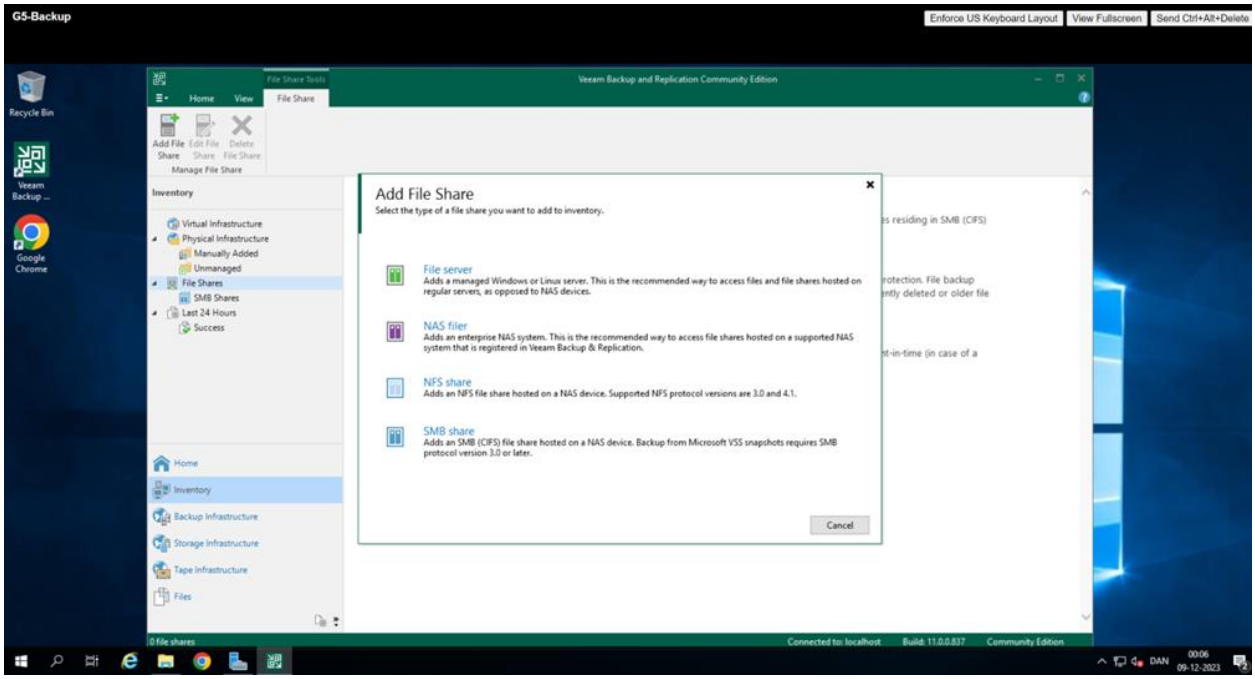
Billede 5.6.1.4: Veeam installeres på Backupserveren

Med Veeam på plads var næste skridt at tilføje en backup-user i domain serveren.

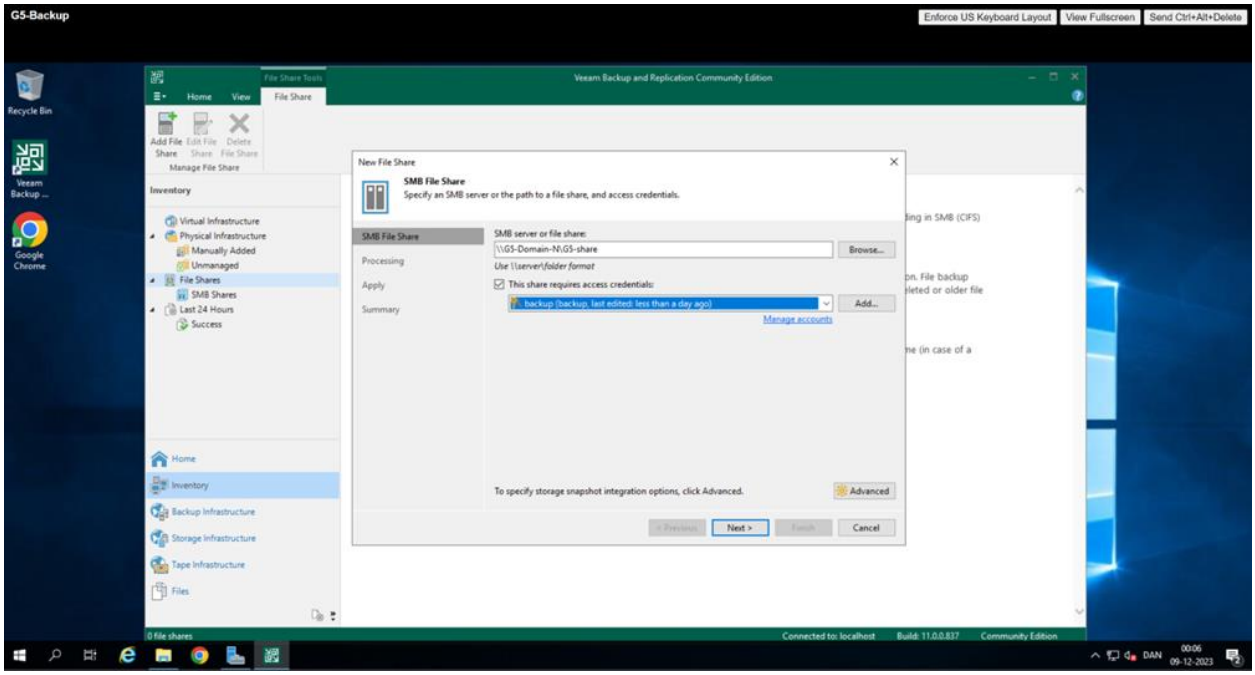


Billede 5.6.1.5: backupuser oprettes i Domain serveren

Nu kunne næste fase begynde - oprettelse af en repository med efterfølgende oprettelse og konfiguration af en SMB share.

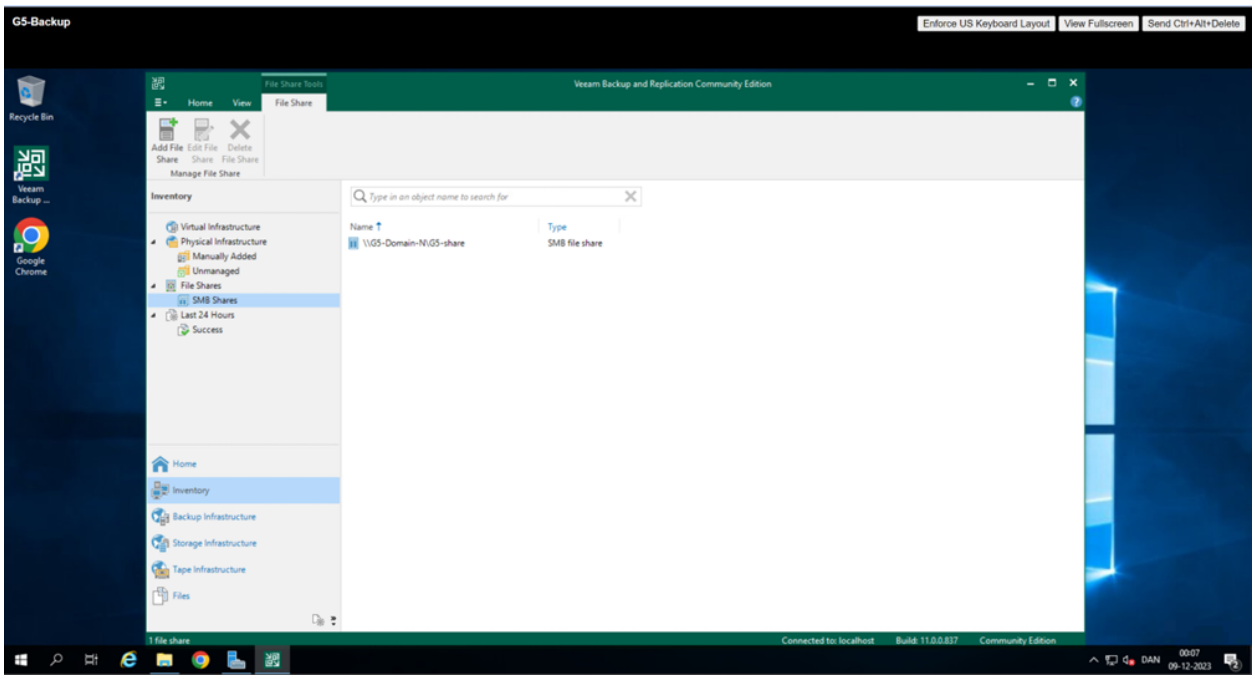


Billede 5.6.1.6: SMB Share tilføjes

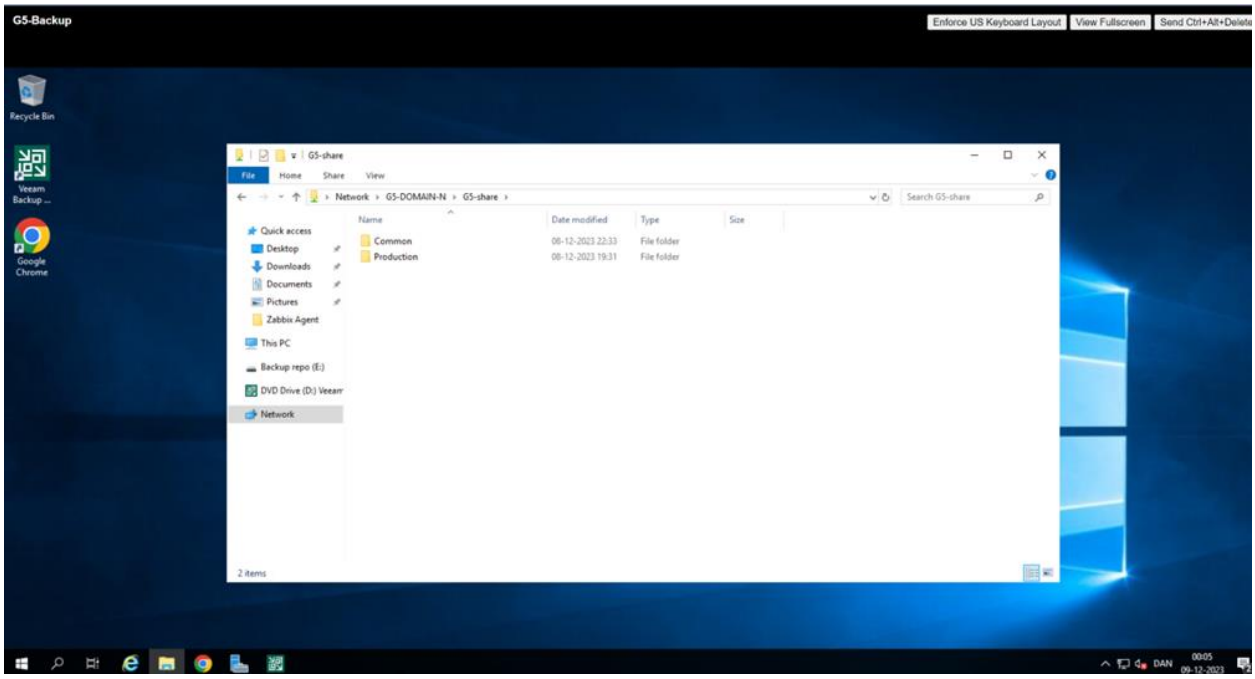


Billede 5.6.1.7: konfiguration af SMB-share

Inden næste skridt verificeres det, at den nye SMB-share var oprettet og at Backupserveren havde adgang til domænet.



Billede 5.6.1.8: bekræftelse på at SMB-share er oprettet

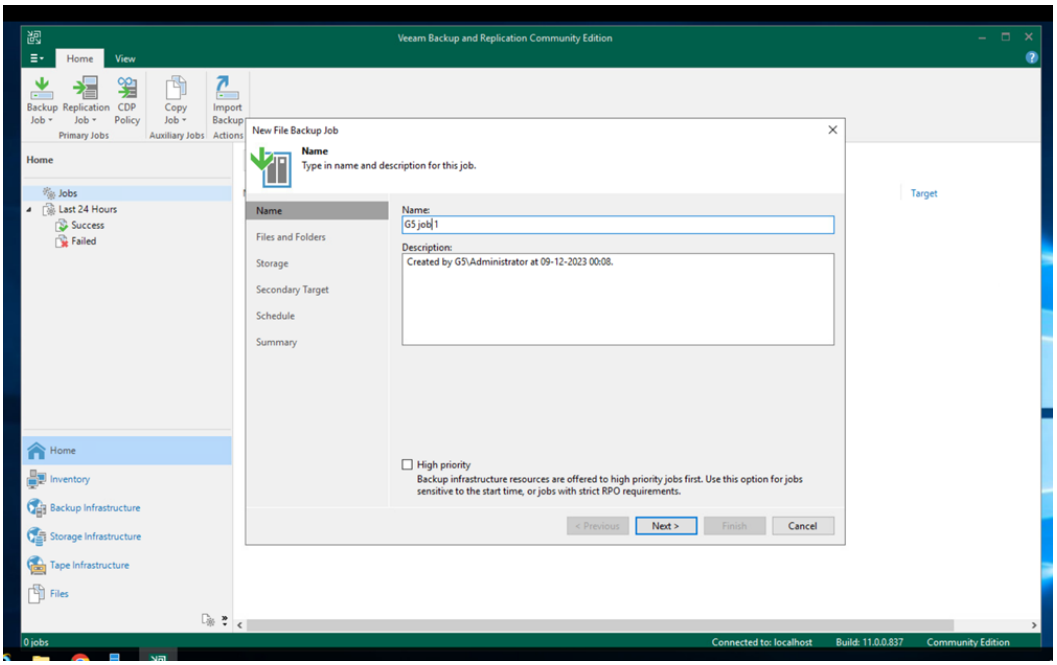


Billede 5.6.1.9: bekræftelse på at backupserveren har adgang til domænenetværket

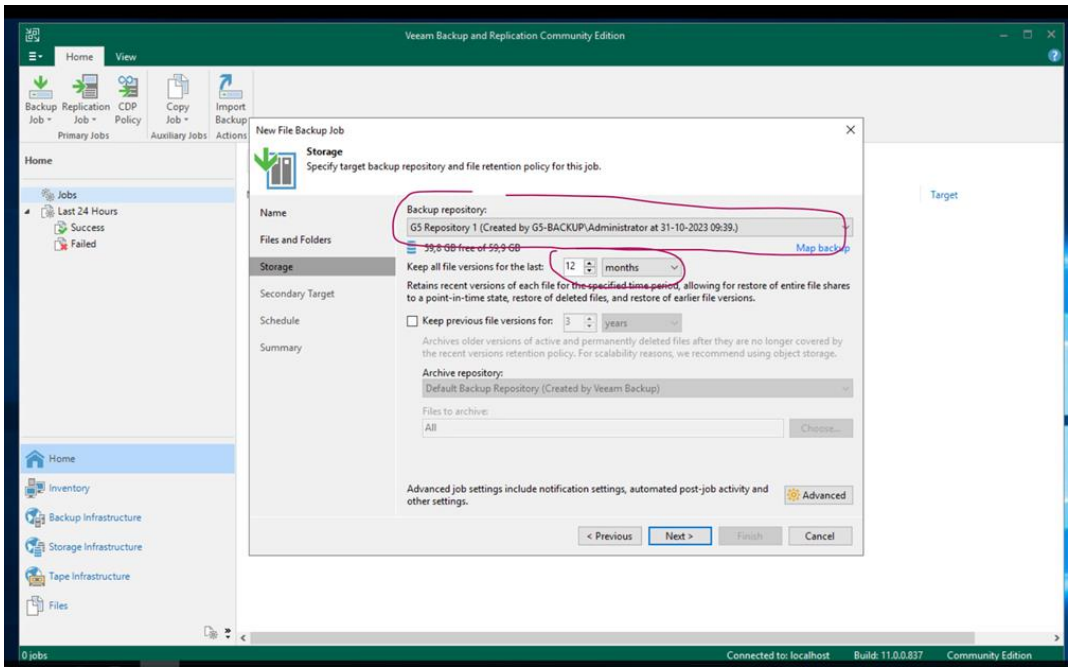
Med disse konfigurationer skulle Veeam være i stand til at foretage backup jobs. Dette testes i afsnit 5.6.2 Test af Veeam Backup.

5.6.2 Test af Veeam Backup

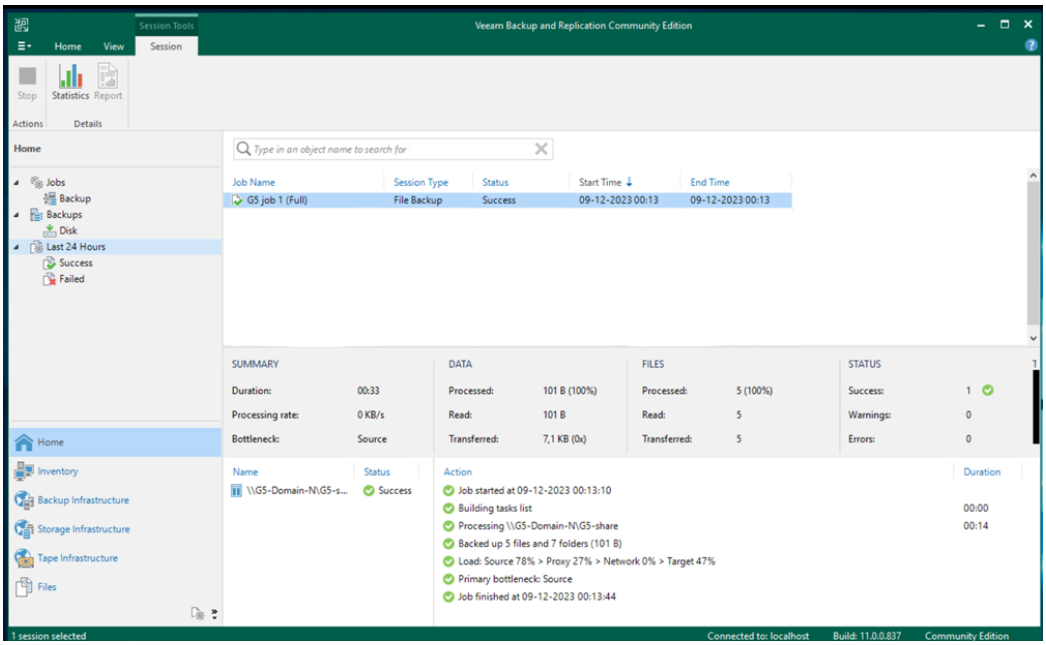
Et backup-job blev oprettet som vist i nedenstående billeder.



Billede 5.6.2.1: Veeam backupjob oprettes og navngives

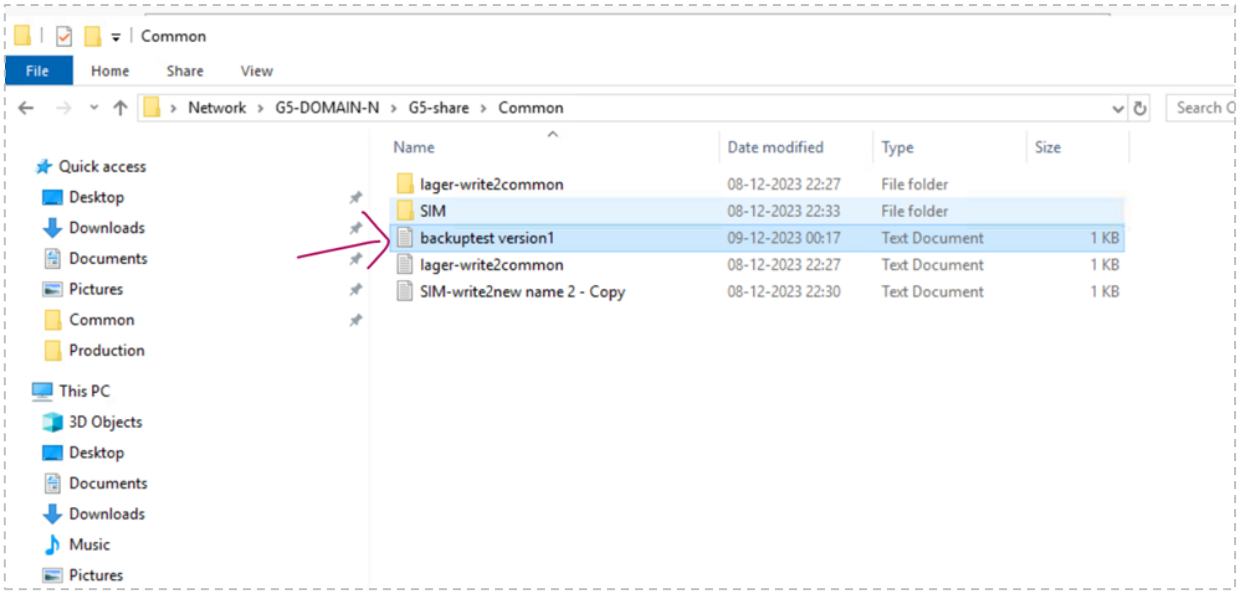


Billede 5.6.2.2: Repository vælges til backupjob



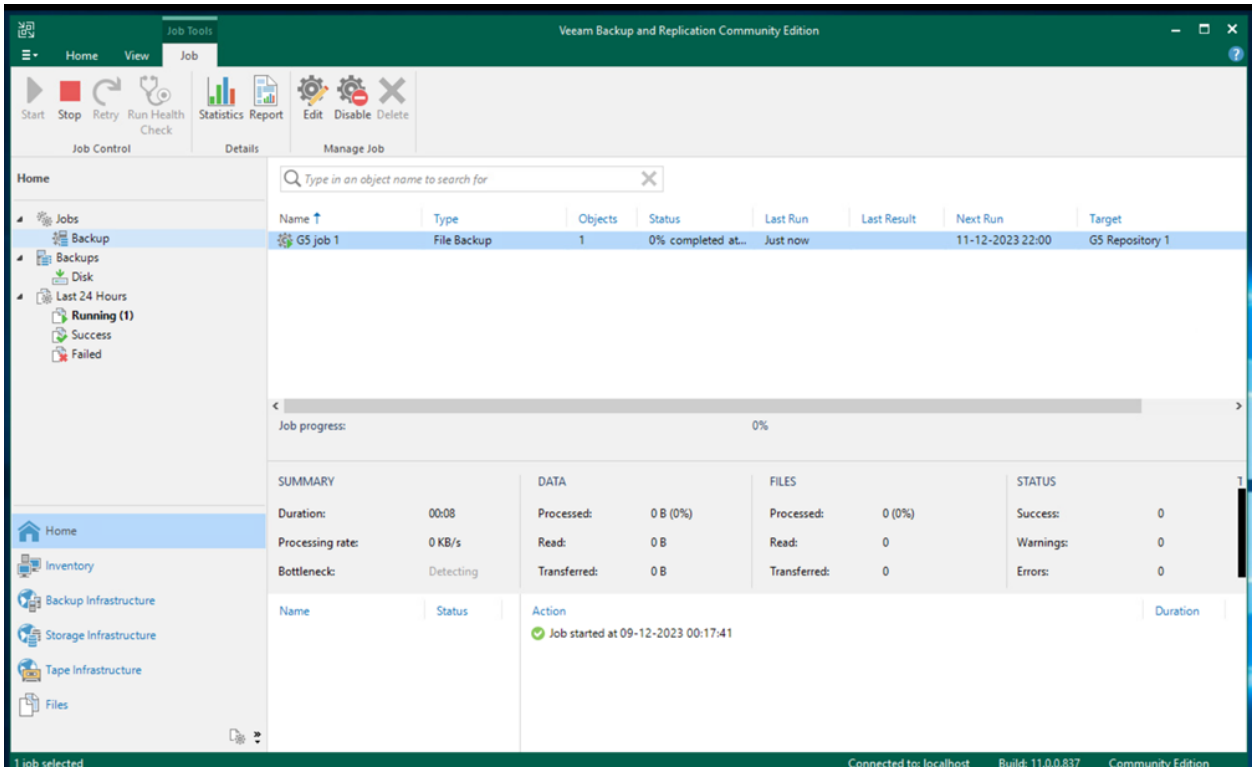
Billede 5.6.2.3: Veeam backupjob oprettet

For at teste funktionaliteten af backupjobbet, blev der først oprettet en fil i en af mapperne, hvorefter at backup blev kørt igen.



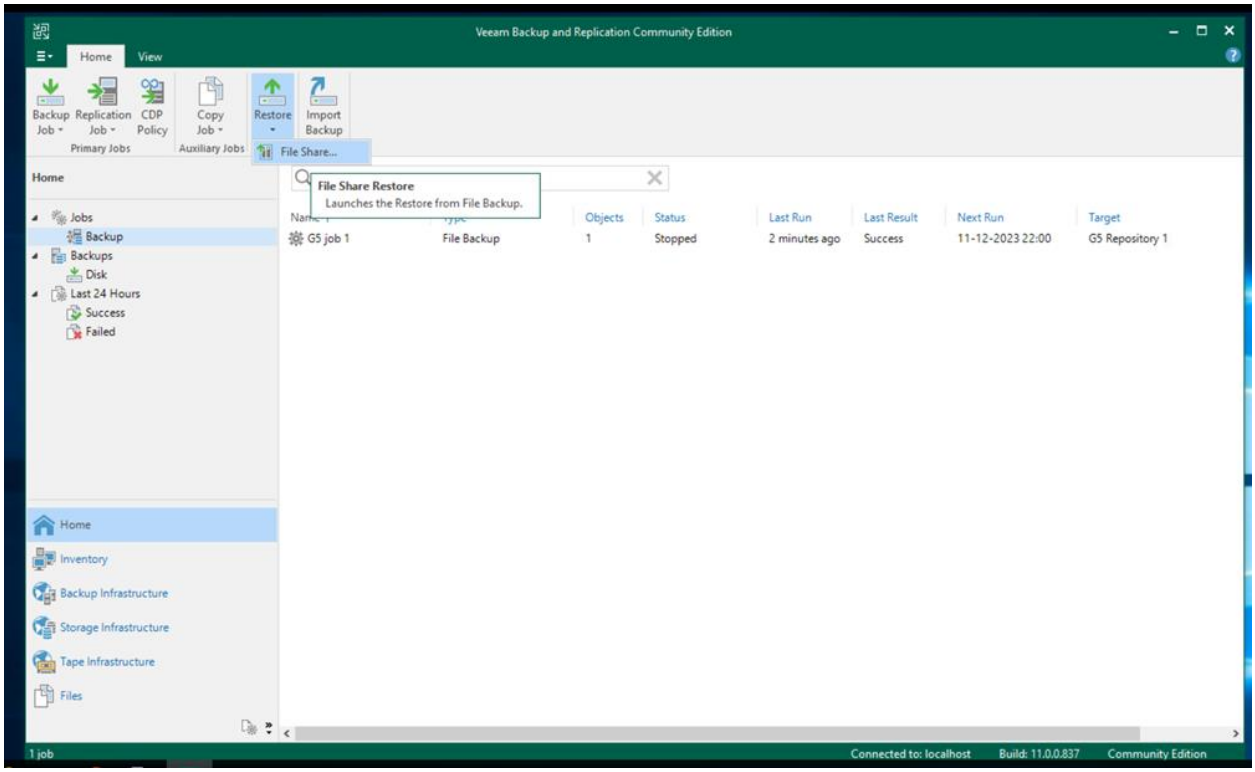
Billede 5.6.2.4: Fil oprettes til testformål

Billede 5.6.2.5: Fil indhold



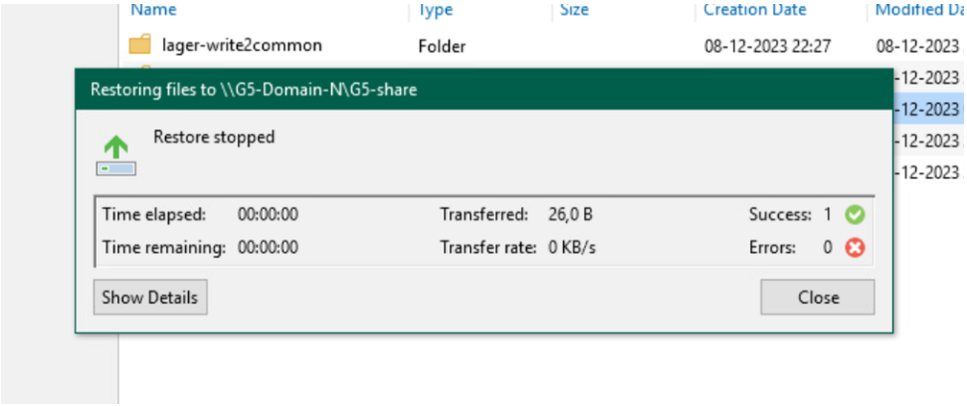
Billede 5.6.2.6: Backup foretages

Herefter blev en ekstra linje tilføjet til tekstfilen. Backup blev kørt igen efterfulgt af første restore-job:



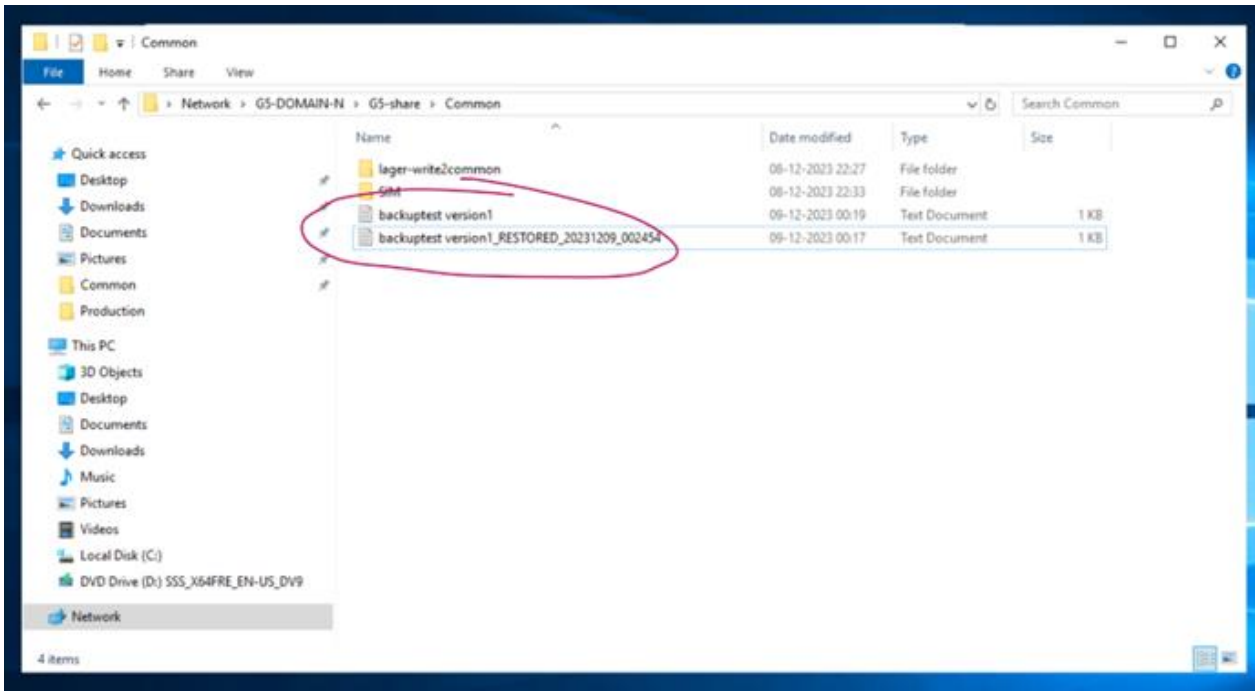
Billede 5.6.2.7: Restore job oprettes

Ved en gendannelse af filen kan man vælge mellem to funktioner: "overskriv" eller "behold". For at teste funktionaliteten valgtes "Behold".



Billede 5.6.2.8: Restorejob køres

Efter kørt restore-job var der nu to filer i mappen.



Billede 5.6.2.9: en RESTORED fil er nu tilføjet i mappen

Slutteligt i testen åbnes begge filer, hvor indholdet sammenlignes.

Billede 5.6.2.10: Backupfil

Billede 5.6.2.11: Restored fil

Hermed bekræftes det, at Veeam Backup & Replication 11 fungerer efter hensigten og backup er sat op for filer og mapper for shared G5.

6. PROJEKTHÅNDTERING

I dette afsnit vil vi præsentere de forskellige metoder, vi har anvendt under vores projektarbejde for at sikre en effektiv og struktureret tilgang. Disse metoder spiller en vigtig rolle i planlægningen og styringen af vores projekt og har bidraget til at skabe overblik, estimere tid og ressourcer samt sikre en trinvis progression. Vi vil kort introducere Vandfaldsmodellen, Work Breakdown Structure (WBS) metoden og brugen af Gantt-kort til tidsplanlægning. Udover de nævnte værktøjer, førte vi en logbog (Bilag 13: Logbog), der havde til formål at give et nutidigt overblik over arbejdsprocessen med statusopdatering. Planen var at denne logfil skulle opdateres dagligt, hvilket den desværre ikke blev.

Ved at kombinere disse metoder har vi opnået et solidt grundlag for vores projektarbejde.

6.1 Vandfaldsmetoden

Projektarbejdet har fulgt den lineære og faseopdelte udviklingsproces, som kendetegner vandfaldsmetoden. Udviklingsparadigmet er opdelt i følgende faser:

- ➔ Analyse
- ➔ Design
- ➔ Implementering & Test
- ➔ Vedligeholdelse

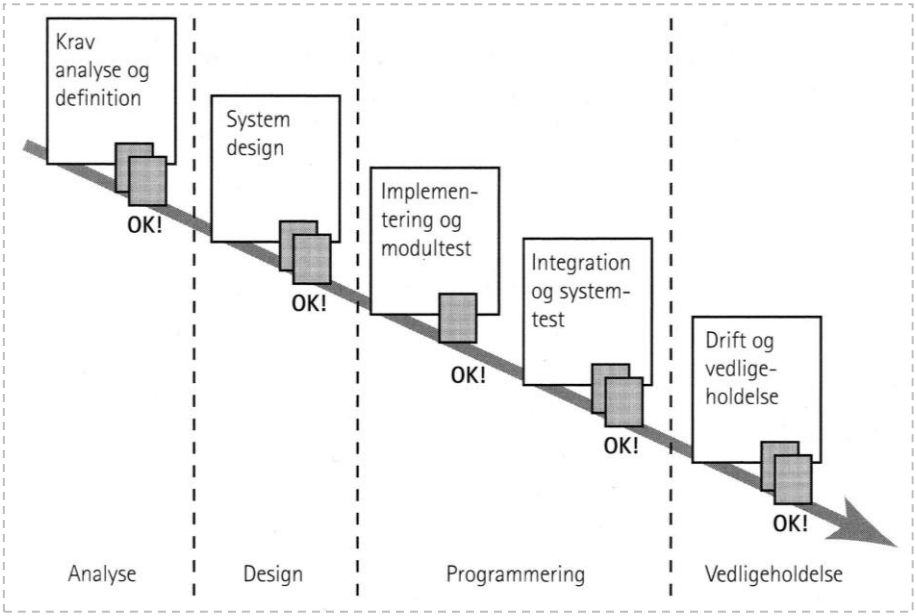


Diagram 6.1.1: "Vandfaldsmetodeparadigmet"
s. 32"Udvikling af multimedier - en helhedsorienteret metode"

Sidstnævnte fase er ikke så fremtrædende i projektet, men kommer mest til udtryk i tankerne for det fremtidige mål. Tankerne om at føre et redundant og virtuelt miljø, der er pålideligt og let at vedligeholde samt let at erstatte ved nedbrud. Dette er dog med forudsætning af, at der er truffet forholdsregler i form af skabelsen af snapshots, templates, kloner, backups, sikkerhedskopier m.v.

Jf. vandfaldsmetoden lægges opgaverne efter en klar struktur, hvor hver fase skal afsluttes før den næste, kan begynde. Det ses eksempelvis i, at behovsanalysen skulle foreligge før kravene, kunne nedfældes. Disse skulle ligge klar før designfasen kunne begynde osv. Denne lineære struktur skinner også igennem i faseopdeling af arbejdsopgaverne som set i WBS-diagrammet og igen i tidsplanlægningen i Gantt-kortet. Disse bliver uddybet i de næste afsnit.

Da udviklingsarbejdet har haft denne naturlige struktur, fandt gruppen det også naturligt, at rapportens opbygning skulle bygges på de samme strukturelle linjer. Selve rapporten er bygget op efter projektmodulerne i WBS-diagrammet og afsnittene er opbygget efter den lineære struktur fra vandfaldsmetoden - design, implementering og test.[12]

6.2 Work Breakdown Structure

For at opnå klarhed og udarbejde en realistisk tidsplan har vi valgt at anvende Work Breakdown Structure (WBS) metoden ved hjælp af Click-up app'en. WBS er en metode, der bryder projektet ned i mindre, håndterbare dele, såsom opgaver eller underopgaver. Dette skaber en overskuelig og struktureret opsummering af projektets omfang og hjælper med at identificere de nødvendige ressourcer og den krævede tidsramme for hver del af projektet.

Projektet deles op i seks dele:

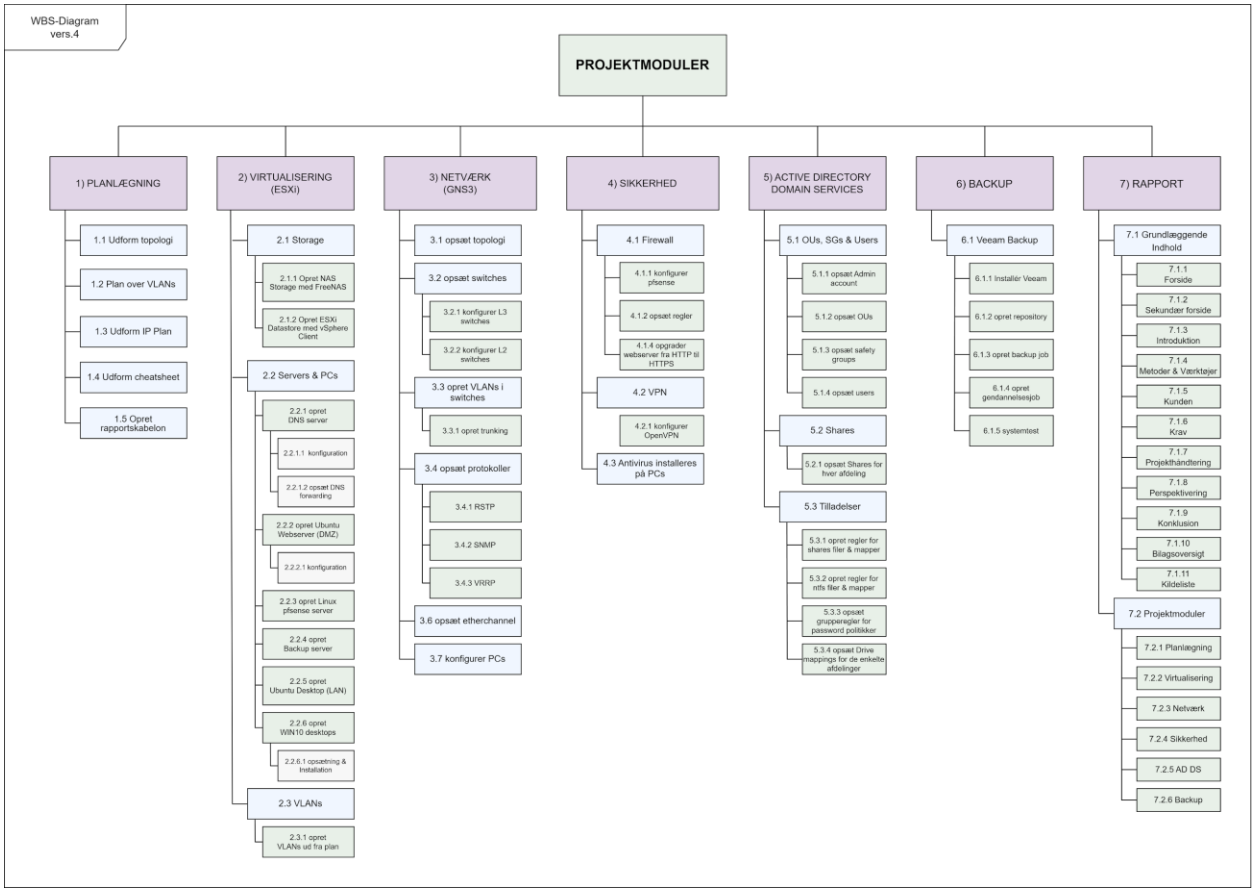
1. Planlægning
    a. Udformning af topologi, VLANs, IPs og cheatsheet
2. Virtualisering (ESXi)
    a. Virtualisering af VLANs, servere & PC's
    b. Oprettelse af Storage, NAS, ESXI
3. Netværk (GNS3)
    a. Opsætning af switches, protokoller og konfiguration

[12] Baseret på afsnittet "Vandfaldsmetoden", s. 32-33, "Udvikling af multimedier - en helhedsorienteret metode"

4. Sikkerhed:
    a. Konfiguration af Firewall, VPN og installation af antivirus
5. Active Directory Domain Service:
    a. Opsætning af AD DS/ OU's, users og sikkerhedsgrupper
    b. Opsætning af Shares
    c. Opsætning af tilladelser
6. Backup:
    a. Veeam
7. Rapport:
    a. Grundlæggende indhold og projekt-moduler

Som følge af uforudset sygdom hos begge gruppemedlemmer, blev det svært at følge vores tidsplan opsat i vores Gantt kortet i Click-up. Dette kan læses i Perspektivering.

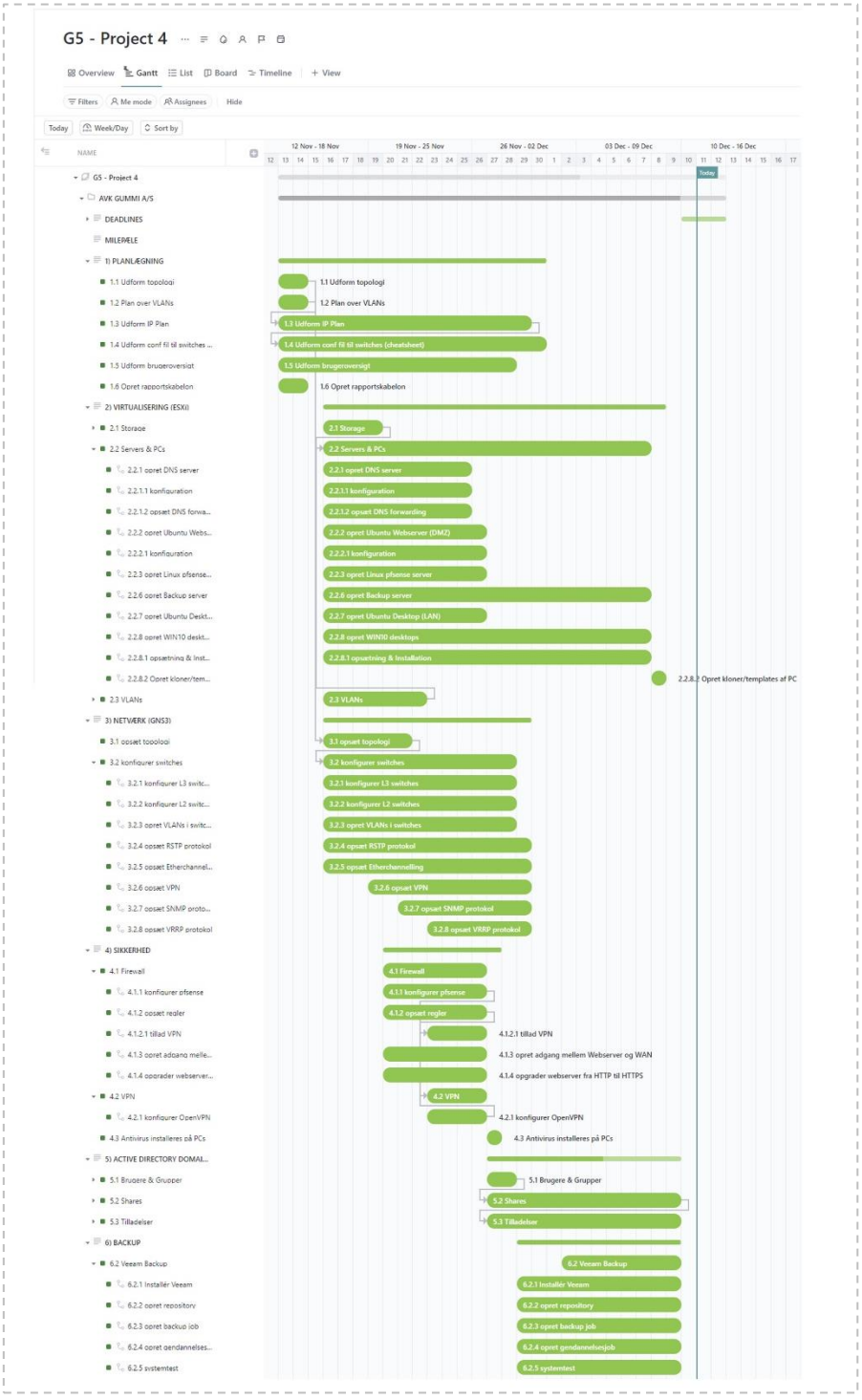
WBS-diagrammet findes i fuld størrelse i Bilag 2: WBS-diagram.



Billede 6.2.1: Bilag 2: WBS-Diagram

6.3 Gantt Chart

For at visualisere og planlægge projektets tidsplan blev også et Gantt-kort brugt. Gantt-kortet er et værktøj, der viser projektets tidsplan i form af en vandret tidslinje med opgaver og deres varighed. Dette giver os mulighed for at identificere afhængigheder mellem opgaver, estimere projektets varighed og planlægge ressourcerne effektivt. Findes i fuld størrelse i Bilag 3: Gantt-Chart.



Billede 6.3.1: Gantt-Chart fra Click-up, Bilag 3: Gant-Chart

7. Perspektivering

Til at starte med har vi udarbejdet dette projekt som en tomandsgruppe, så den almindelige arbejdsproces og uddelegering af arbejdsopgaver, sad vi fælles om. Derfor har vi arbejdet sammen om næsten alt i netværksarbejdet, dog var det nemmere for os at uddelegere rapportskrivning.

Selve gruppedannelsen fungerede rigtig godt og der var et positivt, dynamisk og sundt arbejdsforhold imellem os. Vi var gode til at supplere hinanden, hvor vi hver var svagest og vi var rummelige over for hinandens udfordringer i privatlivet, som kunne besværliggøre arbejdsprocessen. Der har under hele processen været en positiv og god kommunikation, hvor vi hele tiden vidste, hvor i processen vi var.

Vi kom næsten fra start bagud i vores projekt, da vi på skift lå syge sammenlagt i en uge. Så en tomandsgruppe, der arbejdede på halvt blus, forårsagede en større forsinkelse, som vi siden har arbejdet hårdt på at indhente. Senest sad Chanett kun tre dage før deadline for aflevering af projekt og opsatte en ny Domain-server og fik oprettet hele Active Directory-delen og Backup-funktionaliteten over to sene aftener. Vi har givet alt, hvad vi kunne i projektet og er tilfredse med det vi har opnået.

Helt teknisk oplevede vi udfordringer i at omstrukturere vores GNS3 projekt til at passe til vores case. Det var en del af øvelsen, men det skabte lidt forvirring. Dog kan det udledes af test afsnittene, at vi har opnået den ønskede funktionalitet. Den største udfordring var, da vi i den oprindeligt opstillede Domain server ændrede dens IP adresse og skiftede fra VLAN Device til VLAN LAN. Dette skabte problemer med certifikater, og vi var nødsaget til at oprette en ny domain server. Med den efterfølgende server oplevede vi også problemer, idet der ved en fejl var overset nogle steps i konfigurationen af AD DS, hvor netop denne del var vigtig at opsætte i slavisk kronologisk rækkefølge - så Shares-delen kom aldrig til at virke. Ligeledes kunne det tage op mod 20 minutter at skifte mellem brugere på en PC og ligeledes var det ikke muligt at tilføje alle domæne medlemmer til domænet. Underviseren proklamerede at dette skyldtes en domain server, der ikke fungerede. Vi var enige om, at eftersom projektrapporten havde større prioritet, ville vi kigge på AD DS og Backup senere, hvis der var tid. Vi havde ønske om også at opsætte Zabbix jf. de opstillede krav i afsnit 4. Krav, men det nåede vi ikke.

Set tilbage er vi tilfredse med vores indsats som en tomandsgruppe, der samtidig blev ramt af corona. Men havde vi haft tid, ville vi gerne have haft VLAN på virtuelle maskiner til at køre lidt

bedre. Shares, tilladelser og backup kom op at køre, men det var på bekostning af, at PC4 stadigvæk befandt sig på VLAN LAN og ikke VLAN Office og samtidig har en IP-adresse der hedder 10.130.51.133, som ellers burde være 10.130.53.133 jf. Bilag 5: IP Plan. Ved at skifte IP-adresse og VLAN mistede PC'en sin internetopkobling - så der er noget her, der skulle kigges nærmere på. Ligeledes ville vi gerne have kigget nærmere på at opdele IP-adresser i ranges for hver af vores VLANs i GNS3 projektet, men det fik vi heller ikke at se nærmere på. Ligeledes kan vores Cheatsheet og IP Plan virke en smule uoverskueligt, hvilket skyldtes forvirringen i omstruktureringen af GNS3 og samtidig at vi har prioriteret vores tid på andre dele af projektet. Slutteligt kunne vi godt have ønsket os at opsætte group policies, så der kunne opsættes en stærk fælles passwordpolitik samt en regel for centralisering af computere, så fremtidige installationer af computere har præcis den samme software, for eksempelvis AVG antivirus fælles for alle PC'er.

8. Konklusion

Efter gennemførelsen af projektet er der skabt en redundant it-infrastruktur. Dette opnås gennem anvendelse af RAID-1 storage og teknologier som etherchannel, RSTP og VRRP i netværksprojektet. Samtidig sikres fleksibilitet via et virtuelt miljø, hvor snapshots, kloner og skabeloner muliggør en nem implementering af nye enheder eller genoprettelse af fejlede enheder.

Projektet inkluderer også opsætningen af en firewall, der tillader trafik mellem forskellige områder som LAN ► WAN, DMZ ► WAN, LAN ► LAN og WAN ► DMZ.

Inden for firewallen er der implementeret specifikke regler for SNMP, Backup og VPN-adgang. VLANs med trunking er blevet oprettet for at muliggøre kommunikation mellem forskellige afdelinger eller VLANs.

Et velfungerende domænenetværk er etableret med organisatoriske enheder, sikkerhedsgrupper, administratorer og brugere. Dette muliggør deling af filer mellem virksomhedens afdelinger. Brugertilladelser er blevet opsat omhyggeligt, hvilket sikrer, at afdelinger og brugere kun kan tilgå de filer og mapper, der er tildelt dem.

For at sikre fjernadgang er der implementeret en VPN-forbindelse, så medarbejdere kan tilgå virksomhedens netværk fra deres hjemmeadresser. Der er også blevet oprettet SNMP for at muliggøre monitorering af statiske data for netværksenheder, hvilket kan tilgås fra eksempelvis en MIB-browser. Et funktionelt backupsystem og antivirus er blevet implementeret på PC'erne. Dog konkluderes det, at visse krav ikke er opfyldt. Dette inkluderer evnen til at overvåge vitale områder i it-infrastrukturen, som oprindeligt var tiltænkt med Zabbix. Der er heller ikke etableret en robust fælles password-politik gennem Group Policies, og der mangler implementering af Cloud backup.

Vi kan konkludere, at vi til løsningen af projektet har benyttet os af den viden, som vi har tilegnet os på alle tre semestre. Som en del af planlægningsarbejdet har vi arbejdet målrettet med WBS og Gantt, hvor vi kan konkludere at vi grundet sygdom kom bagud med vores deadlines. Vores fremgang og resultater er blevet dokumenteret løbende med brug af screenshots og logbog. I forhold til selve gruppearbejdet kan det konkluderes, at vi har haft en velfungerende gruppe, der har været præget af en positiv og støttende gruppekultur. Der har været stor rummelighed og personlighederne har matchet hinanden godt. Det har været et godt forløb og vi har været tilfredse med den indsats vi har ydet, i forhold til de udfordringer vi har stødt på under arbejdet.

9. Bilagsoversigt

Dette er en oversigt over de samlede bilag tilhørende Project 4.

Bilagsnr.	Navn	Filtype
Bilag 1:	Trusselsoversigt (mindmap)	PDF
Bilag 2:	WBS-diagram	PDF
Bilag 3:	Gantt-Chart	PDF
Bilag 4:	Topologidesign	PDF
Bilag 5:	IP-Plan	PDF
Bilag 6:	Cheatsheet	txt
Bilag 7:	GNS3 Topologi	PDF
Bilag 8:	Conf fil, SW1-IT-L3	txt
Bilag 9:	Conf fil, SW2-Production-L2	txt
Bilag 10:	Conf fil, SW3-Production-L3	txt
Bilag 11:	Conf fil, SW4-Office-L2	txt
Bilag 12:	Project4_GNS3	gns3project
Bilag 13:	Logbog	PDF

10. Kildeliste

Bøger

"CCNA 200-301, Official Cert Guide, Volume 1" af Wendel Odom ved forlaget Cisco Press, 2020

"CCNA Routing and Switching ICND2 200-105 Official Cert Guide" af Wendel Odom, Cisco Press, 2017.

"The Basics of Information Security" af Jason Andress, 1. Udgave, 2011, Forlaget Syngress

"Udvikling af multimedier - en helhedsorienteret metode" af Marie Christensen & Louise Harder Fischer, 2. udgave, 2. oplag 2006, Nyt Teknisk Forlag

Internetkilder

11-12-2023: "Spanning Tree BPDU Guard" af NetworkLessons.com
https://networklessons.com/spanning-tree/spanning-tree-bpduguard

11-12-2023: "5 benefits of virtualization" af IBM.com https://www.ibm.com/blog/5-benefits-of-virtualization/

11-12-2023: "Install Ubuntu Server" af ubuntu.com https://ubuntu.com/tutorials/install-ubuntu-server#2-requirements

11-12-2023: "System Requirements for Ubuntu Desktop" af help.ubuntu.com
https://help.ubuntu.com/community/Installation/SystemRequirements

11-12-2023: "Ultimate guide to VPN tunneling" af vpnmentor.com
https://www.vpnmentor.com/blog/ultimate-guide-to-vpn-tunneling/

11-12-2023: "Delegating administration of OU's"
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/delegating-administration-of-account-ous-and-resource-ous

11-12-2023: "Active directory security groups"
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#what-is-a-security-group-in-active-directory