

Svendeprøveprojekt: GREEN CLASS



Mads B., Palle, Christian Nyhuus og Simon
Svendeprøvehold - IT supporter
Lærer: Bo Larsen

Indholdsfortegnelse

Indledning	4
Netværk	6
Netværkstekning	8
Switch'ne	9
SW1C.....	9
SW1D og SW2D.....	9
SW1A og SW2A.....	9
VLAN	10
VTP.....	10
Operativ Systemer	11
DC01	11
AD	11
DNS	14
DHCP	14
ISA01.....	15
Netværk	15
Firewall	16
FS01	18
WSUS	21
WUP01.....	22
ESX01	25
vCenter	26
Web01	27
Exchange.....	28
TSxx.....	29
TS01 + 02 (Front Ends).....	29

TSSB (Session Broker)	30
Serverdoc.....	32
Konklusion	33
Bilag	34
Bilag 1 – Netværkstegning.....	34
Bilag 2 – IP plan.....	35
Bilag 3 – Kabeloversigt.....	36
Bilag 4 – Opsætningsguide til Outlook 2007	37
Bilag 5 – Serverdoc for DC01	39
Bilag 6 – Serverdoc for ISA01.....	41
Bilag 7 – Serverdoc for FS01	43
Bilag 8 – Serverdoc for WUP01.....	45
Bilag 9 – Serverdoc for ESX01.....	47
Bilag 10 – Serverdoc for vCenter	48
Bilag 11 – Serverdoc for WEB01	50
Bilag 12 – Serverdoc for Exchange	52
Bilag 13 – Serverdoc for TS01.....	54
Bilag 14 – Serverdoc for TS02.....	56
Bilag 15 – Serverdoc for TSSB.....	58
Bilag 16 – Local administrator passwords	60

Indledning

Her til vores svendeproe projekt har vi som gruppe valgt, at projektet hertil skal handle om firmaet Green Class A/S. Vi vil lave en rapport der omhandler Green Class' IT struktur, som vi synes den skal se ud for, at firmaet får den bedste løsning i forhold til deres arbejdsdag. Vi vil gennemgå og beskrive vores forslag til et netværk, som vi mener, vil passe til dem. Vores forslag vil indeholde bl.a. switche, routning og firewall, derudover vil vi også gennemgå deres server setup. Her vil vi fortælle om hvilke roller de enkelte servere har og hvad vi har tænkt at formålet med dem er, i forhold til Green Class.

Green Class

Green Class A/S er en arkitekt- og indretningsvirksomhed som arbejder med at tegne og indrette fremtidens grønne hjem, som både er miljø venlige og energi besparende.

Firmaet består af en direktør, 4 bestyrelsesmedlemmer og 25 medarbejdere fordelt på 6 afdelinger.

Medarbejderne fordeler sig sådan over de 6 afdelinger;

- Administration og Økonomi, 3 medarbejdere
- Kundeservice, 3 medarbejdere
- Salg og Marketing, 4 medarbejdere
- Indretning, 6 medarbejdere
- Arkitekter, 5 medarbejdere
- IT-afdelingen, 4 medarbejdere

Krav fra Green Class

Green Class har selvfølgelig nogle krav til hvad deres løsning skal indeholde og kunne.

Kravene er som følger:

- De skal kunne sende og modtage mails både internt og eksternt, de har domænet greenclass.local. De sender og modtager mange mails, så det er en vigtig del af Green Class A/S.

- Hver medarbejder skal have en mailadresse, samt nogle fælles mailadresser. Green Class går meget op i at svare deres kunder personligt, men de har selvfølgelig fælles adresser såsom salg og info.
- De skal kunne dele filer og dokumenter, og disse filer skal også kunne tilgås uden for arbejdspladsen. F.eks. fra en hjemme pc eller en bærbar pc med internet forbindelse. Deres arkitekter og indrettere er ofte på farten, så dette er et vigtigt punkt.
- De skal have nogle websites – en hjemmeside, som skal bruges af deres kunder. Et intranet, som de selv skal bruge internt.
- Det er et vigtigt element at tingene fungerer stort set hele tiden, så evt. nede tid bliver minimal.

WWW.BLOGGT.DK

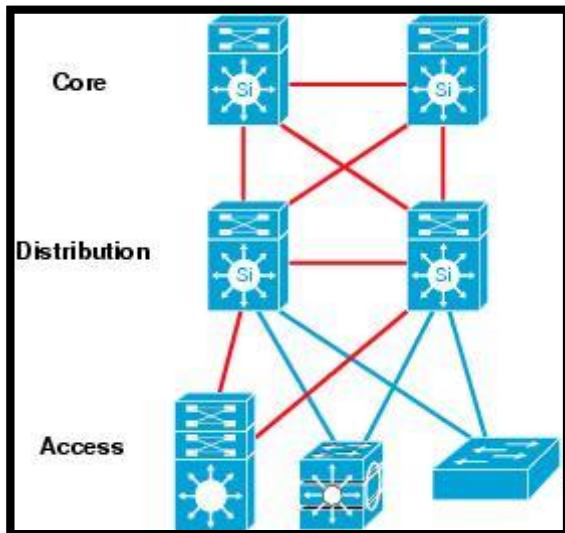
Netværk

Netværket generelt

Netværket er baseret ud fra Ciscos netværks model der består af 3 lag. Core, Distributions og Access.

Vi har dog på grund af mangel på udstyr været nødt til at lave vores egen model af denne.

Ciscos officielle model ser ud således:



Core laget

Core laget er også det man tit relatere til som backbone. Core laget håndterer som regel ikke andet end andre switche og routere. Dvs. enheder på core laget kun er forbundet med andre enheder på core- og distributions laget. På dette lag har vi ingen ACLs eller andet pakke filtrering. Her køre man også altid redundans for at stikkere high availability.

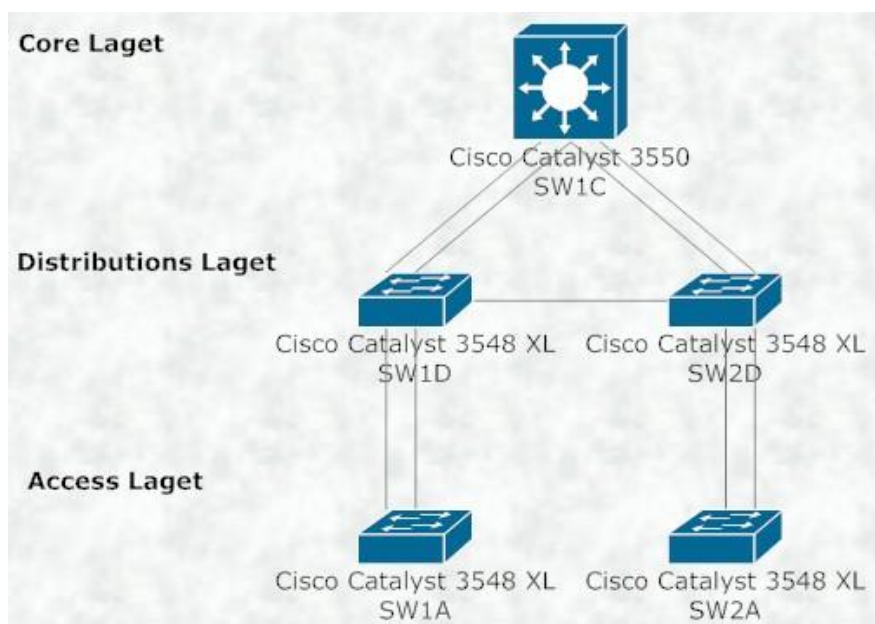
Distributionslaget

Det er fra dette lag at vi har kontakten med access laget, samt det er her vi laver sikkerheden med ACLs osv. Normalt bruger man ikke fiber mellem dette lag og access, samt fra dette lag og op til core laget.

Access laget

Her har vi laget der er helt ud til brugerne, det er her at klienterne bliver sluttet på netværket. Det forgår oftest via enten WLAN eller via Ethernet. Linket til distributions lager forgår typisk via fiber.

Green Class ser ud således:



Vi har i vores setup til Green Class brugt en Cisco Catalyst 3550, hvilket er en layer 3 switch. Denne fungerer ydermere også som router, da vi ikke havde mulighed for at få en router som understøtter router-on-a-stick. Dvs. at routeren skal kunne lave encapsulation med f.eks. dot1q (802.1q) af sub-interface.

Vi har også fire styks Cisco Catalyst 3548 som benyttes både i distributions og access laget.

Vi ville rigtig gerne have haft benyttet fiber switche til de 2 øverste lag, da dette giver en højre stabilitet.

Blandt andet fordi mediet fiber er hurtigere end Ethernet. Og f.eks. i tilfælde af lyn nedslag vil dette heller ikke blive ført videre igennem et fiber kabel, det vil det derimod i et Ethernet kabel.

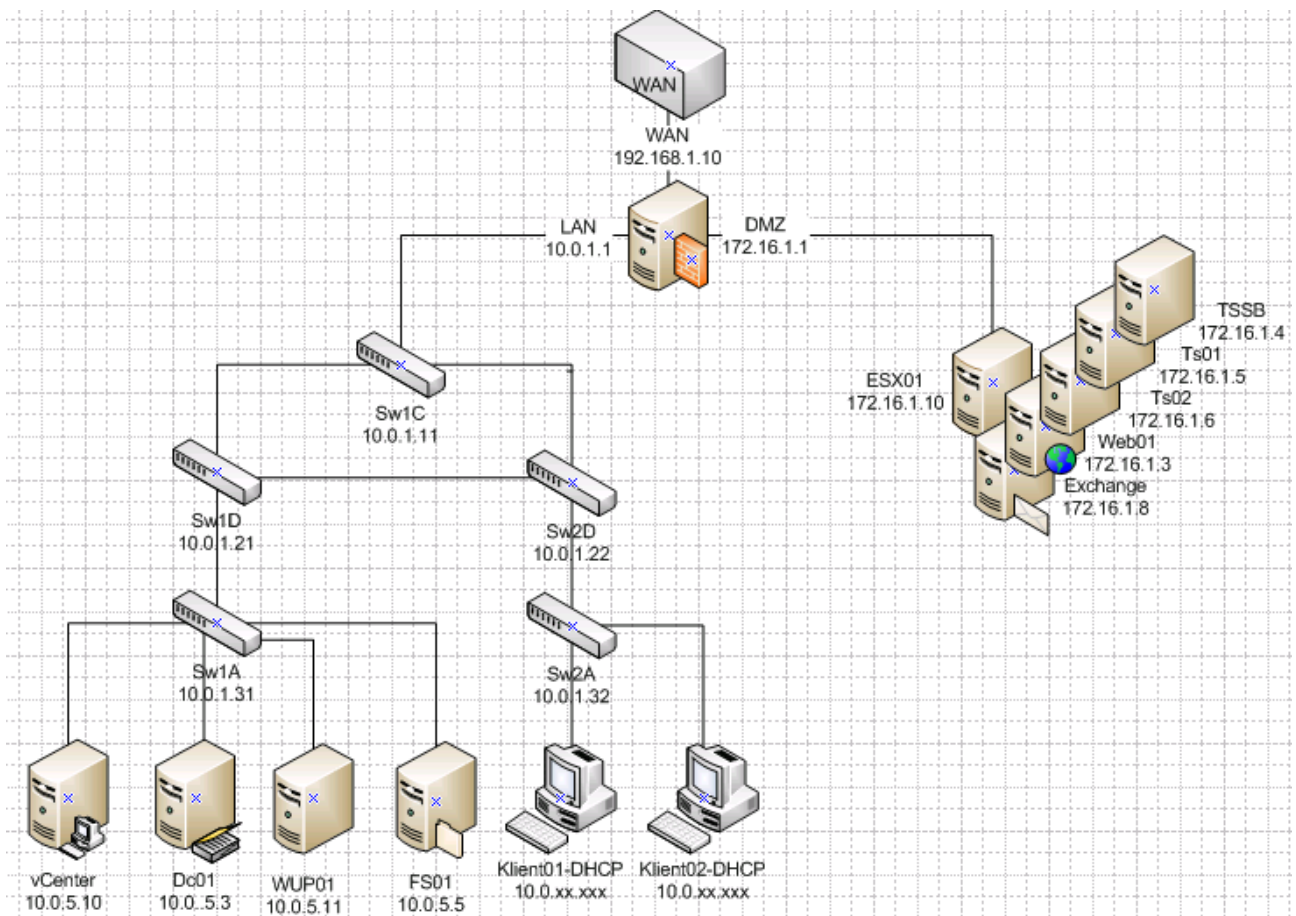
Vi har som backup løsning i stedet valg at vi mellem Core swithen køre et stacking kabel ned i SW1D og SW2D, fra SW1D går der endnu en stacking kabel ned i SW1A og fra SW2D ned i SW2A.

Disse steder er switch'ne dog også forbundet via et krydskabel. Dette har vi gjort for at skabe sikkerhed i vores netværk, hvilket vi har gjort ved hjælp af STP (Spanning Tree Protocol). Hvor vi har givet stacking portene (Gi 0/1 og Gi 0/2) en port prioritet på 16. Dette sikre at STP altid vil vælge denne route hvis den er oppe, da standard prioriteten er 32. Den bruger altid det laveste prioritet først, og falder så over på den prioritet i tilfælde af at den første ikke virker.

Vi har valgt at navngive vores switche på en måde så vi synes de er nemme at finde rundt i, i forhold til vores lag. Core switchen hedder SW1C for Switch 1 Core. Distribution 1 hedder SW1D, Access 1 hedder SW1A osv..

Denne navngivning giver os switch'ne: SW1C, SW1D, SW2D, SW1A og SW2A.

Netværkstegning



Switch'ne

SW1C

Dette er vores Core switch. Det er en Cisco Catalyst 3550 layer 3 switch, som vi også benytter som vores router.

Denne fungerer ydermere som VTP (Vlan Trunking Protocol) server, altså det er her fra vi styre hvilke VLAN's vi har på vores switche.

Den fungerer også som root for STP (Spanning Tree Protocol).

Vi har desuden sat port prioriteten på Gi 0/1 og Gi 0/2 til 16, for at være sikker på at hvis disse linjer er oppe, så skal det være dem som bliver benyttet i stedet for krydskablerne, da disse er Gigabit porte, hvor de andre 48 er 100mbit. Grunden til vi har sat dem til 16 er fordi værdien som standard er 32, og det er laveste prioritet først.

SW1D og SW2D

Disse to er distributions switche, dvs. de forbinder access laget med core laget. Det er begge Cisco Catalyst 3548 XL.

Disse er konfigureret som VTP klienter, dvs. de kan ikke oprette/ændre/slette VLAN's, det er kun vores VTP server der kan det.

SW1A og SW2A

Disse to er access switche, det er her vi kobler klienterne og serverne på. Det er begge Cisco Catalyst 3548 XL.

Vi har bestemt os for at benytte SW1A til serverne også vil vi benytte SW2A til klienter, her i blandt vores trådløse brugere.

Forbindelse til switch'ne

Der er sat telnet adgang op til alle 5 switche med kodeord på, via "line vty 0 15".

Trådløst

Vi har valgt at sætte et Access Point op, så vores netværk kan tilgås trådløst.

Vores access point er af mærket TrendNet, og benytter en retningsbestemt antenne for at give bedre signal i den retning hvor vi skal bruge det.

Opsætning af access point

Access pointet er navngivet GreenClassAP, og køre med et SSID der hedder Green Class.

Det har vi valgt at kryptere med WPA2-PSK. Fordi vi mener det er det sikreste at benytter pt.

Det køre på IEEE 802.11g, frekvens 2.4Ghz, samt vi benytter kanal 8.

VLAN

Vi har valgt at gøre brug af 10 VLAN's. Ud af disse 10 er 7 af dem til forskellige afdelinger, og de sidste 3 er til det native VLAN, altså her hvor vores switche fysik sidder på, samt ISA serveren. Derudover har vi et til serverne og et til de trådløse brugere. Disse VLAN's har nummerne 1, 5, 10, 11, 12, 13, 14, 15, 16 og 20.

Via DHCP får klienterne på afdeling VLAN'ne (10-16 og 20) automatisk en IP adresse, samt konfiguration af DNS- og WINS server samt default gateway.

De får en IP adresse der svare til det VLAN nummer de er på. IP adressen ser således ud 10.0.vlannummer.x

For eksempel sidder man i IT afdelingen er man på VLAN 10, her vil den første der går på få adressen 10.0.10.20. Sidder man i ledelsen vil man få 10.0.15.x.

VLAN Oversigt

Navn	Nummer	Beskrivelse
native	1	Routerne og Switche (management)
Servere	5	Servere
It	10	IT
AdmOko	11	Administration og Økonomi
SalgMark	12	Salg og Marketing
KundeService	13	KundeService
Arkitekter	14	Arkitekter
Ledelse	15	Ledelse
Indretning	16	Indretning
Wireless	20	Wireless connections

VTP

Vi har valgt at gøre brug af den geniale funktion Cisco switche har, nemlig VTP (VLAN Trunking Protocol) der i enkelt hed selv sørge for at alle VLAN ændringer bliver sendt ud på alle switch'ne i VLAN domænet.

Det er sat op således at vi har en VTP server, som er SW1C. Den styre alle vores VLAN, det vil sige at det er her vi opretter, ændre og sletter VLAN's. De andre switche i domænet køre alle som VTP klienter, da disse ikke skal kunne ændre i VLAN databasen. De vil modtage og videre sende informationen som de modtager fra VTP serveren. Der findes en type mere som vi ikke har valgt at gøre brug af, dette er den transperante.

Den er en "selvstændig server" dvs. man kan tilføje, rette og slette VLAN's på denne, men det vil kun påvirke denne switch. Den vil dog heller ikke tage imod information fra VTP serveren, dog vil den stadig videre sende informationen videre rundt i VTP domænet. Vores VTP domæne hedder GreenClass.

Operativ Systemer

DC01

Generelt

DC01 fungerer som Domain Controller i vores setup til Green Class. Vi har valgt at lave en Domain Controller, da vi synes det er vigtigt at samle og styre vigtige ting fra et centralt sted. På DC01 finder vi bl.a. AD'et, DHCP og DNS, som jo alle 3 er meget vigtige ting at have styr på og det gør en Domain Controller jo ganske godt.

DC01 er installeret på en Fysisk server med Windows Server 2003 R2 Enterprise, hvorefter der så er blevet installeret rollerne; Domain Controller (Active Directory), DNS, DHCP og WINS. Vi har valgt en 2003 udgave, da det er det vi har beskæftiget os med i vores skole undervisning og derfor noget vi kender til. Vi har valgt den lidt sikre løsning, frem for at vælge en Server 2008, fordi DC01 er en meget vigtig server i vores setup til Green Class.

Det er meget vigtigt at DC01 fungerer, da den bruges til og af så mange ting. F.eks. mange af de andre servere bruger bl.a. den som DNS server. Og for klienterne, der bruger den til at få deres IP adresser via DHCP og til at styre rettigheder for f.eks. filer og mapper. For Exchange serveren er DC01 meget vigtig da den står for valideringen af brugerne. (For mere info se evt. bilag 5)

AD

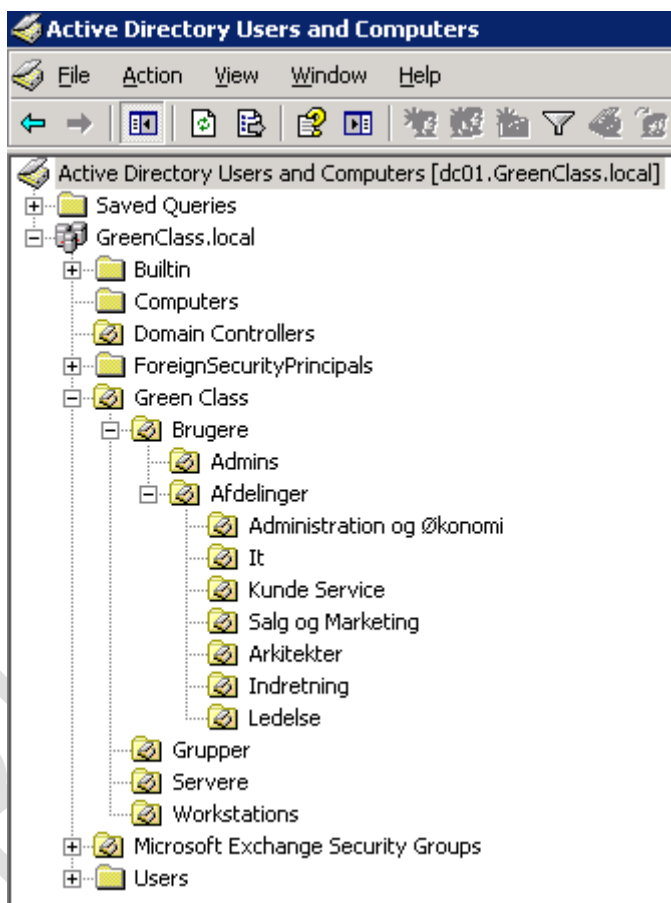
Generelt

På vores Domain Controller finder vi selvfølgelig AD'et hvor bl.a. Green Class medarbejdere skal have deres egen bruger oprettet. AD'et skal styre rettighederne for Green Class, så der ikke er nogle som kommer til f.eks. at åbne dokumenter som de ikke burde se. Derfor vil vi oprette mapper til de enkelte afdelinger, så hver afdeling har deres egen mappe, som fælles gemmested for dokumenter m.v..

OU'er

Vi har først og fremmest valgt at lave et OU der hedder Green Class. (Se billede på næste side.) Dette OU bruges til at samle de ting som vi opretter til Green Class, som ikke følger med installationen af Active Directory. Det har vi så underopdelt i Brugere, Grupper, Servere og Workstations. OU'et Brugere er så igen opdelt i Admins og Afdelinger. I OU'et Admins findes IT afdelingens administrator brugere, som har fulde rettigheder på f.eks. alle servere og mapper. Under Afdelinger finder vi et OU til hver afdeling hos Green

Class plus et OU til Ledelsen. I hvert af disse afdelings OU'er findes brugere til de medarbejdere der hører til afdelingen. Bemærk at IT afdelingen har 2 brugere pr. mand. En almindelig bruger, som de bruger til at logge på f.eks. deres pc'er og mail, og en administrator brugere som bruges når der skal laves ændringer på bl.a. servere. Denne opdeling har vi valgt for bl.a. at kunne holde styr på hvornår de er på for at arbejde på en server og hvornår de er inde for at lave ændringer i opsætningen. Dermed er det nemmere senere at bruge f.eks. Event Log til at se hvad der kunne have skabt et problem eller en fejl. Navngivningen af administrator brugerne sker ved at tage admin + brugernavn. Dvs. at hvis brugernavnet for den almindelige bruger er peter, så er administrator brugernavnet adminpeter.



OU'et Grupper bruges til at holde styr på alle Green Class's grupper, både med og uden mailadresser tilknyttet. Der findes bl.a. grupper til de enkelte afdelinger, der alle er

Universal grupper, da de også skal bruges som mailgrupper. Og Exchange 2007 vil kun acceptere grupper der står til at være Universal. Derudover har vi valgt at oprette grupper som styre rettighederne til at kunne åbne forskellige programmer, for bl.a. at kunne styre hvilke og hvor mange licenser Green Class skal investere i til de forskellige programmer. Et eksempel kunne være en gruppe der hedder Office, så det kun er medlemmer af denne gruppe som kan bruge programmerne i Office pakken.

I OU'ne Servere og Workstations skal bruges til at placere servere og medarbejdernes Pc'er, som er meldt ind i domænet greenclass.local, et samlet sted i AD'et.

GPO'er generelt

Først og fremmest har vi valgt at installere og bruge Group Policy Management, da vi mener det er med til at give et rigtig godt overblik over de GPO'er vi har lavet og for den sags skyld vil lave i fremtiden.

Vi har valgt at bruge GPO'er, fordi de er gode til at lave og styre forskellige indstillinger for brugerne. Vi vil komme ind på nogle af de forskellige GPO'er i løbet af rapporten. Dvs. de bliver beskrevet sammen med det de bruges til eller sammen med. Men vi vil da lige nævne et par stykker her.

Først har vi lavet en policy som gælder for alle almindelige bruger, som gør at de alle får det samme baggrundsbillede. Og dertil også at de ikke kan ændre på denne indstilling.

Desktop/Active Desktop	
Policy	Setting
Active Desktop Wallpaper	Enabled
Wallpaper Name:	\\FS01.Greenclass.local\Shares\default\wallpaper.jpg
Example: Using a local path: C:\windows\web\wallpaper\home.jpg	
Example: Using a UNC path: \\Server\Share\Corp.jpg	
Wallpaper Style:	Stretch
Policy	Setting
Allow only bitmapped wallpaper	Disabled
Disable Active Desktop	Disabled
Enable Active Desktop	Enabled
Allows HTML and JPEG Wallpaper	
Policy	Setting
Prohibit changes	Enabled

Som det kan ses så ligger baggrundsbilledet i et share på serveren FS01, fordi her har alle brugere adgang til.

Så har vi også lavet en policy som opretter nogle centrale links/favoritter i deres Internet Explorer. Det er f.eks. links til deres Intranet, hjemmeside og OWA. (Se billede her under)

Internet Explorer Maintenance	
URLs/Important URLs	
Name	URL
Home page URL	http://gc.nyhuus.eu/intranet
Search bar URL	Not configured
Online support page URL	Not configured
URLs/Favorites and Links	
Policy	Setting
Place favorites and links at the top of the list in the order specified below	Enabled
Delete existing Favorites and Links, if present	Not configured
Delete existing channels, if present	Not configured
Favorites	
Name	URL
Green Class Intranet	http://gc.nyhuus.eu/intranet
Green Class Website	http://gc.nyhuus.eu
Dokumentations Wiki	http://gc.nyhuus.eu/doku
OWA	https://exchange.greenclass.local/owa
google	http://www.google.dk

DNS

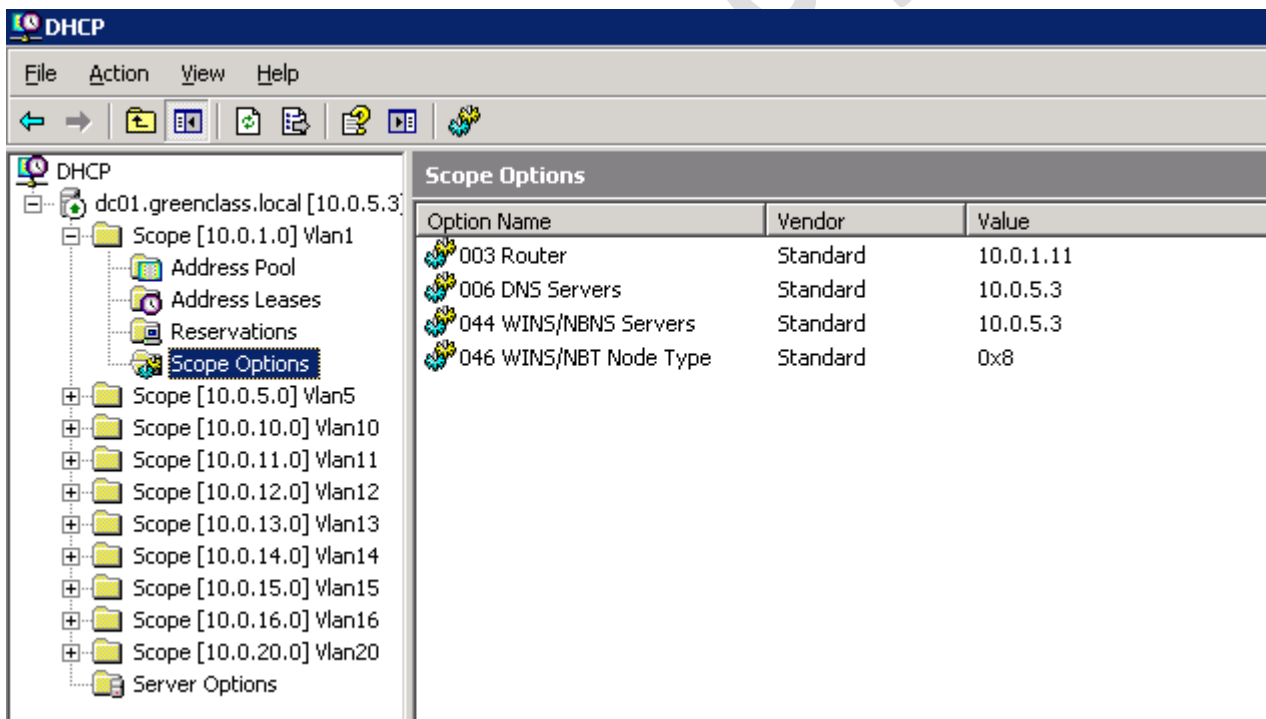
På DC01 har vi også installeret DNS, som styrer DNS for alle vores servere. Vi har opsat alle serverne i DNS'en med både forward og reverse lookup zoner. Det betyder bl.a. at alle serverne kan tilgås via deres navn + .greenclass.local, f.eks. dc01.greenclass.local.

Dog er det sådan at hvis man laver en reverse lookup for web01's IP adresse, så vil man få at vide at det er gc.nyhuus.eu. Det er fordi vi har sat det op så man kan tage de 3 websites på web01 ude fra internettet.

Alle DNS opslag som ikke omhandler greenclass.local eller gc.nyhuus.eu, bliver sent videre til openDNS.org via deres 2 IP adresser 208.67.222.222 og 208.67.220.220.

DHCP

DC01 fungerer også som DHCP server, og dermed den som tildeler IP adresser til de forskellige klienter. Der er først og fremmest lavet scopes til de forskellige VLAN's, ud fra princippet VLAN YY's scopes starter ved 10.0.YY.20 og slutter ved 10.0.YY.254. Dertil kommer at 10.0.YY.1 er default gateway. DC01's IP adresse (10.0.5.3) er sat som både WINS server og DNS server.



ISA01

Generelt

ISA01 køre på en fysisk server med Windows Server 2003 R2 Enterprise, og herpå er så installeret ISA Server 2006 Enterprise.

Vi har valgt ISA, primært af den årsag at det er det vi har lært igennem et valgfrit speciale fag. Vi synes ISA er et rigtig godt værktøj til

firewall og cache

håndtering. Vi havde også

overvejet at benytte

pfSense hvilket er baseret

på linux, men det gik vi fra

igen af den årsag er der ikke

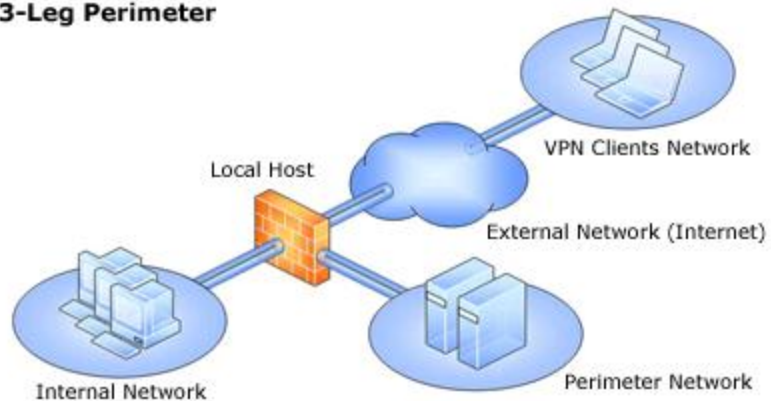
rigtig var nogle af os der

kender ret meget til linux.

Mere info om serveren

findes i bilag 6.

3-Leg Perimeter



Netværk

Vores netværk er bygget op som det ses her på billedet herover, nemlig med en Intern zone (LAN), en Ekstern zone (WAN) og en DMZ zone hvor servere som skal kontaktes fra WAN findes.

Netværks regler

Vi har i alt 6 forskellige netværks regler, heraf er de fire router og de sidste to er nat.

- Localhost Adgang – Localhost => All protected networks via ROUTE
- VPN adgang til LAN – VPN => Internal (LAN) via ROUTE
- LAN og VPN adgang til DMZ – LAN, VPN => DNZ via ROUTE
- DMZ adgang til LAN og VPN – DMZ => LAN, VPN via ROUTE
- DMZ adgang til eksternt (WAN) – DMZ => WAN via NAT
- LAN og VPN adgang til eksternt (WAN) LAN, VPN => WAN via NAT

DMZ

Vi har valgt at benytte en DMZ zone fordi vi mener det giver os mere sikkerhed i vores netværk.

Her har vi valgt at placere Web, Exchange samt vores tre terminal servere, da det er servere man skal kunne tilgå ude fra.

Firewall

Firewall er en rigtig god beskyttelse overfor trusler ude fra, så vel som inde fra også.

Vi har blokeret stort set alt i vores firewall. Der er åben for internet sider (port 80) fra DMZ og LAN, sådan så folk har adgang til at se diverse hjemmesider. De har også adgang til FTP på port 21. Samt at de har adgang til Messenger.

Vi har en lille åbning for DNS hvilket gør at vores DNS server (DC01) og kun DC01 har adgang til at kontakte openDNS.org på 2 IP adresser som er 208.67.222.222 og 208.67.220.220, ellers er alt andet DNS ud af til blokeret. I mellem DMZ og LAN har vi DNS åben fra DMZ og til DC01. ISA servere i sig selv benytter også vores interne DNS server for at den skal kunne tilgå alle vores egne servere via deres DNS navne.

Hvad angår DHCP så har vi tilladt ISA serveren og kun den, at modtage DNS fra det eksterne netværk, så den kan modtage IP opsætning fra vores ISP. Internt har vi åbnet DHCP relay fra LAN til DMZ og DHCP request fra DMZ til LAN.

Publishing

Web01

Web01 er host for vores 3 hjemmesider. Denne er publiceret via ISA serveren så den kan tilgås ude fra. Den er sat op til at lytte på port 80 og 81. Grunden til vi har sat port 81 på er at port 80 allerede routes videre til ebokz.dk, en af skolens hjemmesider der også går gennem samme router.

Den er ydermere sat op til kun at vise hjemmesiden hvis den bliver tilgået via gc.nyhuus.eu, 87.63.202.202 (Skolens WAN IP), 192.168.1.10 (ISA01's WAN IP), www.greenclass.local og web01.greenclass.local.

Exchange

Det var også meningen at Exchange serveren skulle publiceres, men på grund af problemer med at få forwardet portene i skolens router, så er dette ikke muligt. Dog er ISA01 sat op så hvis der ikke var problemer med routeren så vil Green Class medarbejderne også kunne oprette forbindelse til deres Exchange profil via en Outlook 2007 klient fra f.eks. en hjemme pc. Eller de vil kunne bruge webmail OWA, som følger med Exchange 2007.

Cache

Der er sat cacheing op, med en størrelse på 5GB. Der er lavet en GPO der gør at brugere automatisk vil blive sat op til at benytte ISA serveren som Proxy.

User Configuration (Enabled)			hide
Windows Settings			hide
Internet Explorer Maintenance			hide
Browser User Interface/Customized Title Bar			show
Connection/Proxy Settings			hide
Enable proxy settings			
Protocol	Server	Port	
HTTP	ISA01.GreenClass.local	8080	
Secure	ISA01.GreenClass.local	8080	
FTP	ISA01.GreenClass.local	8080	
Gopher	ISA01.GreenClass.local	8080	
Socks	ISA01.GreenClass.local	8080	
Exceptions:			
	Do not use proxy server for addresses beginning with		
	Do not use proxy server for local (intranet) addresses	Enabled	

VPN

Der er mulighed for at tilgå LAN netværket ude fra via VPN PPTP. Dog mangler skolens router opsætning også her.

Dette er meget brugbart hvis en arkitekt er ude ved en kunde, og arkitekten skal bruge noget fra sit eget brugerdrev som ligger internt på FS01. Ved at tilgå LAN netværket via VPN, vil de få det nøjagtigt som hvis de sad oppe på kontoret og var sluttet til fra LAN siden af netværket.

For at man kan logge ind VPN kræver det at ens bruger er medlem af AD gruppen Remote users, da det kræver en godkendt bruger at tilgå LAN netværket via VPN.

FS01

Generelt

FS01 fungerer som File Server, og er installeret på en fysisk server med Windows Server 2003 R2 Enterprise som grundsten. Hertil kommer så at vi har installeret rollen File Server.

Vi har valgt at have en File server, da Green Class gerne vil kunne tilgå deres filer fra forskellige locationer. Med en File Server kan vi samle de data som de skal bruge og tilgå forskellige steder fra. Vi har også valgt at lave nogle shares og netværksdrev, som de kan bruge når de vil gemme, dele og tilgå data.

For mere info om serveren se evt. bilag 7.

Roaming Profiles

Flere af medarbejderne i Green Class A/S arbejder fra flere forskellige lokaliteter, og derfor skal kunne tilgå deres data ligegyldigt om de så sidder ved deres stationære pc på kontoret eller om de tilgår TS setuppet via RDP på en bærbar pc, har vi valgt at Roaming Profiles. Det er smart da deres data så kun gemmes et sted, og dermed kan de altid tilgå.

Til Roaming Profiles har vi lavet et share (en delt mappe) her på Fileservicen, FS01, som hedder "Roaming".

Users har rettigheden "Change" som share permission, så de kan tilgå og ændre i mapper i sharet.

Derudover er der så lavet NTFS rettigheder, hvor administratorer har Full Control og brugerne kun har List Folder Contents. Dermed bliver Users låst til kun at kunne se mappe strukturen.

I mappen "Roaming" bliver der så vores GPO "Roaming User" lavet en mappe til hver bruger den første gang de logger på. På denne brugermappe har brugeren selv så Full Control, da det er brugerens egen.

Users har ingen rettigheder, da rettighederne fra mappen Roaming ikke bliver nedarvet. Normalt vil Administrators ikke få rettigheder på en Roaming Profile mappe, men via GPO har vi sagt at administrators har Full Control rettighed. Derved kan de lave rettelser og løse problemer for brugeren. (Se billede.)

Computer Configuration (Enabled)		hide
Administrative Templates		hide
System/User Profiles		hide
Policy	Setting	
Add the Administrators security group to roaming user profiles	Enabled	

Vi har valgt kun at centraliser My Documents og Application Data, vi mener det kun er disse to der vil give mening for medarbejderne i Green Class A/S. Man kan også centralisere Skrivebord og Start Menu, men da nogle dels vil arbejde direkte på en Pc som er meldt i AD'et og dels på TS serverne. Dermed vil der være

installeret forskellige programmer og derfor vil Skrivebordet og Start Menuen se forskellige ud, da der vil være forskellige genveje til programmer mv.

Grunden til at vi har valgt My Documents er fordi det er her folk gemmer deres dokumenter mm., som de skal altid skal have adgang til.

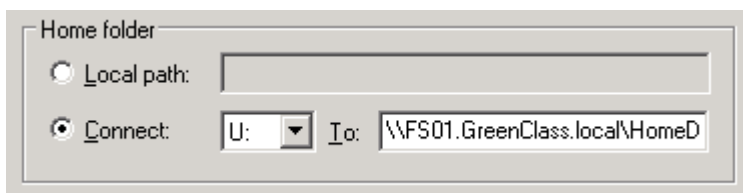
I Application data findes f.eks. en masse pr. bruger indstillinger til Office pakken, som bl.a. templates, signaturer og Outlook profilen. Derfor er denne også vigtig for brugerne at have adgang til, lige meget hvor de logger på.

Centraliseringen af My Documents og Application Data sker også via GPO'en Roaming, hvor vi har lavet en Folder Redirection af de 2 mapper, her over til FS01. (Se billede.)

User Configuration (Enabled)	hide
Windows Settings	hide
Folder Redirection	hide
Application Data	hide
Setting: Basic (Redirect everyone's folder to the same location)	hide
Path: \\Fs01\Roaming\%USERNAME%\Application Data	
Options	hide
Grant user exclusive rights to Application Data	Disabled
Move the contents of Application Data to the new location	Enabled
Policy Removal Behavior	Leave contents
My Documents	hide
Setting: Basic (Redirect everyone's folder to the same location)	hide
Path: \\Fs01\Roaming\%USERNAME%\My Documents	
Options	hide
Grant user exclusive rights to My Documents	Disabled
Move the contents of My Documents to the new location	Enabled
Policy Removal Behavior	Leave contents

Shares og Netværksdrev

Udover et share til Roaming så har vi også lavet et share der hedder HomeDrives og et der hedder Grupper. HomeDrives bruges til at give de forskellige brugere deres eget lille drev hvor de kan gemme data. Dette drev bliver lavet via en indstilling på hver bruger i ad'et.



Home folder

Local path:

Connect: U: I: \\FS01.GreenClass.local\HomeD

Under sharet Grupper findes en mappe til hver afdeling, og disse mapper bliver fordelt til brugerne ud fra hvilken afdeling de hører til. Disse drev bliver tildelt via en GPO som starter et script når brugeren logger på.

User Configuration (Enabled)	hide
Windows Settings	hide
Scripts	hide
Logon	hide
Name	Parameters
\\GreenClass.local\NETLOGON\Ledelse.bat	

Et eksempel på et script:

```
@ECHO OFF
set group=Ledelse
NET USE K: "\\FS01.GreenClass.local\Grupper\%group%" /PERSISTENT:NO
EXIT
```

WSUS

WSUS (Windows Server Update Services) er et genialt værktøj, det gør at vi kan nøjes med at downloade opdateringer til kun en server, denne server sørger så for at alle servere og klienter i vores netværk bliver holdt up to date, vi kan 100 % selv bestemme hvilke opdatering vi vil have via WSUS administrationen. Dette spare os for en masse trafik på WAN siden, som vi har det nu har vi en forbindelse til Microsoft det er vores FS01 hvorpå WSUS ligger, den synkronisere kl. 02:00. Altså på et tidspunkt der ikke er nogle brugere på internettet, så den fungere helt ugenert. I stedet for at vi havde alle 10 servere samt alle klienter direkte på Microsoft update, så ville der lige pludselig komme stort load på internettet på grund af opdateringer. Vi har så konfigureret via GPO at klienter og servere bliver opsat til at benytte vores WSUS server i stedet for Microsoft update.

Computer Configuration (Enabled)		hide
Administrative Templates		hide
Windows Components/Windows Update		hide
Policy	Setting	
Allow Automatic Updates immediate installation	Enabled	
Allow non-administrators to receive update notifications	Disabled	
Automatic Updates detection frequency	Enabled	
Check for updates at the following interval (hours):	8	
Policy	Setting	
Configure Automatic Updates	Enabled	
Configure automatic updating: The following settings are only required and applicable if 4 is selected.	4 - Auto download and schedule the install	
Scheduled install day:	0 - Every day	
Scheduled install time:	03:00	
Policy	Setting	
Delay Restart for scheduled installations	Enabled	
Wait the following period before proceeding with a scheduled restart (minutes):	30	
Policy	Setting	
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled	
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Disabled	
Enable client-side targeting	Enabled	
Target group name for this computer	Servere	
Policy	Setting	
No auto-restart for scheduled Automatic Updates installations	Disabled	
Re-prompt for restart with scheduled installations	Enabled	
Wait the following period before prompting again with a scheduled restart (minutes):	5	
Policy	Setting	
Specify intranet Microsoft update service location	Enabled	
Set the intranet update service for detecting updates:	http://10.0.5.5	
Set the intranet statistics server: (example: http://IntranetUpd01)	http://10.0.5.5	

WUP01

Generelt

WUP01 fungerer som overvågningsserver, og er placeret i vores LAN miljø. Dvs. at den bruges til at overvåge vores andre servere og switche. Grundlæggende overvåger den ved at WUP01 henvender sig til serverne og switch'ne, for at checke om de svarer som de skal ud fra hvad der er sat op af overvågning.

Vi har valgt at have en overvågningsserver, da vi mener at det er vigtigt for en IT afdeling at vide om servere og switche fungerer. Vi synes det er vigtigt at man holder øje med vigtigt services, protokoller og porte. Man kan jo have et website som bare skal være kørende, da hele virksomheden bygger på f.eks. nethandel, bestillinger og/eller reklame via websitet. Eller måske er det super vigtigt at firmaet altid kan modtage mails, ellers mister de måske ordrer.

Med overvågning kan man selvfølgelig ikke undgå at der kommer nedbrud, men nede tiden vil med sandsynlighed være noget kortere. Tiden vil være mindre, da IT afdelingen ikke først reagere når brugere har henvendt sig, ang. fejl, men så snart de får en alarm så kan de begynde fejlfinding og fejlretning.

Hos Green Class A/S er det selvfølgelig vigtigt at deres website www.greenclass.local virker så både nye og gamle kunder kan finde info og hjælp. Derudover så skal Exchange serveren jo også kunne modtage og sende mails, da medarbejderne kommunikere meget både internt og eksternt via mail.

Display Name	Host Name	Address	Device Type	Status
ISA01 (LAN interface)	ISA01.greenclass.local	10.0.1.1	Windows 2003 S...	
SW1C	SW1C	10.0.1.11	Switch	
SW1D	SW1D	10.0.1.21	Switch	
SW2D	SW2D	10.0.1.22	Switch	
SW1A (Servere)	SW1A	10.0.1.31	Switch	
SW2A (Klienter)	SW2A	10.0.1.32	Switch	
dc01.greenclass.local	dc01.greenclass.local	10.0.5.3	Windows 2003 S...	
fs01.greenclass.local	fs01.greenclass.local	10.0.5.5	Windows 2003 S...	
vcenter.greenclass.local	vcenter.greenclass.local	10.0.5.10	Windows 2003 S...	
ISA01 (DMZ interface)	ISA01.greenclass.local	172.16.1.1	Windows 2003 S...	
web01.greenclass.local	web01.greenclass.local	172.16.1.3	Web Server	
tssb.greenclass.local	tssb.greenclass.local	172.16.1.4	Windows Server	
ts01.greenclass.local	ts01.greenclass.local	172.16.1.5	Windows Server	
ts02.greenclass.local	ts02.greenclass.local	172.16.1.6	Windows Server	
exchange.greenclass.local	exchange.greenclass.local	172.16.1.8	Email server	
esx01.greenclass.local	esx01.greenclass.local	172.16.1.10	Linux Server	
ISA01 (WAN interface)	ISA01.greenclass.local	192.168.1.10	Windows 2003 S...	

Vi har valgt at arbejde med overvågningsprogrammet WhatsUp Gold, da der i vores gruppe er lidt erfaring med at arbejde med det til dagligt. Det er forholdsvis simpelt og så kører det på en Windows platform, og Windows er det vi i gruppen har mest kendskab til og har arbejdet med i skoletiden.

Opsætning generelt

Vi har installeret WhatsUp Gold på en fysisk server med Windows Server 2003 R2 32 bit Enterprise. Den er installeret på en fysik server og placeret i vores LAN miljø. Det er den fordi den kun skal kommunikere med interne servere og skal altså ikke hverken modtage eller sende data via Internet.

Der er ikke installeret noget ud over en almindelig Enterprise installation af Windows Server 2003. Dog installerer WhatsUp Gold selv en Microsoft SQL Server 2005 Express Edition. For mere info om serveren så se bilag 8.

Servicevindue

Vi har valgt at have et tidsrum hvor vores servere ikke bliver overvåget, og her har vi valgt tidsrummet mellem kl. 16:00 og kl. 08:00 næste morgen på hverdage. Samt servicevindue hele weekenden. Det har vi fordi det er mellem tidsrummet kl. 08:00 og kl. 16:00 at vi arbejder på serverne, og derfor her vi har brug for at vide om der skulle være problemer på en eller flere af serverne. F.eks. har det været en fordel da vi skulle lukke ned for nogle ting i firewall'en på ISA serveren. Så kunne vi nemlig hurtigt få et overblik over om der var noget vi hvad lavet forkert eller bare lige glemt at tænke på.

Normalt vil man bruge et servicevindue til at genstarte serveren efter f.eks. at den har fået installeret opdateringer eller til at opgradere serveren med flere RAM eller anden hardware.

Hvis dette nu ikke var et skoleprojekt, men rent faktisk var et setup i en rigtig virksomhed, så vil servicevinduet nok ikke være så stort. Her vil vi have valgt et mindre servicevindue om natten. Det kunne f.eks. have været fra kl. 00:00 til kl. 06:00, da der formentlig ikke er nogle som vil skulle bruge serverne i dette tidsinterval.

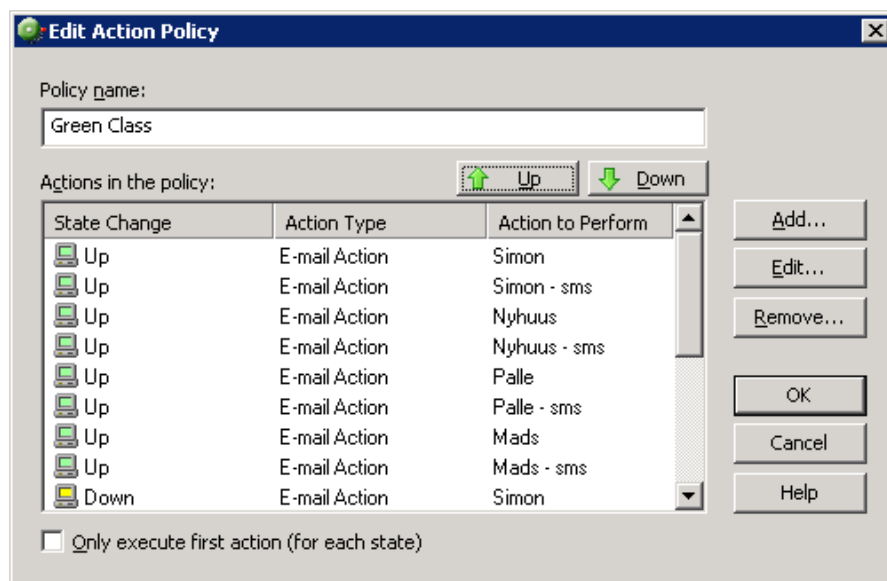
Man kunne jo også lave et differentieret overvågningssetup, hvor man havde forskellige servicevinduer, alt efter hvilken type server det er. F.eks. kunne vores TS servere godt have et forholdsvis stort servicevindue, i forhold til vores mail og web-server der gerne skal have et så lille servicevindue som muligt.

Vigtigst af alt er det at servicevinduet passer til vigtigheden af serverne, og hvornår de bruges.

Alarmer

Vi har valgt at IT afdelingen skal modtage alarmer via mail og SMS, for at sikre at alarmerne ikke bliver overset også selvom de ikke lige er ved deres Pc og dermed deres mail.

Mailadresserne og "mobilnummerne" er samlet i en alarm policy i WhatsUp. Denne policy er så sat på de enkelte ting man vil overvåge. Hvad der bliver overvåget kan ses i bilagene med serverdoc for de enkelte servere.



Mail og SMS opsætning

For at kunne sende mails ud fra WhatsUp, så skal man bruge en SMTP server. Her bruger vi Exchange serveren, da den jo heldigt nok har til formål at sende mails ud.

For at kunne sende SMS'er ud, så skal man bruge en SMS gateway, for at sende ud på mobilnettet. Vi har ikke nogle sms gateways ved hånden, så vi har valgt at bruge en service ude i byen. Servicen kommer fra hosting firmaet DIR A/S, og fungerer ved at man sender en mail til en mailadresse hos dem og så bliver mailen sendt videre som en SMS.

ESX01

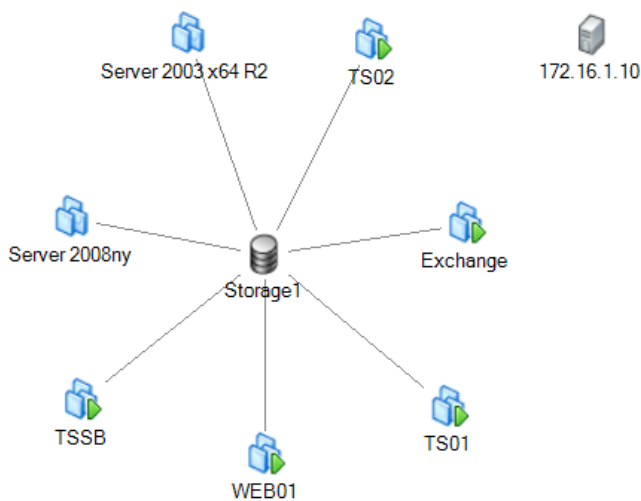
Generelt

ESX01 er en VMware ESX 4.0, og dermed en 64 bit maskine. Den bruges som host for alle de virtuelle servere, som vi har valgt at Green Class skal have i deres setup. Info om serverens hardware kan findes i bilag 9.

Vi har valgt at bruge virtuelle servere, da vi klart mener at det er fremtiden, at køre virtuelt. Det er nemt lige at lave en ny server, lave redundans eller backup af hele servere.

Netværk

ESX01 har et Storage hvor alle de virtuelle servere har deres logiske diske på. Herunder ses et billede over hvordan de 5 servere er forbundet. "Server 2003x64 R2" og "Server 2008ny" er templates, og er derfor ikke kørende. Disse findes for at man hurtigt kan sætte en ny server op, hvis der skulle blive brug for det. Hvis f.eks. firmaet får flere medarbejdere og de derfor får brug for en ekstra TS server.



Virtuelle server

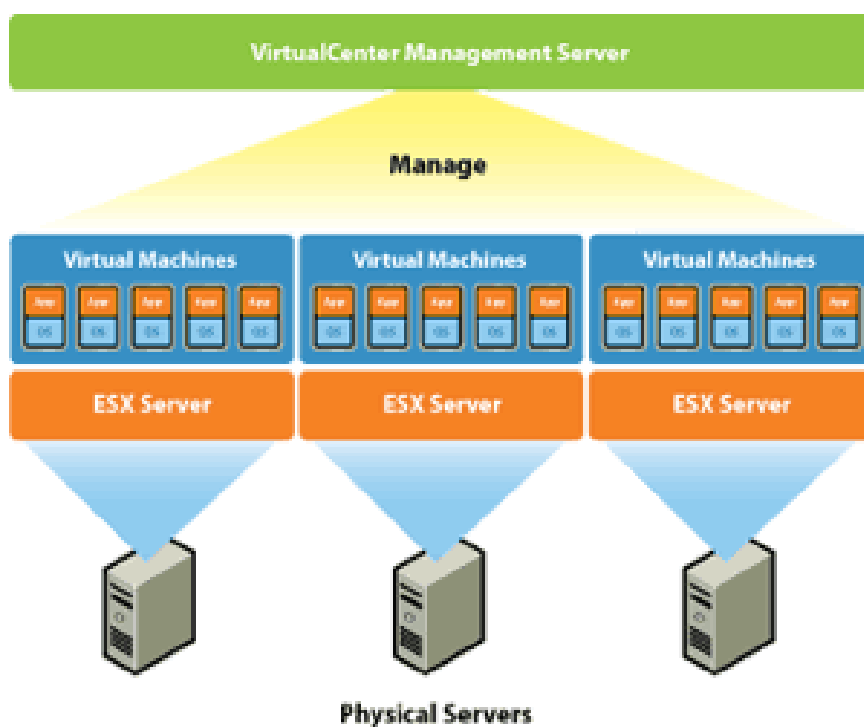
Vi har valgt at det er de servere som skal være i DMZ'en der skal være virtuelle. Dvs. at følgende servere er virtuelle:

- Exchange
- WEB01
- TS01
- TS02
- TSSB

vCenter

Generelt

vCenter er en fysisk server med Windows Server 2003 R2 Enterprise, hvor der er installeret vCenter server, fra VMware ESX 4.0. Vi har valgt at installere vCenter, da det giver nogle flere muligheder end bare at tilgå ESX server direkte via vSphere Client. Det giver mulighed for at se flere ESX server i samme vSphere Client, og nem mulighed for at genstarte ESX serveren. Se evt. også bilag 10 for mere info.



Web01

Generelt

Web01 er som navnet næsten siger det selv, en web server. Den er installeret op på en virtuel server med en Windows Server 2003 R2 64 bit Enterprise.

Vi har benyttet os af et gratis CMS systemer der hedder Joomla til vores offentlige hjemmeside. Joomla er lavet i PHP.

Vi har derudover et intranet som er baseret på blog systemet WordPress som ligeledes er lavet i PHP, her køre vi LDAP opslag imod vores Windows AD (DC01) for at kan benytte vores AD brugere til at logge ind på intranettet med. Er man medlem af vores Green Class Administrators gruppe i AD'et, vil man automatisk blive administrator på intranettet.

Vi har som vores sidste hjemmeside også en dokumentation som køre på dokuwiki, hvilket er en lille version af et wiki system. Da de plugins vi kunne finde til LDAP opslag med AD ikke rigtig havde nogle bruger styringer valgte vi ikke at bruge dette, da det kun er folk i IT afdelingen der skal have adgang til denne dokumentation.

Det er muligt for os at benytte LDAP opslag til alle vores hjemmesider hvis vi har behov for det.

Websites

Intranet – <http://gc.nyhuus.eu:81/intranet/> ude fra inde fra virker <http://gc.nyhuus.eu:81/intranet> også.

Hjemmeside – <http://gc.nyhuus.eu:81> ude fra inde fra virker <http://gc.nyhuus.eu> også.

Dokumentation – <http://gc.nyhuus.eu:81/doku/> ude fra virker <http://gc.nyhuus.eu/doku/> også.

Opsætning

Vi har sat vores webserver op ved brug af programmet WAMP Server 2 som indeholder Apache, PHP, MySQL og PHPmyAdmin. Grunden til dette er at vi havde nogle udfordringer med at få PHP til at fungere med LDAP opslag på IIS. For mere info se bilag 11.

Exchange

Generelt

Som navnet siger så fungerer denne server som en Exchange server, som skal bruges som mailserver for Green Class. Det er en Exchange Server 2007 udgave, som ligger oven på en virtuel server med Windows Server 2008 Enterprise 32 bit. Se evt. bilag 12 for mere info om serveren.

Vi kunne have valgt bare at installere en POP3 mailserver, men i dagens arbejdsliv bliver mail mere og mere vigtigt og skal kunne mere og mere, og derfor har vi valgt at bruge Exchange. Her kan en bruger f.eks. have flere mailadresser tilknyttet og man kan også have grupper med mailadresser, så flere kan modtage den samme mail. Med Exchange får man også kalender og dertil deling af kalender. Man kan også lave ressourcer, såsom mødelokaler og andre ting som kan/skal bookes.

Opsætning

Først og fremmest skal det siges at vi godt ved at man ikke bør installere Exchange 2007 oven på et 32 bit Operativ System, da det ikke er supporteret. Men vi havde kun en 32 bit udgave af Windows Server 2008, og Microsoft skriver selv at det fint kan bruges til studie og test. Derfor valgte vi at det godt kunne gå an til dette skoleprojekt.

Fra den ene bekendelse til den anden. Grundet at ESX01 ikke kunne få flere RAM, så har Exchange Serveren ikke fået nok RAM til at kunne køre ubeklageligt, men den fungerer ganske ude mærket. Lidt langsom at arbejde på men den virker. I et normalt setup vil der selvfølgelig skulle flere RAM til.

Brug af Exchange

For at Green Class kan bruge deres Exchange, så er der lavet en opsætningsguide til Outlook 2007 til dem. (Se bilag 4) Den hjælper dem trin for trin med at sætte en profil op, så de kan bruge deres Outlook 2007 til at sende og modtage mails.

Derudover kan de tilgå webmail via linket <https://exchange.greenclass.local/owa> , hvor de kan logge ind med brugernavn og password.

TSxx

Generelt

Vi har valgt at Green Class skal have et Terminal Server setup, så de på den måde kan arbejde hjemmefra eller via deres bærbar Pc, når de er på farten. TS servere gør jo at det er nemt at komme til at arbejde bare man har en internetforbindelse. Så kan man nemlig via RDP og Windows klienters mstsc oprette forbindelse til serveren og dermed arbejde med firmaets programmer og data, stort set som var man tilstede med kollegaerne.

Vores TS setup består af 2 Terminal Servere, eller front ends om man vil, en Terminal Server Session Broker og så File Serveren med Roaming Profile datene. Derudover kan det tænkes at der måske skal en DB/SQL Server til, hvis Green Class' økonomi system kræver det, men det har vi ikke taget med i vores setup.

Alle TS Servere er virtuelle servere, med Windows Server 2008 Enterprise installeret. 2008 er valgt da den netop har Session Broker rollen som en del Terminal Server, den findes ikke 203.

Her skal det så igen nævnes at der ikke er nok RAM i ESX01, og derfor har især TS01 og TS02 ikke RAM nok til at kunne fungere ordentligt i virkeligheden. Men det går lige i vores "test" setup, da der ikke er mere end et par brugere på serverne ad gangen.

Mere info om alle tre TS Servere findes i bilag 13, 14 og 15.

TS01 + 02 (Front Ends)

TS01 og TS02 er de 2 servere som Green Class' medarbejdere skal logge på via RDP, når de ikke er på firmaets adresse. Her vil de kunne finde de ting som de også bruger når de ikke er på farten. Her snakker vi Office pakken, deres mail og evt. Økonomi system. Derudover kan de selvfølgelig finde deres data via shares mv. til File Serveren (FS01).

Opsætning

Efter installation af Server 2008, så er Terminal Server rollen installeret. For at kunne bruge en Session Broker sammen med sine front ends, så skal man sætte de forskellige servere op til at bruge Session Brokren.

Properties

General | Licensing | **TS Session Broker**

Join a farm in TS Session Broker

TS Session Broker server name or IP address:

Farm name in TS Session Broker:

Participate in Session Broker Load-Balancing

Relative weight of this server in the farm

Use IP address redirection (recommended)

Clear this check box only if your load balancer supports the use of [TS Session Broker routing tokens](#).

Select IP addresses to be used for reconnection:

IP Address	Network Connection
<input checked="" type="checkbox"/> 172.16.1.6	Local Area Connection

Clients running Remote Desktop Connection 5.2 and earlier will use only the first IPv4 address.

OK Cancel Apply

Først skal man fortælle hvilken server der er Session Broker, vi har gjort det ved at taste IP adresse for TSSB. Så skal man give TS farmen et navn, og her har vi valgt TSFARM. Relative weight har betydning for hvordan Session Brokern skal fordele RDP forbindelserne på de forskellige front ends. Er de ens så fordeles de lige. Er de forskellige så fordeles de værdier man vælger.

TSSB (Session Broker)

TSSB fungerer som Session Broker, dvs. at den fordeler brugerne på, i vores tilfælde, de 2 TS servere. Det gør den bl.a. ved at kigge på de 2 serveres load. Det er f.eks. RAM og CPU forbrug. Den ser simpelthen på hvor mange frie ressourcer serverne har og sender så brugen hen hvor der er flest frie ressourcer. Derudover kan man selv, som skrevet lidt tidligere, sætte nogle indstillinger som gør at den ene server får flere brugere end den anden.

Udover at fordele brugere, så kan Session Brokern også finde ud af, hvis en bruger har en disconnect session på en af serverne og så forbinde brugeren til den igen, når der igen bliver logget ind, så brugeren ikke får endnu en session.

Opsætning

Efter installation af Server 2008, så er Terminal Server rollen installeret. Derudover er der installeret rollen TS Session Broker, for at den kan fungere som det. Herefter skal TS serverne tilføjes til Session Directory Computers local group på Session Broker serveren.

I DNS er der lavet records som peger ts.greenclass.local ind på de 2 IP adresser som TS01 og TS02 har, og dermed kan man fange TS farmen ved at lave en RDP til ts.greenclass.local.

Serverdoc

Vi har valgt at lave dokumentation over alle serverne, da vi finder det meget vigtigt at der er styr på dokumentationen. Vi har valgt at kalde det for Serverdoc, og de er tilføjet denne rapport som bilag. Serverdoc er en god måde at holde styr på sine servere, især i en fejlfindingssituation, så man har noget at gå ud fra.

Serverens formål

Dette afsnit beskriver hvilket formål serveren har, eller sagt med andre ord, hvilken rolle den har i det setup vi nu har lavet til Green Class.

Serverens afhængighed

Her beskrives hvis serveren er afhængig af andre servere, f.eks. hvis en anden server skal være kørende for at denne server virker.

Serverinfo

Her skrives info om hardware. Dvs. bl.a. server type, RAM, Diske og CPU.

Netværk

I dette afsnit skal der beskrives Netkort(ene)s IP info og evt. manuelt tilføjede router.

Operativ System

Her noteres hvilket Operativ System der kører på serveren.

Server Roller

Her skal notes hvilke Roller der er installeret, hvis det er en Windows Server.

Software

I dette afsnit vil der blive skrevet det software der er installeret udover standart fra Server installationen.

Windows Update

Her vil stå noget om hvordan serveren modtager opdateringer, hvis det er en Windows Server.

Overvågning

Her skrives hvordan serverens servicevindue er og hvad der bliver overvåget.

Evt. flere afsnit kunne være;

- Problemer og løsning (Navn, dato og beskrivelse af problem og løsning)
- Serverændringer (Navn, dato og beskrivelse af ændringer der er lavet på serveren)

Disse to er rigtig gode til en evt. fejlfinding, da man så har tidligere erfaringer at gå ud fra.

Konklusion

Vi har nu lavet vores svendeproe projekt og er ved at afslutte vores rapport. Vi har med udgangspunkt i de ting vi vidste om Green Class og de krav de stillede til deres setup, lavet og skrevet det vi mente vil passe til dem.

Vi har først og fremmest lavet et grundlæggende netværk, som sørger for at de kan komme i kontakt med hinanden og resten af verden. Vi har lavet netværks failover på vigtige forbindelser i netværket, via STP så selvom en forbindelse skulle gå ned, så er der en anden der tager over.

De har fået et godt setup, som er forholdsvis nemt at holde ved lige, og de har via DHCP nemt ved at sætte nye klienter på netværket.

De har fået centralt sikkerhed via ISA01 med dennes Firewall, så der ikke bare er åbent til alt muligt både inde- og udefra. Hertil kommer, at de med DC01 og dennes AD har fået sikkerhed via brugerrettigheder på mapper og filer.

Vi har givet dem en mail server, så de kan sende og modtage mails. Denne mail server er tilmed en Exchange 2007 server, som giver dem flere features.

De har fået en File Server så de nemt kan gemme og dele deres filer et centralt sted. Hertil kommer, at de kan tilgå disse delte data, selvom de ikke lige er på arbejdspladsen. De kan nemlig enten lave en VPN forbindelse til ISA01 og dermed fungere, som sad de på deres arbejds-pc. Eller de kan tilgå deres nye TS setup direkte fra internettet via RDP, og også her kunne tilgå deres data ikke mindst pga. Roaming Profile og netværksdrev.

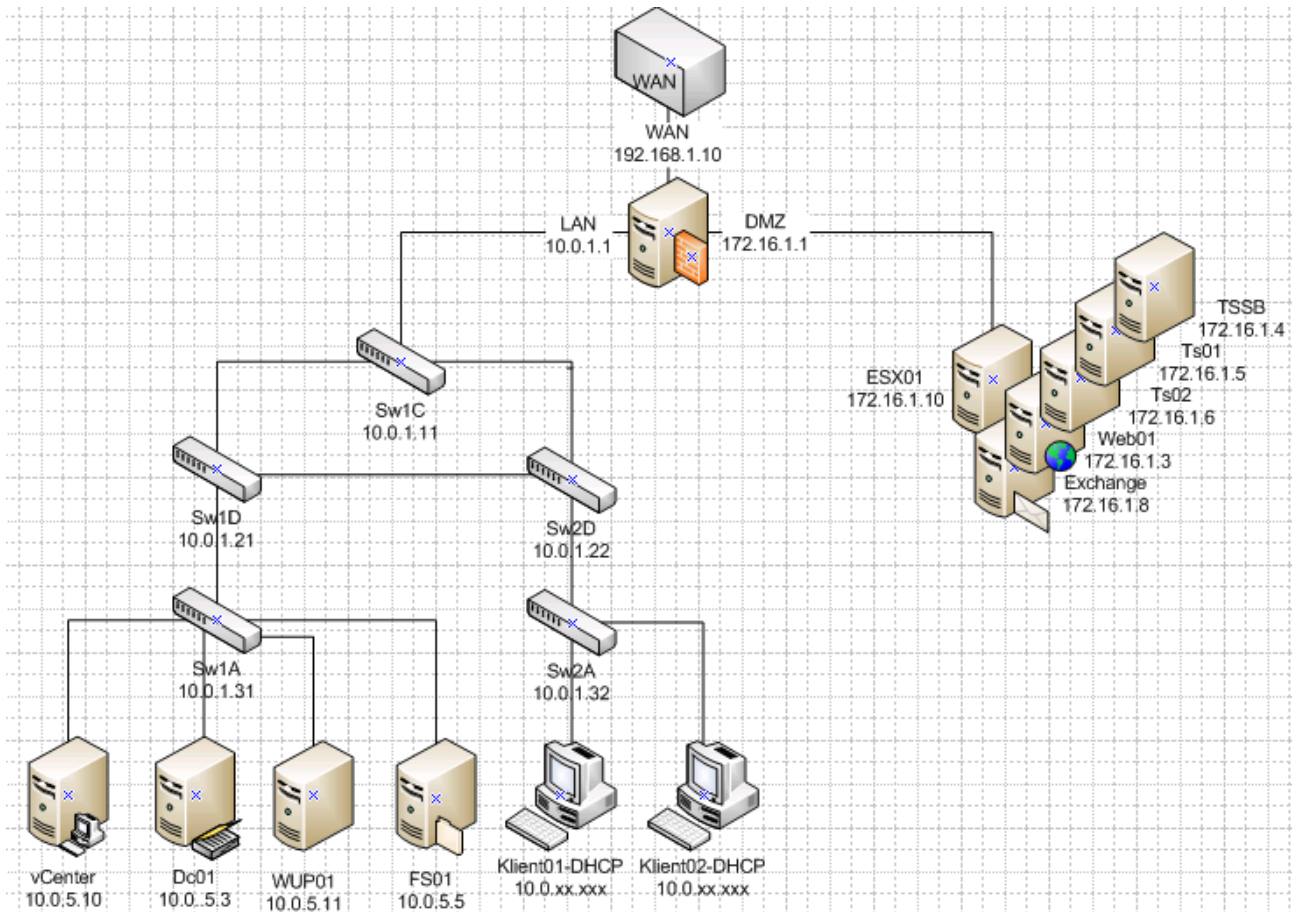
De har med deres WEB01 fået nogle websites, bl.a. en hjemmeside, et intranet samt en dokumentations side, hvor IT afdelingen bl.a. har sin Serverdoc for hver server, så de kan holde styr på dem.

Sidst men ikke mindst har vi lavet en overvågningsserver, så IT afdelingen kan holde øje med om servere og switcher kører som de skal. Dermed skal evt. nede tid gerne kunne sænkes til et minimum.

Denne rapport med tilhørende bilag giver Green Class et godt overblik over deres nye setup.

Bilag

Bilag 1 – Netværkstegning



Bilag 2 – IP plan

ISA01	172.16.1.1	SW1C	10.0.5.1
WEB01	172.16.1.3	DC01	10.0.5.3
TSSB	172.16.1.4		
TS01	172.16.1.5	FS01	10.0.5.5
TS02	172.16.1.6		
Exchange	172.16.1.8		
ESX01	172.16.1.10	vCenter	10.0.5.10
		WUP01	10.0.5.11

WWW.BlogIT.dk

Bilag 3 – Kabeloversigt

ISA01		
Fra port	- Til enhed	Port
NIC01	- WAN	N/A
NIC02	- ESX01	DMZ
NIC03	- SW1C	Fa 0/1

SW1C		
Fra port	- Til enhed	Port
Gi 0/1	- SW1D	Gi 0/1
Gi 0/2	- SW2D	Gi 0/1
Fa 0/1	- ISA01	NIC03
Fa 0/2	- SW1D	Fa 0/1
Fa 0/4	- SW2D	Fa 0/1

SW1D		
Fra port	- Til enhed	Port
Gi 0/1	- SW1C	Gi 0/1
Gi 0/2	- SW1A	Gi 0/1
Fa 0/1	- SW1C	Fa 0/2
Fa 0/2	- SW2D	Fa 0/2
Fa 0/48	- SW2A	Fa 0/48

SW2D		
Fra port	- Til enhed	Port
Gi 0/1	- SW1C	Gi 0/1
Gi 0/2	- SW2A	Gi 0/1
Fa 0/1	- SW1C	Fa 0/4
Fa 0/2	- SW1D	Fa 0/2
Fa 0/48	- SW2A	Fa 0/48

SW1A		
Fra port	- Til enhed	Port
Gi 0/1	- SW1D	Gi 0/2
Fa 0/1	- DC01	NIC01
Fa 0/2	- FS01	NIC01
Fa 0/3	- vCenter	NIC01
Fa 0/4	- WUP01	NIC01
Fa 0/48	- SW1D	Fa 0/48

SW2A		
Fra port	- Til enhed	Port
Gi 0/1	- SW2D	Gi 0/2
Fa 0/1	- GreenClassAP	NIC01
Fa 0/48	- SW2D	Fa 0/48

Bilag 4 – Opsætningsguide til Outlook 2007

Åben Kontrolpanel – Post/Mail

Vælg "Vis Profiler" (Hvis der findes Outlook profiler i forvejen.)

Vælg "Tilføj"

Tildel profilen et navn og klik "OK"

Sæt flueben i "Konfigurer serverindstillinger eller yderligere servertyper manuelt"

Klik "Næste"

Vælg "Microsoft Exchange" og Klik "Næste"

Tilføj ny e-mail-konto

Microsoft Exchange-indstillinger
Du kan angive de oplysninger, der er nødvendige for at oprette forbindelse til Microsoft Exchange.

Skriv navnet på Microsoft Exchange-serveren. Spørg systemadministratoren, hvis du mangler oplysninger.

Microsoft Exchange-server:

Brug Cachelagret Exchange-tilstand

Skriv navnet på den postkasse, administratoren har konfigureret til dig. Navnet på postkassen er normalt dit brugernavn.

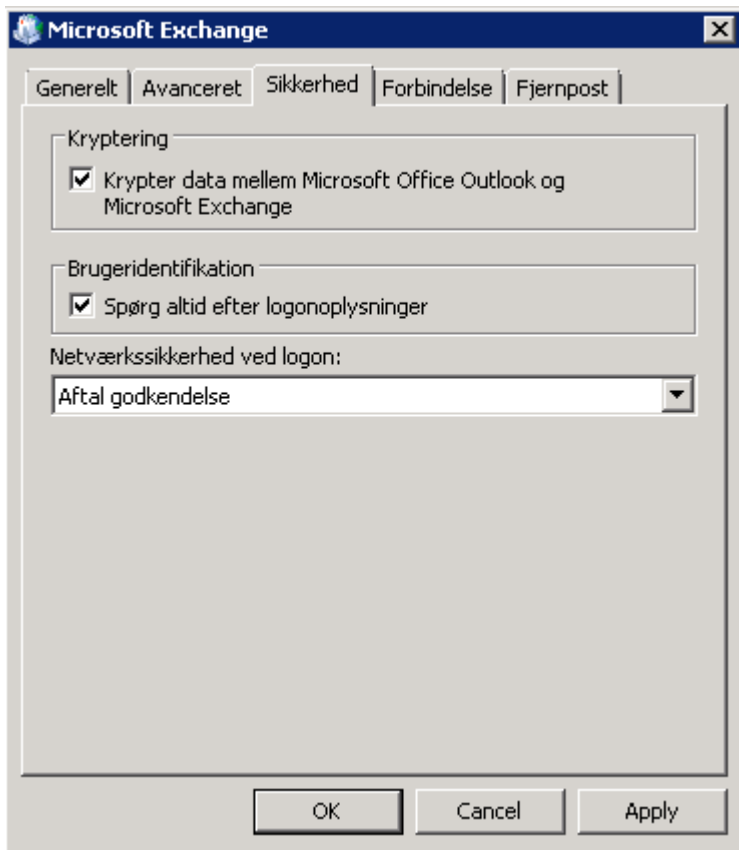
Brugernavn:

Udfyld felterne som vist her ovenfor.

Microsoft Exchange-server: exchange.greenclass.local

Brugernavn: brugernavn@greenclass.local (f.eks. ses@greenclass.local)

Vælg "Flere indstillinger..."



Under fanebladet "Sikkerhed"

Sæt flueben i "Spørg altid efter logonoplysninger" og klik "OK"

Vælg "Kontroller navn"

Indtast Brugernavn og Password og klik "OK"

Når der er kommet en under Navn/Brugernavn, så klik "Næste" og "Udfør"

Bilag 5 – Serverdoc for DC01

Hostname:

DC01.GREENCLASS.local

Serverens formål:

Serveren fungerer som Domain Controller, hvor bl.a. vores AD, DNS og DHCP styres fra.

Serverens afhængighed:

Serveren er ikke som sådan afhængig nogen andre servere, dog så er den afhængig af at ISA01 kører da det er herfra at den får sin internet forbindelse. Internet forbindelsen er vigtig, da det er via den at DC01's får noget af dens DNS, da den bruger OpenDNS.

Serverinfo:

Servertype: IBM xSeries 330

Hardware:

- CPU: Intel Pentium III 1266MHz Dual
- RAM: 3GB
- Diske: 18,2GB x 2 (RAID 1)

Netværk:

Netkort:

- IP-adresse: 10.0.5.3
- Maske: 255.255.255.0
- Gateway: 10.0.5.1
- DNS-Server: 127.0.0.1

Operativ System:

Windows Server 2003 Enterprise, 32 bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- DHCP
- DNS
- Domain Controller (Active Directory)
- WINS

Software:

Software der er installeret ud over OS:

- avast! Antivirus Server edition
-

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- RDP (3389)
- DNS

Bilag 6 – Serverdoc for ISA01

Hostname:

ISA01.GREENCLASS.local

Serverens formål:

Serveren fungerer som Firewall, cacheserver, VPN.

Serverens afhængighed:

Serveren er ikke afhængig af andre servere.

Serverinfo:

Servertype: IBM xSeries 330

Hardware:

- CPU: Intel Pentium III Dual 1133MHz
- RAM: 3GB
- Diske: 18,2GB x 2 (RAID 1)

Netværk:

Netkort: (DMZ)

- IP-adresse: 172.16.1.1
- Maske: 255.255.255.0
- Gateway:
- DNS-Server:

Netkort: (WAN)

- IP-adresse: 192.168.1.10
- Maske: 255.255.255.0
- Gateway: 192.168.1.1
- DNS-Server: 10.0.5.3

Netkort: (LAN)

- IP-adresse: 10.0.1.1
- Maske: 255.255.255.0
- Gateway:
- DNS-Server:

Route:

10.0.0.0 /16 sendes til 10.0.1.11

Lavet med: ROUTE -p ADD 10.0.0.0 MASK 255.255.0.0 10.0.1.11

Operativ System:

Windows Server 2003 Enterprise, 32 bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Remote Access / VPN Server

Software:

Software der er installeret ud over OS:

- avast! Antivirus
- ISA 2006

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping (10.0.1.1 (LAN))
- Ping (172.16.1.1(DMZ))
- Ping (192.168.1.10 (WAN))
- RDP (10.0.1.1 (LAN))
- RDP (172.16.1.1(DMZ))
- RDP (192.168.1.10 (WAN))

Bilag 7 – Serverdoc for FS01

Hostname:

FS01.GREENCLASS.local

Serverens formål:

Serveren fungerer som Filserver.

Serverens afhængighed:

Serveren er afhængig af ISA01 og DC01.

Serverinfo:

Servertype: IBM xSeries 330

Hardware:

- CPU: Intel Pentium III 1266MHz Dual
- RAM: 3GB
- Diske: 36GB x 2 (RAID 1)

Netværk:

Netkort:

- IP-adresse: 10.0.5.5
- Maske: 255.255.255.0
- Gateway: 10.0.5.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2003 Enterprise, 32 bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Fileserver

Software:

Software der er installeret ud over OS:

- avast! Antivirus

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- RDP (3389)

Bilag 8 – Serverdoc for WUP01

Hostname:

WUP01.GREENCLASS.local

Serverens formål:

Serveren fungerer som overvågningsserver.

Serverens afhængighed:

Serveren er afhængig af ISA01 og Exchange server for at kunne sende mails.

Serverinfo:

Servertype: IBM xSeries 330

Hardware:

- CPU: Intel Pentium III 930MHz
- RAM: 1GB
- Diske: 2 x 18,2GB (RAID 1)

Netværk:

Netkort:

- IP-adresse: 10.0.5.11
- Maske: 255.255.255.0
- Gateway: 10.0.5.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2003 Enterprise, 32 bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Ingen roller.

Software:

Software der er installeret ud over OS:

- avast! Antivirus server edition
- Ipswitch Whatsup Gold v.14.1

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Denne server bliver af gode grunde ikke overvåget, da det ikke giver meget mening at overvåge sig selv.

WWW.BLOGGT.DK

Bilag 9 – Serverdoc for ESX01

Hostname:

ESX01.GREENCLASS.local

Serverens formål:

Serveren fungerer som VMware ESX 4.0 server, og bruges som host til de virtuelle maskiner.

Serverens afhængighed:

Serveren er afhængig af ISA01.

Serverinfo:

Servertype:

Hardware:

- CPU: AMD Phenom (TM) II X4 905e 2,499GHz
- RAM: 4GB
- Diske: 231,50 GB

Netværk:

Netkort:

- IP-adresse: 172.16.1.10
- Maske: 255.255.255.0
- Gateway: 172.16.1.1
- DNS-Server: 10.0.5.3

Operativ System:

VMware ESX 4.0

Software:

Software der er installeret ud over OS:

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- RDP (3389)

Bilag 10 – Serverdoc for vCenter

Hostname:

vcenter.GREENCLASS.local

Serverens formål:

Serveren fungerer som til at hoste vCenter server, som kommer med ESX 4.0.

Serverens afhængighed:

Serveren er afhængig af ESX01 og ISA01.

Serverinfo:

Servertype: IBM xSeries 330

Hardware:

- CPU: Intel Pentium III Dual 1266MHz
- RAM: 3GB
- Diske: 18,2GB x 2 (RAID 1)

Netværk:

Netkort:

- IP-adresse: 10.0.5.10
- Maske: 255.255.255.0
- Gateway: 10.0.5.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2003 Enterprise, 32 bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Ingen roller

Software:

Software der er installeret ud over OS:

- avast! Antivirus
- vCenter fra VMware

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- RDP (3389)
- Ping

WWW.BLOGGT.AK

Bilag 11 – Serverdoc for WEB01

Hostname:

WEB01.GREENCLASS.local

Serverens formål:

Serveren fungerer som Webserver

Serverens afhængighed:

Serveren er afhængig af

Serverinfo:

Servertype: Virtuel

Hardware:

- CPU: AMD Phenom (TM) II X4 905e
- RAM: 1GB
- Diske: 16GB

Netværk:

Netkort:

- IP-adresse: 172.16.1.3
- Maske: 255.255.255.0
- Gateway: 172.16.1.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2003 Enterprise, 64 bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Ingen roller

Software:

Software der er installeret ud over OS:

- avast! Antivirus
- Microsoft Web Platform Installer 2.0
- WampServer 2.0
- PHP 5.2.11

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- http
- http af intranet
- http af doku
- http af www

Bilag 12 – Serverdoc for Exchange

Hostname:

Exchange.GREENCLASS.local

Serverens formål:

Serveren fungerer som Mailserver, via Exchange 2007

Serverens afhængighed:

Serveren er afhængig af ESX01, DC01 og ISA01.

Serverinfo:

Servertype: Virtuel

Hardware:

- CPU: AMD Phenom (TM) II X4 905e
- RAM: 1GB
- Diske: 20GB

Netværk:

Netkort:

- IP-adresse: 172.16.1.8
- Maske: 255.255.255.0
- Gateway: 172.16.1.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2008 Enterprise, 32bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Ingen roller

Software:

Software der er installeret ud over OS:

- avast! Antivirus
- Microsoft Exchange Server 2007

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- http
- HTTPS
- RDP
- SMTP

Bilag 13 – Serverdoc for TS01

Hostname:

TS01.GREENCLASS.local

Serverens formål:

Serveren fungerer som Terminal server.

Serverens afhængighed:

Serveren er afhængig af ESX01, DC01 og ISA01.

Serverinfo:

Servertype: Virtuel

Hardware:

- CPU: AMD Phenom(tm) II X4 905e
- RAM: 512 MB
- Diske: 20 GB

Netværk:

Netkort:

- IP-adresse: 172.16.1.5
- Maske: 255.255.255.0
- Gateway: 172.16.1.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2008 Enterprise, 32 bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Terminal Server

Software:

Software der er installeret ud over OS:

- avast! Antivirus
- Microsoft Office 2007 Enterprise

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- RDP (3389)

Bilag 14 – Serverdoc for TS02

Hostname:

TS02.GREENCLASS.local

Serverens formål:

Serveren fungerer som Terminal Server.

Serverens afhængighed:

Serveren er afhængig af ESX01, DC01 og ISA01.

Serverinfo:

Servertype: Virtuel

Hardware:

- CPU: AMD Phentom (tm) II X4 905e
- RAM: 512 MB
- Diske: 20 GB

Netværk:

Netkort:

- IP-adresse: 172.16.1.6
- Maske: 255.255.255.0
- Gateway: 172.16.1.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2008 Enterprise, 32bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Terminal Server

Software:

Software der er installeret ud over OS:

- avast! Antivirus
- Microsoft Office 2007 Enterprise

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- RDP (3389)

WWW.BLOGGT.AK

Bilag 15 – Serverdoc for TSSB

Hostname:

TSSB.GREENCLASS.local

Serverens formål:

Serveren fungerer som...

Serverens afhængighed:

Serveren er afhængig af

Serverinfo:

Servertype:

Hardware:

- CPU: AMD Phenom (TM) II X4 905e
- RAM: 512 MB
- Diske: 20GB

Netværk:

Netkort:

- IP-adresse: 172.16.1.4
- Maske: 255.255.255.0
- Gateway: 172.16.1.1
- DNS-Server: 10.0.5.3

Operativ System:

Windows Server 2008 Enterprise Service Pack 1, 32bit

Server rolle(r):

Roller som er blevet tilføjet ud over standard:

- Terminal Server (Session Broker)

Software:

Software der er installeret ud over OS:

- avast! Antivirus
-

Windows update:

Serveren bliver holdt opdateret via vores FS01, som også fungerer som WSUS server. Disse opdateringer bliver installeret kl. 03:00

Overvågning:

Overvågningen holder øje med om evt. porte ikke svare korrekt tilbage, 24-7-365, minus der hvor serveren er i servicevindue.

Servicevindue:

Et servicevindue er der hvor serveren ikke bliver overvåget, dvs. det er her man kan lave ændringer, installer opdateringer eller på anden vis lave ting på serveren uden der kommer alarmer.

Der er servicevindue mellem kl. 16:00 og 08:00.

Følgende ting overvåges:

- Ping
- RDP (3389)

WWW.BLOGGT.AK

Bilag 16 - Local administrator passwords

GreenClassAP	
Brugernavn	Kodeord
Administrator	dataitdatait

ISA01	
Brugernavn	Kodeord
Administrator	datait

DC01	
Brugernavn	Kodeord
Administrator	datait

FS01	
Brugernavn	Kodeord
Administrator	datait

WEB01	
Brugernavn	Kodeord
Administrator	datait

vCenter01	
Brugernavn	Kodeord
Administrator	datait

TS XX / Exchange	
Brugernavn	Kodeord
Administrator	Datait123

Switche	
Brugernavn	Kodeord
(Intet)	dataitdatait

WUP01	
Brugernavn	Kodeord
Administrator	datait

ESX01	
Brugernavn	Kodeord
root	dataitdatait