Dansk Vinimport A/S

Arbejdsdokumentation fra Rasmus og Lilly.

Indledning

Dette dokument dækker over arbejdet udført i månederne december og januar af Rasmus Hende Svenson og Lilly Fredberg Andersen på vejne af Dansk Vinimport A/S.

Arbejdet bestod af opsættelse af et lokalt netværk, baseret på en Windows Server 2019 instans, som kunne understøtte netværkslogin fra flere forskellige computere. Derudover skulle der med dette netværk fremstilles et program der kunne hjælpe personalet med at holde styr på varebeholdningen, via en storskærm i kontoret.

Indholdsfortegnelse

Overblik

Vores tidsplan blev overholdt på den måde at vi blev færdige til den aftalte tid. I dette afsnit vil der være et kort overblik over hvad de afregnede arbejdstimer blev anvendt på.

Planlægning

Planlægning tog kun en enkelt arbejdsdag i alt, med møder med kunden osv.

Opsætning

Denne fase tog betydeligt længere end forventet, hele 3 arbejdsdage, på grund af det enormt upålidelige teknik der blev overrakt til os. På Dansk Vinimport's anvisning, anvendte vi den teknik som de havde anskaffet sig brugt, og vi kan nu efter at arbejdet er udført dokumentere at de ekstra arbejdstimer vi anvendte på at få disse til at samarbejde gør at vores forslag om at købe nye, men billige, maskiner, ville have givet en mindre regning.

9 ud af 10 maskiner givet til os var dysfunktionelle, og dette gav et enormt tidsspild.

Vi håber at denne erfaring vil tages i betragning i fremtiden.

I slutningen af d. 19 december havde vi alt grundopsætning gennemført, en dag længere end forventet.

Netværk

Som det blev anvist, så er netværket designet til at være let skalerbart. Vi har i dette formål ikke gået på kompromis med sikkerhed, og har sat jeres indtil videre eneste router op med to virtuelle lokale netværk (VLAN). Den ene kan i forbinde til via ethernet stikkene installeret i jeres bygning, og er et *internt* netværk. Jeres delte firmamapper osv., deles fra serveren via dette VLAN.

Det andet er tilkoplet det trådløse netværk, og går direkte til internettet, med ingen kopling til serveren. Dette betyder at eventuelle gæster ikke kommer til at påvirke jeres netværkssikkerhed overhovedet.

Det interne VLAN netværk er sat op med en subnet maske der gør den i stand til at holde på i alt 30 klienter på samme tid. Wi-Fi netværket har også en rækkevidde på i alt 30 brugere, men har derudover også en meget kort DHCP lease timer, således at den ikke opbruges på en dag med mange gæster.

Selveste opsætningen gik ganske som planlagt, og faktisk fik vi indhentet en masse tid da meget af arbejdet kunne udføres sideløbende med andre trin.

Router

Netværket kører over en Cisco 800 Series router. Da det ikke blev bedt om, kommer denne *uden* Cisco's web-baserede konfigurationsværktøj. I denne sektion vil vi kort dække over hvordan man eventuelt kan udvide netværket skulle det være nødvendigt.

Som nævnt er netværket lige nu opdelt i 2 VLANer, disse kan ses ved at tilgå Cisco konsollen, og ved at træde ind i **executive** tilstand, og ved at benytte sig af kommandoen **show ip interface brief**.

```
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0              unassigned      YES unset  up                    up
FastEthernet1              unassigned      YES unset  up                    down
FastEthernet2              unassigned      YES unset  up                    down
FastEthernet3              unassigned      YES unset  up                    down
FastEthernet4              unassigned      YES NVRAM  administratively down down
Vlan1                      10.10.10.1      YES NVRAM  up                    up
Vlan10                     192.168.1.1     YES NVRAM  up                    up
Vlan20                     192.168.1.33    YES NVRAM  down                  down
Wlan-GigabitEthernet0      unassigned      YES unset  up                    up
wlan-ap0                   10.10.10.1      YES TFTP   up                    up
```

Figur 1: Interfaceoversigten med de relevante VLANer synlige

Her kan resultatet af denne kommando ses. Bemærk at FastEthernet3 sædvanligvis ville være oppe, men dette skærmbillede blev taget imens kun serveren var tændt.

VLAN10 er det **interne** netværk. **VLAN20** er et **BYOD** (Bring Your Own Device) netværk.

De to benyttede kabeludgange, som begge benytter **VLAN10,** er **FastEthernet0** til **serveren** og **FastEthernet3** til switchen til kontoret. **VLAN20** er tildelt **Wlan-GigabitEthernet0**, som er det trådløse netværk.

Er det nødvendigt at forbinde flere switches til routeren, kan disse tilføjes til VLAN netværket via følgende kommandoer inde i **global configuration mode** (*config t*), her med Ethernet1 som eksempel:

interface FastEthernet1 og så **switchport access vlan 10**.

Udvidelse af netværket fra routerens side

Siden det subnet der er opsat kun rummer 30 klienter, kan det være at i en dag gerne vil udvide denne. Dette er heldigvis en simpel process, men kræver at i gennemfører nogle trin på både routeren og jeres server.

Det første trin i denne process er at udvide VLAN10 netværket. Det er vigtigt at bemærke at det ikke er praktisk uden større infrastrukturændringer at tilføje flere VLAN netværk, da serveren kun kan tilgås gennem VLAN10. Ændringer til dette vil nødvendiggøre endnu større infrasturkturændringer, da serveren i sin nuværende konfiguration **ikke** kan differentiere imellem DHCP anmodninger fra forskellige VLAN'er, og DHCP tildelingen vil derfor give en fejl.

For ordentligt at kunne håndtere flere VLAN'er til den samme server, skal serveren kunne have flere netværkskort for at kunne differentiere imellem trafik fra det ene eller andet VLAN. Dette undgås i BYOD netværket ved at lade Cisco routeren håndtere DHCP i stedet, hvorved serveren ikke behøves at blive involveret.

Men det nuværende VLAN kan let udvides fra **global configuration mode**, via kommandoen **interface VLAN10**. Herfra kan du, for eksempel, udvide netværket til 250 klienter via tildelinengen af et større subnetwork. Dette gennemføres via kommandoen **ip address 192.168.1.1 255.255.255.0**. Hermed ændres subnet masken til at rumme 254 klienter.

Om nødvendigt kan netværket gøres endnu større, men vi anbefaler her at man her begynder at overveje om ens infrastruktur skal ændres på flere måder.

Udvidelse af netværket fra serverens side

For at serveren fortsat kan fungere ordentligt efter at adresse rækkevidden justeres, skal **DHCP** og den **statiske IP konfiguration** justeres.

Dette **kan** undgås ved at fastholde serverens gamle IP adresse, men det **kan ikke anbefales**. Som udgangspunkt burde routerens IP fastholdes som den første IP adresse indenfor rækkevidden, og serverens IP fastholdes som den anden. Dette er af standardiseringsårsager.

Ændring af serverens statiske IP-adresse kan medføre uventede bivirkninger. Vi anbefaler derfor at man udfører disse ændringer i en ferie, hvor der er rigelig med tid til at rette op på disse eventuelle problemer. Problemerne skyldes mange ting, og nogle af dem kan springes over.

Klienternes DHCP-Lease

En af de problemer der kan forudses og springes over er at klienterne efter IP ændringen stadig vil have gamle værdier sat til deres DNS samt standard gateway. Dette kan let løses ved at tvinge klienten til at nulstille dens netværkskonfiguraiton.

Dette kan let gøres fra kommandolinjen via kommandoerne **ipconfig /release** efterfulgt af **ipconfig /renew**.

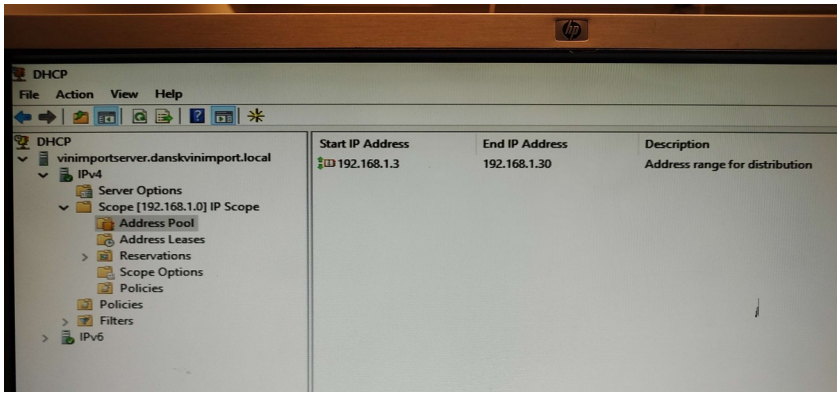
DNS tjenesten

Windows Server 2019 **burde** automatisk konfigurere sin DNS tjeneste til at passe til dens nye IP adresse. Hvis DNS tjenesten ikke fungerer som forventet, så kontroller at dette er blevet udført korrekt, da fejl kan forekomme.

DHCP rækkevidden

Det er vigtigt at man husker at justere selveste DHCP tjeneste på serveren. Hvis du har udvidet adressemængden på routeren, skal DHCP rækkevidden afspejle dette. Dette kan gøres inde fra DHCP kontrolpanelet, og er en relativ simpel proces.

På billedet ovenfor kan DHCP tjeneste observeres. Inde i ”Address Pool” kan rækkevidden justeres. Husk at fornye de nuværende leases på klienterne efter en ændring herinde.

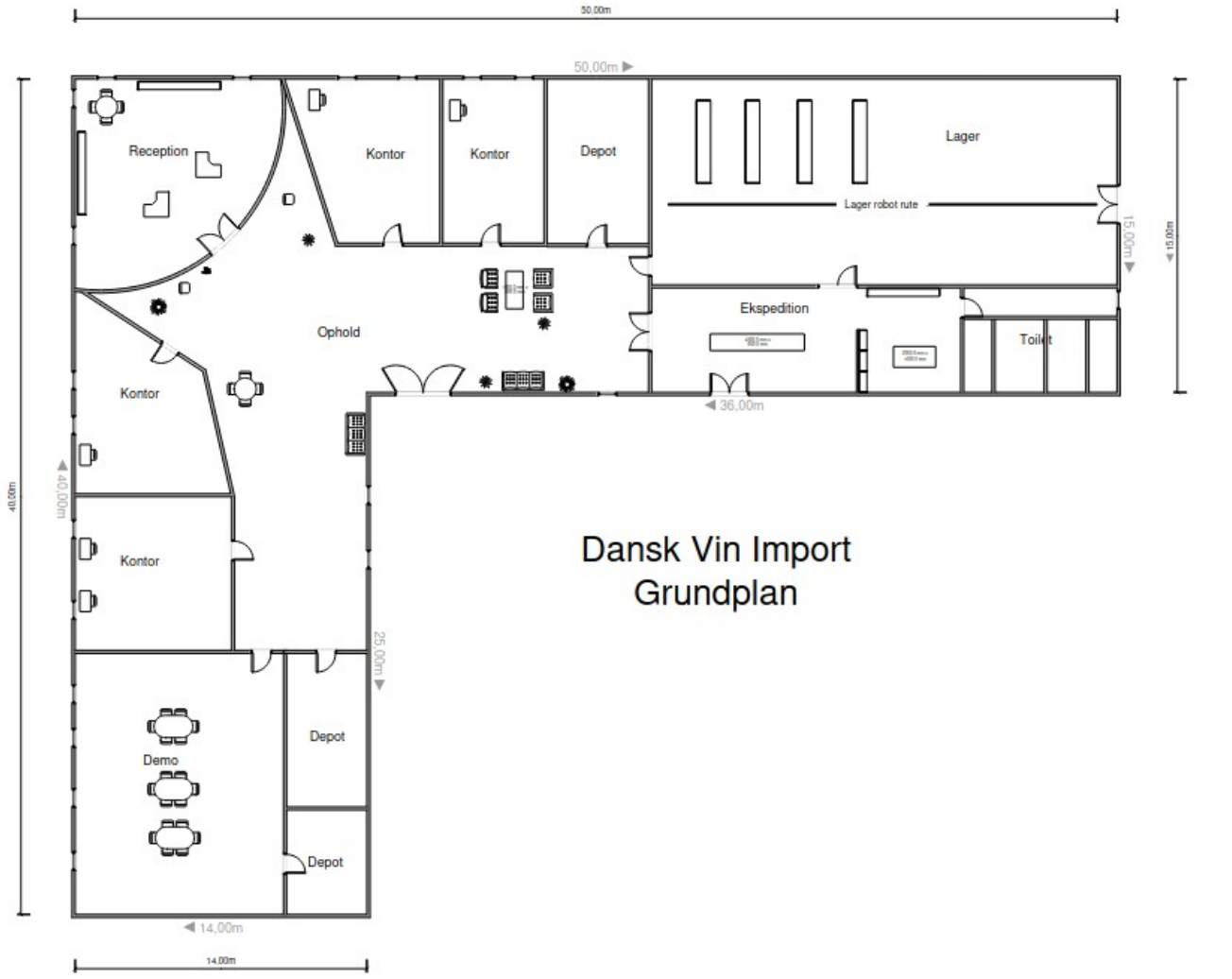


Figur 2: DHCP tjenesten med den nuværende konfiguration synlig

Fysisk Opsætning

På nuværende tidspunkt er netværket **ikke** aktiveret, og det er der flere grunde til. Serveren og routeren er begge to i et rulleskab som let kan flyttes ind hvor det skal være, hvorfra det hele kan tændes sammen. Der er som sådan ikke noget problem her.

Problemer opstår i jeres kontors opbygning.



Figur 3: Bygningsplanen til jeres kontor

Det sikreste, og mindst forstyrrende, sted at anbringe dette skab ville være depotet vest for lageret. Vi antager at dette lokale ville være svagt trafikeret, da det ikke har nogen gennemgangsmuligheder og bruges til opbevaring. Dette har to fordele:

Sikkerhedsfordelen: Oftere lukket dør

Et mindre trafikkeret lokale er oftere aflåst, og låses sjældent op. Dette mindsker chancen for at døren glemmes at låses, og mindre chance for at forbipasserende ser serverkassen ved et tilfælde.

Servereskabet er godt nok låst af, men det er bare et almindeligt aluminiumsskab, og kan ødelægges uden meget værktøj. Direkte adgang til routeren og serveren introducerer enorm stor risiko, også selvom begge dele er låst bag ved kodeord.

Komfortfordelen: Ikke en arbejdsplads

Et serverskab bliver varmt. Jo større jeres virksomhed, og jo mere i laver, jo varmere bliver den. Desuden så har vi indstillet den forsynede computer som serveren kører på til ikke at tage hensyn til støj; altså kører blæseren på fuld smæk næsten hele tiden. Dette øger ydeevnen ved at forhindre al 'throttling' af hardwaren, og sænker chancen for at komponenterne tager skade igennem langtids døgnbrug.

Dette betyder at anbringelse i et kontor eller lignende ville være ubehageligt.

Routeren og serveren kunne i denne forbindelse adskilles, men af administrative årsager er det meget praktisk at have de to tæt på hinanden.

Ulempen: Dækning

Den store ulempe ved placeringen her er selvfølgelig at den ikke er central. Det betyder at i, med denne ene router, vil opleve svag dækning fra det trådløse netværk i de sydvestlige mødelokaler. Vi antog dog at dette ikke ville være et stort problem, da alt personale er koblet til netværket igennem kabelforbindelser.

Skulle Wi-Fi dækning ønskes i mødelokalerne, kan dette let ordnes med en ekstra trådløs router i lokalet, forbundet med kabel. Dette ville næppe være dyrt, og ville være meget sikrere end at flytte selveste routeren ud i receptionen.

Brugeropsætning

Sikkerhedsadvarsel

Af sikkerhedsmæssige bekymringer der kommer med at give eksterne konsulter adgang til serveren, er brugerettighederne meget nøje sat op. Som udgangspunkt har folk på domænet ingen rettigheder, og kan ikke tilgå noget som helst på serveren andet end DHCP og DNS.

Under normale omstændigheder ville vi anbefale at køre konsulterne igennem det samme BYOD netværk som gæsterne, altså igennem Wi-Fi netværket. Men da det var ønsket at de kom på domænet, er dette ønske blevet opfyldt på så sikker vis som muligt.

Vi vil her **kraftigt** anbefale at sikkerheden af jeres server ikke påvirkes yderligere. **Giv ikke eksternt personale** adgang til firmafiler eller andet på serveren end hvad vi har sat op. Oven i den allerede usikre situation som i har bedt om, har i også forsynet både gammelt hardware og licens til en forældet Windows Server udgave (2019).

Husk derfor at der med alderen på proprietært software følger en **eksponentielt øget risiko** for at der opdages loophuller og sikkerhedssvagheder. Disse sikkerhedssvagheder bliver lettere at udnytte jo længere inde i systemmet den kriminelle allerede er, så jo mindre i giver, jo sikrere er i.

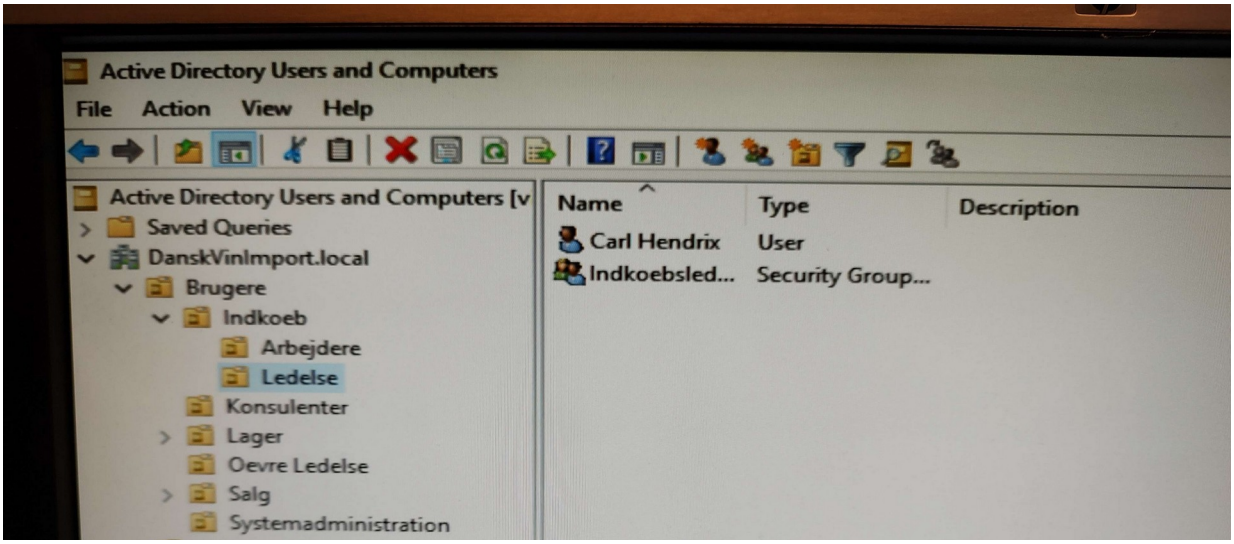
Allerede at konsulterne har printeradgang giver dem en indgangsvinkel til serveren, og vi vil derfor **kraftigt** anbefale at dette genovervejes, eller at det håndteres igennem en anden tjeneste, såsom en webportal der kan scanne de sendte dokumenter først inden print. Dette skyldes at der i Windows operativsystemet **hyppigt** forekommer sikkerhedssvagheder i forbindelse med den mindste slags adgang til serveren. Svagheder såsom CVE-2018-8626 krævede ikke andet end en DNS forespørgsel, og svagheder som CVE-2018-0802 krævede intet andet end at dokumentet håndteres af Office-pakken.

Brugerplan

Vores opsætning er derfor sat op med sikkerhed som prioritet, men uden at ofre administratorens tid alt for meget. Alle personalegrupper har en tilsvarende brugergruppe i domænet, som man så kan tildele forskellige rettigheder for at inkludere alle i gruppen. Disse grupper kan let placeres i deres egne grupper også.

Brugergruppernes opsætning passede godt ind i vores tidsplan.

På nuværende tidspunkt indeholder disse grupper hver især kun en enkelt bruger, men alt på serveren er sat op med disse grupper, inklusivt fællesmapperne. Dette betyder at når der skal tilføjes nye ansatte til domænet, så skal de kun tilføjes til denne ene gruppe, frem for manuelt tilføjes til de enkelte mapper en af gangen.



Figur 4: Brugergruppekonfigurationen

Brugerne og deres grupper er let opdelt i undermapper inde under Active Directory, og burde være lige til at gå til. Grupperne er tildelt således at alle ansatte er del af 'Ansatte' gruppen, så ønskes der at alle ansatte har adgang til noget, skal det blot tildeles denne gruppe. Konsulenter er **ikke** del af denne gruppering, og har i stedet deres egen, separate gruppe.

Ønskes en ny bruger, så tilføjes de blot i den passende undermappe og tilføjes bagefter til den passende gruppe inde i undermappen. Dette vil automatisk give dem adgang til de relevante netværksmapper, **med en undtagelse**.

Den private netværksmappe skal manuelt oprettes på nuværende tidspunkt. Dette er heldigvis en simpel proces.

De forudinstillede mapper er: Salg, Regnskab, Lager og Faelles. De er tildelt de rettigheder som er angivet i ordren.

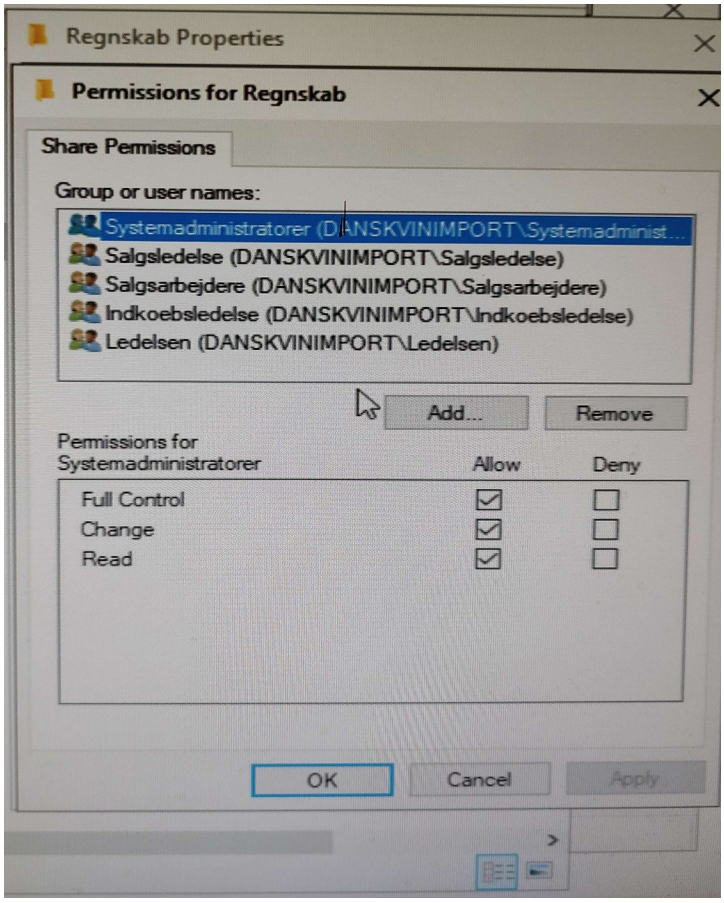
Alle brugere er sat op med en minimum password længde på 7 tegn, samt et kompleksitetskrav. Vi følte at dette var et nogenlunde kompromis imellem praktikalitet og sikkerhed, men dette kan let konfigueres i domain policies. Ændre policy'en for 'Ansatte' gruppen for at gøre dette på tværs af firmaet.

Netværksmappeopsætning

Netværksmapperne som er forudindstillet inkluderer også en privat mappe til hver enkelt ansat. Disse kan findes på serveren under Dokumenter\PrivatNetwork. Bemærk at mappen her er lidt særligt indtillet, da den benytter **Access-Based Enumeration**. I praksis betyder dette at kun den relevante bruger kan se de mapper de kan tilgå, ingen anden. Dette gør mappen lettere at overskue fra **klientens synspunkt**.

En ny mappe der oprettes her burde følge følgende standarder:

- Brugerens brugernavn som mappenavn
- Ingen delingsindstillinger, disse arves fra hovedmappen
- Sikkerhedsindstillinger der giver den relevante bruger, og kun den relevante bruger, read og write tilladelse.



Figur 5: Her kan sikkerhedsindstillingerne på en af de delte mapper observeres, men processen er den samme for de private.

Hvis skridtene følges ordentligt, vil der oprettes en undermappe i PrivatNetworks, som kun kan ses og tilgås af brugeren og administratoren.

Overvågningsprogram

Som angivet, er der sammen med opsætningsarbejdet blevet udviklet et program til at samarbejde med Dansk Vinimport's indkøbte overvågningsløsning, som kan anvendes på storskærme til let at give et overblik over status af lager og salg.

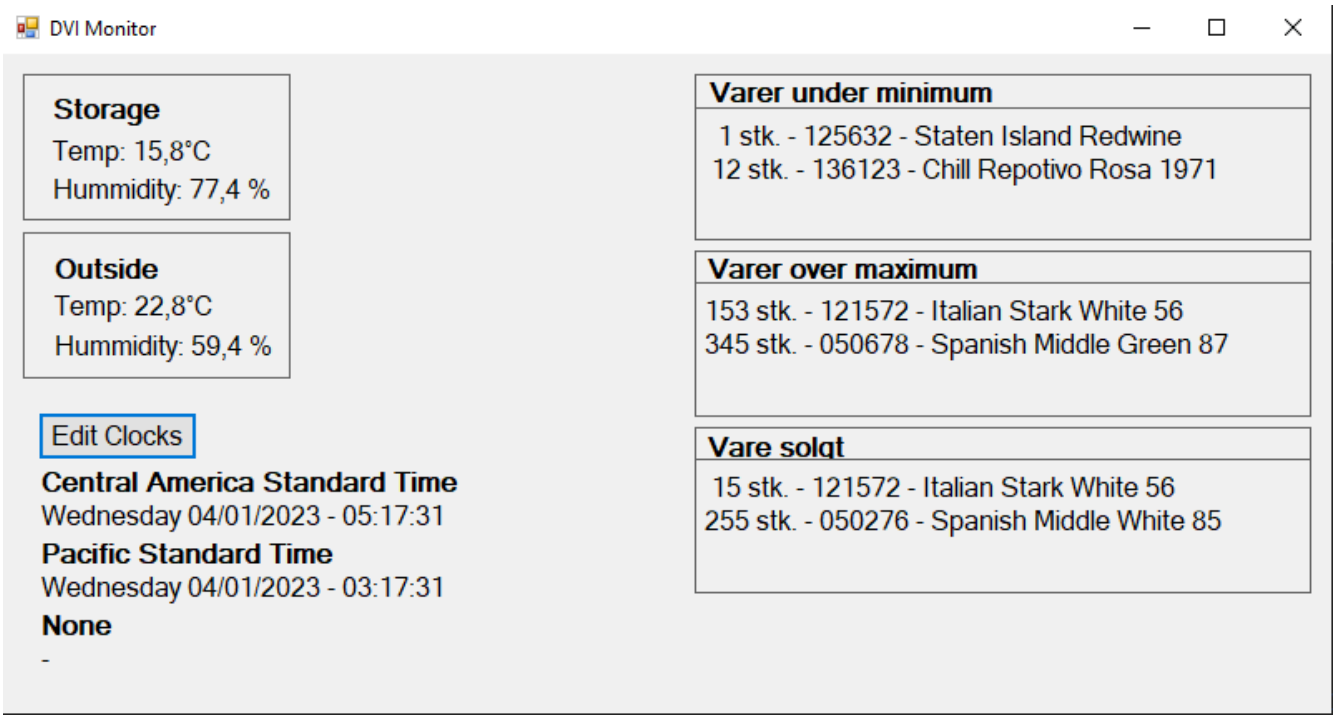
Som del af aftalen afleverer vi også den originale kode til dette, så det kan ændres og videreudvikles i fremtiden.

Programmet er skrevet i C# og benytter proprietære kodebiblioteker fra Microsoft, hovedsageligt .NET igennem Windows Forms, så bemærk at programmet *ikke* vil køre som planlagt på andre operativsystemer. Dette skyldes den metode hvorved jeres eksterne overvågningsløsning afleverer dataen som den opsamler. Denne data gør det betydeligt lettere at behandle det med C#.

Skulle det nogensinde ønskes at migrere til andre operativsystemer, burde dette ændres.

Specifikationer

Programmet har følgende funktioner, alle som angivet af kravene givet af Dansk Vinimport.



Figur 6: DVI monitoren i dens nuværende konfiguration

Temperatur og luftfugtighed, tidsindikationer fra flere tidszoner, samt lageroplysninger.

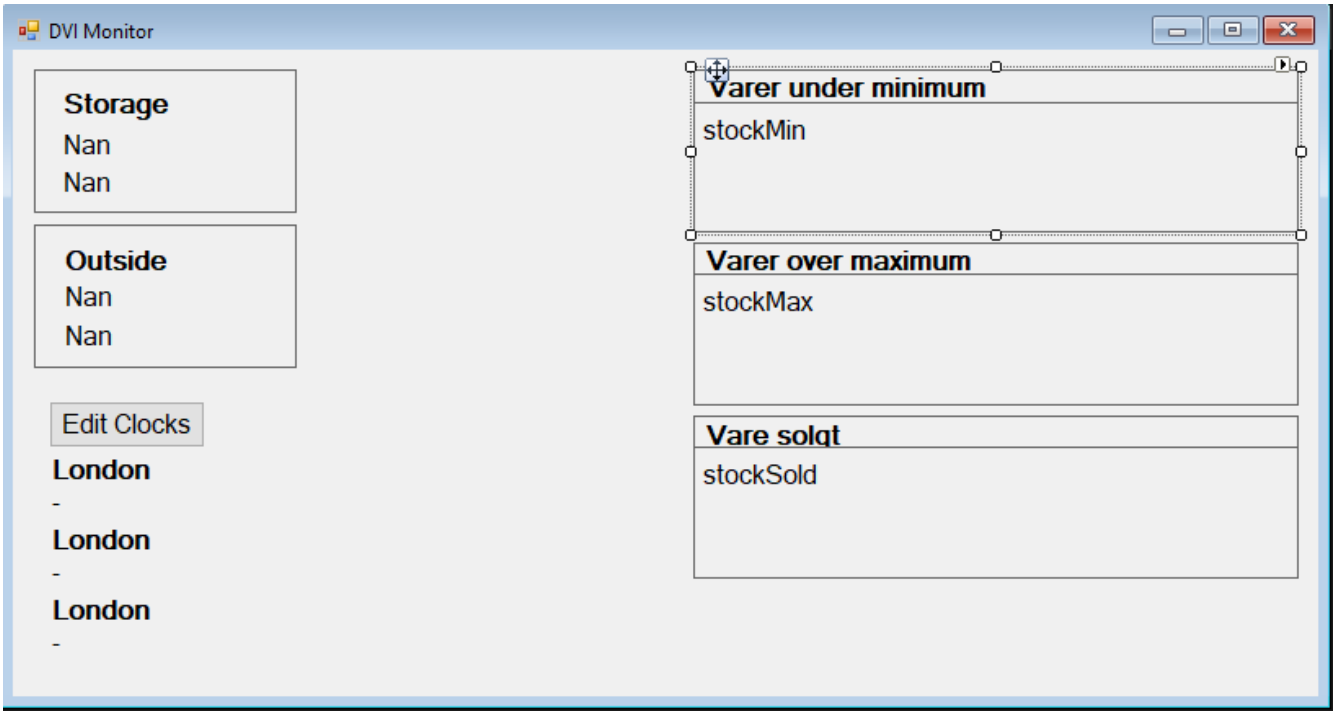
Design

Som nævnt er programmet designet i Windows Forms. Det er enormt gavnligt at være bekendt med dette hvis man vil arbejde på koden i fremtiden. Noget af det vigtigste ved Windows Forms er at det er designet til at blive arbejdet med via Visual Studio. Ikke Visual Studio Code, men helst Visual Studio.

Der er tale om et Microsoft værktøj, og Microsoft vil helst have at man arbejde med det iggenem deres egne værktøjer.

Elementer kan dog herigennem let tilføjes, redigeres og/eller fjernes. Selvom opsætningen kan være lidt bøvlet, er denne løsning valgt da den kan udføres af folk som ikke er særlig kyndige i kode vha. nogle YouTube instrukser.

Da de forskellige dele af programmet er inddelt i paneler, kan man nemt ændre layoutet uden at skulle fumle rundt med individuelle tekst komponenter.

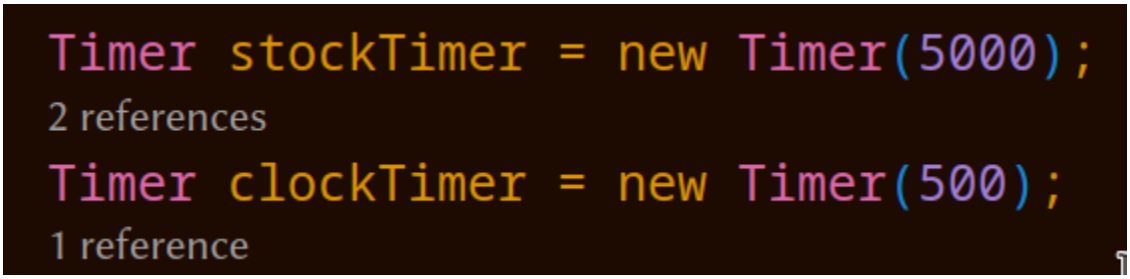


Figur 7: Overvågelsesprogrammet med opdateret udseende, i deaktiveret tilstand

Kode

Hvis man vil lave hurtige ændringer, er dette lettest at gøre igennem DVI_Monitor.cs, som indeholder mange af mekanismerne bag ved facaden.

Vigtigst af alt så indeholder den tidsindstillingerne for hvor regelmæssigt informationerne fra tredjepartsprogrammet skal opdateres. Fra vores side af er dette sat til 5000 ms til lageret, og 500 ms til urene. Dette kan let ændres for at spare på processorkraften igennem objekterne stockTimer og clockTimer.



Figur 8: Kildeteksten ansvarlig for opdateringsfrekvensen

Når timerne udløber, udløser det hver sin metode, som er ansvarlig for at opdatere de relevante værdier. Værdierne eksisterer i Windows Forms koden, som er autogeneret. Denne kan findes i projektmappen også, men det anbefales ikke at røre den manuelt.