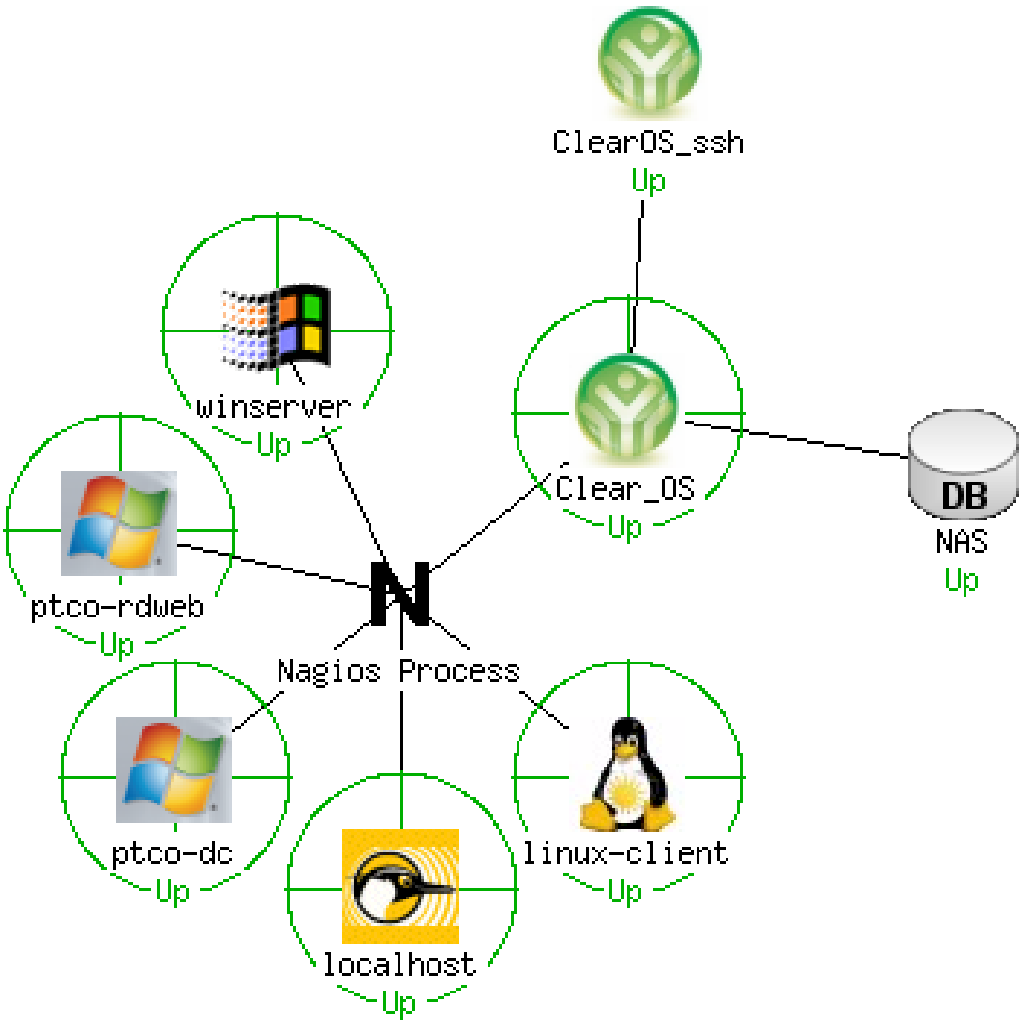


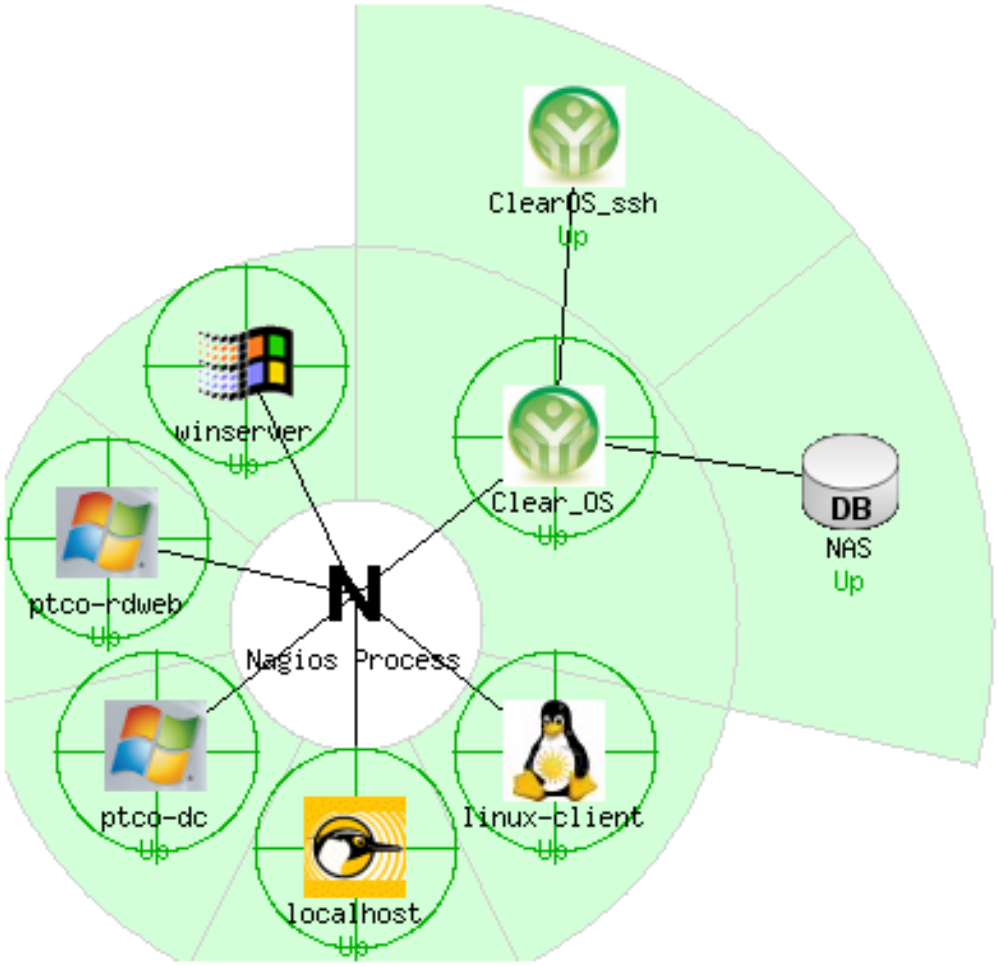
C-Proef

Dedicated servers beheren en monitoren

onder Windows Server 2008 R2 en Linux Servers

Pascal Kinoo – Tony De Baets
Schooljaar 2011-2012

Syntra Midden-Vlaanderen
Hogekouter 1
9100 Sint-Niklaas



C-Proef

Dedicated servers beheren en monitoren

onder Windows Server 2008 R2 en Linux Servers

Pascal Kinoo – Tony De Baets

Schooljaar 2011-2012

1 Intro

In de fictieve opzet van onze C-proef voorzien we een imaginaire KMO van virtuele servers gemonitord doorheen een tijdelijk netwerk. Dit is de eerste stap die twee ambitieuze netwerkbeheerders doorlopen om een voeling te hebben met de praktijk.

Heeft onze C-proef, tijdens de moordende mondelinge verdediging, de kritische Syntra-jury kunnen overtuigen van de maturiteit die we ambiëren dan lezen we binnen enkele maanden in het vakblad 'Ondernemend Vlaanderen': Twee ambitieuze Syntra afgestudeerde netwerkbeheerders voorzien een bloeiende KMO van performante servers werkende op een stabiel en een redundant netwerk.

Dit moet toch de vrucht, het succes en de apotheose zijn van drie jaar verrijkende netwerkbeheerders opleiding bij Syntra Sint-Niklaas.

In onze C-Proef voorzien we een KMO van verschillende servers die allen een dedicated taken op zich nemen, een LAN netwerk waarbij alles met elkaar lokaal wordt verbonden. Via een ClearOS server wordt op een gecontroleerde manier het netwerk met de buitenwereld opengezet en hij fungeert tevens als DHCP server.

We gaan ervan uit dat onze eindklant zelf niets zal ondernemen om het geheel te superviseren en laat staan dat hij bij averij persoonlijk zou ingrijpen. Als service, die commercieel werd opgenomen in een jaarlijks preventief en curatief onderhoudscontract, nemen we die taak op ons. Een Nagios monitoring server overwaakt het geheel. Controleert of alles normaal blijft werken of er geen kritische waardes worden bereikt. Beeld je in dat de bedrijfleider je om 7.00 uit je bed belt om te zeggen dat de applicatie server platligt. Hierdoor treedt onherroepelijk werkverlet op voor gans het bedrijf want de externe techniekers kunnen hun planning niet consulteren. De boekhouder kan niet facturen. De verkoopsdienst kan geen offertes uitwerken. En toch had je die pijnlijke telefoonoproep kunnen vermijden. Hadden we de storage drempels correct ingesteld, zouden we een week geleden via mail zijn ingelicht dat de opslagcapaciteit van de applicatieserver de meest kritische drempel van 10% vrij ruimte had bereikt. Dan had je zelf naar de CEO kunnen bellen met het bericht: 'Ik zie dat je opslagcapaciteit een kritische drempel overschreden heeft' of nog 'Dat een HD van de RAID50 storage de mist is ingegaan'. Dan had de CEO zich de geruststellende opmerking gemaakt dat het onderhoudscontract hem de service verleent die hem beloofd werd. Een betere reclame als startende ondernemer kan je je niet inbeelden.

We voorzien een Windows Domain Controller die de rechten van ieder gebruiker binnen onze KMO beheert. Een Terminal Server zal alle ondersteuning verlenen aan de verkoopsdienst. Een goeie venter is voornamelijk op baan om zijn producten aan de man prijzen. Vanop afstand moet hij de mogelijkheid hebben om de dagprijzen te consulteren of offertes uit te werken. Zijn uitgewerkte offerte zijn verbonden met het bedrijfs-NRP pakket. Een offerte wordt onmiddellijk gecontroleerd met de stockvoorraden, aankooptoeleveringen en beloofde levertermijnen.

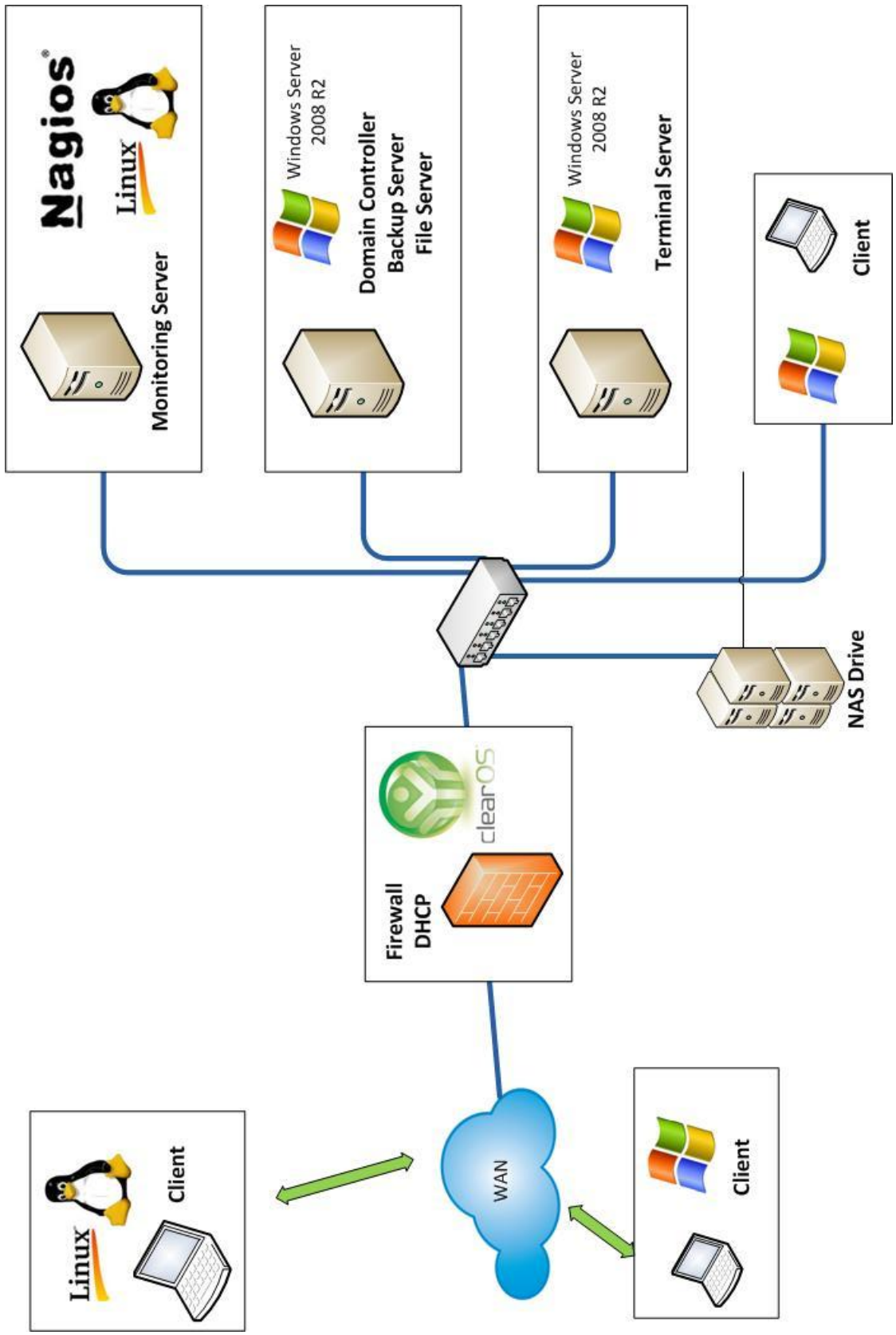
Daarnaast hebben we een backup server die zich in het domein bevindt. In de praktijk zou het niet onverstandig zijn dat die zich op een andere locatie te zetten en zou bereikbaar zijn via VPN tunnel. Mocht er zich lokaal problemen voordoen in onze KMO dan is de backup-server op een andere locatie hiervan vrijwaard. Ik denk bijvoorbeeld aan brand- of waterschade.

Onze C-proef is op labo-schaal uitgewerkt met de interpolatie dat hij evengoed op echte servers kan draaien.

Een werk - en dus ook onze C-proef - is een levend project. Het is steeds vatbaar voor verbeteringen en dit hebben we ook ervaren bij het uitwerken van deze taak. Zouden we niet beter dit zo doen? Dit zou ook nog anders kunnen. Maar dead-lines zijn de boosdoeners. Je dient met compromissen leven. We hebben voldoening van ons afgewerkt product zonder de pretentie te hebben dat het niet voor verbetering vatbaar is.

2 Inhoudstabel

3 Samenvatting



Hierboven vind je de topologie van onze C-proef. De verschillende deelnemers nemen een specifieke taak op zich. Het was niet mogelijk om voor iedere server of client een aparte fysieke machine te gebruiken. Hierdoor hebben we op onze biede PC's de verschillende servers virtueel verdeeld. De rechtse machines (Nagios monitoring Server, Windows Domain Controller, Windows Terminal Server en Windows client) draaien virtueel. De Clear OS Server die fungeert als Firewall en DHCP hebben we op een computer van Syntra gezet. Dit had het grote voordeel dat we apart onze opzet verder konden uitwerken. En als we bij Syntra samenkwamen konden we onze nieuwe aanpassingen 'in real time' uitproberen.

De Clear OS gebruiken we als Firewall voor de communicatie met de buitenwereld. Op een gebruiksvriendelijke manier kunnen we poorten, tijdstippen, inkomende en uitgaand verkeer controleren en beperken. Daarnaast gebruiken we de Clear OS als DHCP server. We hebben in ons imaginaire KMO het LAN netwerk in de range 10.10.10.0/24 vastgelegd.

De twee Windows servers zijn de bouwstenen van onze KMO. De Domain Controller neemt het beheer van alle rechten voor iedere gebruiker op zich. Het idee is dat ieder gebruiker werkt vanop zijn PC aangesloten op het domein. De DC zal het aanloggen van de gebruiker op zich nemen en de toegang tot de Remote Desktop server programma's beheren. De Remote Desktop server is een aparte server. De Remote Desktop server zal voor iedere gebruiker in het domein een nieuwe sessie op zich nemen. De CPU load wordt zo mooi bijgehouden en bijgestuurd indien nodig.

Alle data wordt in de File Server gecentraliseerd. Dit heeft het voordeel dat alle gegevens gegroepeerd blijven en enkel beschikbaar zijn voor de bevoegden personen. Het nemen van back-ups kan eveneens eenvoudig gebeuren daar alle gegevens gecentraliseerd zijn.

We hebben veel aandacht gelegd in het monitoren van het systeem. Dit had een dubbel voordeel. Het liet ons toe om een visueel beeld te krijgen van het geheel. Is een gebruiker nog actief en bereikbaar? Is er nog communicatie onderling? Maar het ander voordeel was dat we voeling kregen met verschillende communicatie protocollen overheen het TCP/IP netwerk. De mogelijkheden van Nagios zijn onbeperkt. Het was een uitdaging om de verschillende mogelijkheden uit te proberen en productief te reproduceren.

4 TCP/IP

4.1 Wat?

TCP/IP is een verzamelnaam voor de reeks netwerkprotocollen die voor een grote meerderheid van de netwerkcommunicatie tussen computers instaan. Het internet is het grootste en bekendste TCP/IP-netwerk. De naam TCP/IP is een samentrekking van de twee bekendste protocollen die deel uit maken van de TCP/IP-protocol*stack* (= protocol*stapel*): het Transmission Control Protocol (TCP) en het internetprotocol (IP). TCP/IP wordt uitgesproken als "TCP over IP" of meestal *"tiesiepie ajpie"*.

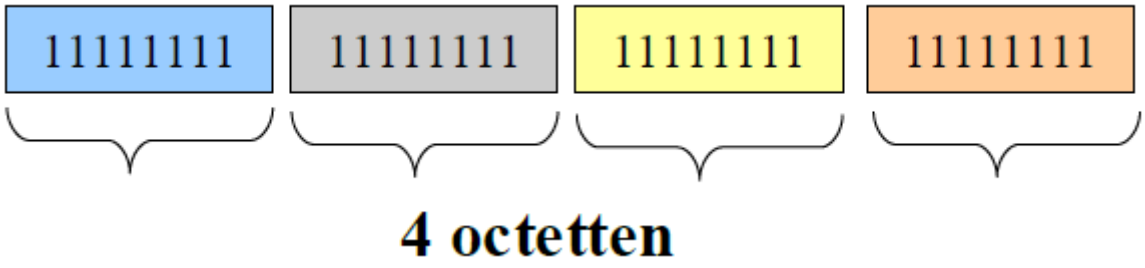
Waarom gebruiken we TCP/IP?

- Het is Routable.
- Bedrijfszeker. Het is ontworpen om te kunnen weerstaan aan het uitvallen van communicatielijnen in oorlogssituatie.
- Gemakkelijk uitbreidbaar

4.2 TCP/IP-adressering

4.2.1 IP-adressen

IP-adressen bestaan uit 4 octetten. Een octet is een byte, of te wel 8 bits. Een bit kan de waarde 1 of 0 hebben, en is dus binair (bi = 2, 2 waarden).



4.2.2 Binair naar decimaal

Om binair te kunnen rekenen, en visa versa, heb je deze reeks nodig:

.	.	.	.	.	.	.	.
128	64	32	16	8	4	2	1

Staat er een bit op 1 dan wordt de decimale waarde gebruikt. Staat een bit op 0 dan is de decimale waarde 0.

1	1	1	0	0	0	1	1
128	64	32	16	8	4	2	1

128+64+32+0+0+0+2+1 = 227

4.2.3 Decimaal naar binair

De binaire waarde van 189 kan als volgt worden gevonden. Begin bij de high-order bit (het eerste bit in het octet). Als je 128 uit het getal kan halen, zet je dit bit op 1. Als het niet kan zet je hem op 0. Kan het, dan trek je 128 van het getal af, en kijk je of 64 uit het getal gehaald kan worden. Kan dit, dan wordt dit bit 1, anders 0. Dus:

Bijvoorbeeld het getal 189:

Is 189 groter dan 128, dan moet de eerste bit op 1 (anders 0) staan.

1							
128	64	32	16	8	4	2	1

189 – 128 = 61

Is 61 groter dan 64, dan tweede bit op 1 (anders 0)

Is 61 groter dan 32, dan derde bit op 1 (anders 0)

1	0	1					
128	64	32	16	8	4	2	1

61 – 32 = 29

1	0	1	1				
128	64	32	16	8	4	2	1

29 – 16 = 13

1	0	1	1	1			
128	64	32	16	8	4	2	1

13 – 8 = 5

1	0	1	1	1	1		
128	64	32	16	8	4	2	1

5 – 4 = 1
1 gaat niet in 2 dus de zevende bit staat op 0

1	0	1	1	1	1	0	1
128	64	32	16	8	4	2	1

1 – 1 = 0

Resultaat: 10111101

4.2.4 Klassenverdeling

IP-adressen zijn verdeeld in 3 classes:

Bij een A-class adres mogen de laatste 3 octetten vrij benoemd worden (de host-id = X, Y en Z). De eerste staat vast (het network-id = W).

W X Y Z

Bij een B-class adres mogen de laatste 2 octetten vrij benoemd worden (de host-id = Y en Z). De eerste 2 staan vast (het network-id = W en X).

W **X** Y Z

Bij een C-class adres mogen de laatste octet vrij benoemd worden (de host-id = Z). De eerste 3 staan vast (het network-id = W, X en Y).

W **X** **Y** Z

Het aantal mogelijkheden is zeer groot. Aangezien een bot 2 mogelijkheden heeft, is het totaal aantal mogelijkheden gelijk aan 2^x. Waarbij ^{x} het aantal beschikbare bits is.

Bij een A-class adres heb je:

a. 1 octet voor het network-id, dus 8 bits. Aantal mogelijke netten is dan 2^8 , dus 256
b. 3 octet voor de host-id, dus 24 bits. Aantal hosts pet net is dan 2^{24}, dus 16 777 216

Bij een B-class adres heb je:

a. 2 octet voor het network-id, dus 16 bits. Aantal mogelijke netten is dan 2^{16}, dus 65 536
b. 2 octet voor de host-id, dus 16 bits. Aantal hosts per net is dan 2^{16}, dus 65 536

Bij een C-class adres heb je:

a. 1 octet voor het network-id, dus 24 bits. Aantal mogelijke netten is dan 2^{24}, dus 16 777 216
b. 3 octet voor de host-id, dus 8 bits. Aantal hosts per net is dan 2^8, dus 256

4.2.5 Regels van klassen

4.2.5.1 Regel 1

Bij een A-class adres moet de high-order bit (het eerste bitje) van octet **W** op 0 staan. Dus in plaats van 8 bits, houdt je er maar 7 over voor het network-id. Aantal mogelijke netten is dus 2^7, dus 128. De network-id's lopen dus van 00000000 t/m 01111111. Decimaal is dat 0 t/m 127.

Bij een B-class adres moeten de 2 high-order bits (de eerste 2 bitjes) van octet **W** op 10 staan. Dus in plaats van 16 bits, houdt je er maar 14 over voor het network-id. Aantal mogelijke netten is dan 2^{14}, dus 1638. De network-id's lopen dus van 10000000 t/m 10111111. Decimaal is dat 128 t/m 191.

Bij een C-class adres moeten de 3 high-order bits (de eerste 3 bitjes) van octet **W** op 110 staan. Dus in plaats van 24 bits, houdt je er maar 21 over voor het network-id. Aantal mogelijke netten is dan 2^{21}, dus 2 097 152. De network-id's lopen dus van 11000000 t/m 11011111. Decimaal is dat 192 t/m 223.

4.2.5.2 Regel 2

De vrije bits in het network-id van class A, B of C adres mogen nooit alleen maar de waarde 1 of de waarde 0 hebben.

Bij een A-class gaat dit als volgt:

FOUT	GOED
0**000000** = 0	0**0000001** = 1
0**1111111** = 127	0**1111110** = 126

Bij een B-class gaat dit als volgt:

FOUT	GOED
10**000000.00000000** = 128.0	10**000000.00000001** = 128.1
10**111111.11111111** = 191.255	10**111111.11111110** = 191.254

Bij een C-class gaat dit als volgt:

FOUT	GOED
110**00000.00000000.00000000** = 192.0.0	110**00000.00000000.00000001** = 192.0.1
110**11111.11111111.11111111** = 224.255.255	110**11111.11111111.11111110** = 224.255.254

Toch wordt de range 127.0.01 t/m 127.255.255.254 gebruikt, en wel voor TCP/IP test doeleinden (zoals 127.0.0.1 voor het testen van de localhost).

Ook zijn er een aantal Private Network Ranges, die niet op het internet gebruikt worden en die intern zonder problemen gebruikt kunnen worden. Genaamd de niet routable ip adressen.
Voor de A-class is dit 10.0.0.0 t/m 10.255.255.255
Voor de B-class is dit 172.16.0.0 t/m 172.31.255.255
Voor de C-class is dit 192.168.0.0 t/m 192.168.255.255

4.2.6 IP class overview

Klasse	1° octet	Aantal Ranges	Aantal Hosts	Aantal Networks
A-klasse	0xxx xxxx	0 tot 127	16 777 214	126
B-klasse	10xx xxxx	128 tot 191	65 534	16 384
C-klasse	110x xxxx	192 tot 223	254	2 097 152

4.2.7 AND-ing

AND-ing is de term die gebruikt wordt voor het bepalen of een ip-packet binnen het eigen segment/subnet moet worden afgeleverd, of doorgetrapt moet worden naar een andere segment/subnet. AND-ing gaat als volgt in het werk.

We hebben een *destination ip*-adres, een *source-ip* adres en een *subnetmask*.

Destination IP adres	131.107.2.200
Source IP adres	131.107.3.11
Subnetmask	255.255.255.0

Dit zijn de volgende binaire waarden.

Destination IP adres	10000011.01101011.00000010.11001000
Source IP adres	10000011.01101011.00000011.00001011
Subnetmask	11111111.11111111.11111111.00000000

AND-ing is het tegen over elkaar zetten van subnetmask en ip-adres.
Regels:
0 op 0 wordt 0
0 op 1 wordt 0
1 op 0 wordt 0
1 op 1 wordt 1

Destination IP adres	10000011.01101011.00000010.11001000
Subnetmask	11111111.11111111.11111111.00000000
Network IP adres	10000011.01101011.00000010.00000000
Network IP adres in decimalen	131.107.2.0

Source IP adres	10000011.01101011.00000011.00001011
Subnetmask	11111111.11111111.11111111.00000000
Network IP adres	10000011.01101011.00000011.00000000
Network IP adres in decimalen	131.107.3.0

De network-adressen zijn iet gelijk, de IP-packet moet naar een ander segment/subnet.

4.2.8 Subnetting

Bij normale IP-adressen horen de volgende subnetmasks bij de verschillende adres classes.

A-class	255.0.0.0
B-class	255.255.0.0
C-class	255.255.255.0

Overal waar 255 staat (zie AND-ing) wordt het network-id gemaskeerd. Zo is te zien of een packet lokaal of in een ander segment/subnet thuishoort. Bij subnetting pikken we alleen een bit (of meerdere) van de host-id en voegen deze bij het network-id. bij A-class adres bijvoorbeeld ziet het er als volgt uit:

11111111	1…….	……..	……..
W	X	Y	Z

Octet **W** is het network-id in een class A adres. We pakken nu een high-order bit van het **X** octet bij het network-id.

Het subnetmask wordt nu 255.128.0.0. Het **X** octet wordt nu als sunbetmask 128. We hebben nu als resultaat 1 range aan A adressen, verdeelt in 2 rangen. Het trucje hierbij is dat de decimale van het laatste bit wat aan staat in het **X** octet. 128 is.

1	.	.	.	.	.	.	.
128	64	32	16	8	4	2	1

Dit is de stapgrootte, de ruimte tussen begin en eind van de range. Dus de ranges lopen als volgt:

255.**0**.0.1 t/m 255.**127**.255.254
255.**128**.0.1 t/m 255.**255**.255.254

Aangezien het aantal opties 256 (0 t/m 255), lopen de ranges ook vanaf 0. Van 0 t/m 127 zijn 128 opties (de stapgrootte).

Maar omdat het subnetmask zelf al werkt met 1 en 255 (standaard), valt zowel de eerste als de tweede range af, omdat octet **X** geen 0 en 255 mag zijn. Dus subnetmask van 255.128.0.0 levert geen valide ranges op.

Dan gaan we een stapje verder. We pakken nu twee high-order (eerste 2 bits) van het **X** octet bij het network-id.

11111111	11……	……..	……..
W	X	Y	Z

Het subnetmask wordt nu 255.192.0.0. het **X** octet wordt nu als subnetmask 192. We hebben nu als resultaat 1 range aan class A adressen, verdeelt in 4 ranges. Als we weer het trucje toepassen, is de stapgrootte hier 64.

1	1	.	.	.	.	.	.
128	64	32	16	8	4	2	1

Dit is de stapgrootte, de ruimte tussen begin en eind adres van de range. Dus lopen de ranges als volgt:

255.**0**.0.1 t/m 255.**63**.255.254
255.**64**.0.1 t/m 255.**127**.255.254
255.**128**.0.1 t/m 255.**191**.255.254
255.**192**.0.1 t/m 255.**255**.255.254

Wederom valt zowel de eerste als de laatste range af, omdat octet **X** geen 0 of 255 mag zijn. Dus een subnetmask van 255.192.0.0 levert 2 valide ranges op.

Subnetting betekent altijd dat er adressen wegvallen. Maar hoe groter het aantal subnetten, hoe kleiner de ranges, dus hoe minder adressen wegvallen.

We hebben 4 subnetten, waarvan er 2 valide zijn. Het laatste bitje wat aangezet werd vertegenwoordigde de waarde 64. Dit is ook de stapgrootte. Met behulp hiervan kan je ook snel het aantal subnetten berekenen: 256/64 = 4. Hier moet je altijd 2 vanaf trekken, dus 2 subnetten.

Formule subnetten berekenen aan de hand van de stapgrootte:

(256/stapgrootte) – 2 = aantal subnetten

Het aantal hosts is te berekenen door te kijken naar het aantal bits wat beschikbaar blijft voor de host-id. In het voorbeeld zijn dit er 6. Dus 2^6, wat 64 maakt. Ook deze weer min 2 (geen 0, geen 255), en dus 62 hosts.

Als we de eerste 4 bits hadden aangezet hadden we de volgende gegevens gehad.

Subnetmask	255.240.0.0
Stapgrootte	16
Aantal subnets	(256/16) – 2 = 14
Aantal hosts	$2^4 – 2 = 14$

4.2.9 IP-subnetting overview

Subnetmask

Binair	Decimaal	Aantal subnets	Aantal Class A Hosts	Aantal Class B Hosts	Aantal Class C Hosts
10000000	128	Invalid	Invalid	Invalid	Invalid
11000000	192	2	4 194 302	16 382	62
11100000	224	6	2 097 150	4 190	30
11110000	240	14	1 048 574	4 094	14
11111000	248	30	524 286	2 046	6
11111100	252	62	262 142	1 022	2
11111110	254	126	131 070	510	Invalid
11111111	255	254	65 534	254	Invalid

subnets	2^1-2	2^2-2	2^3-2	2^4-2	2^5-2	2^6-2	2^7-2	2^8-2
	128	64	32	16	8	4	2	1

4.2.10 Waarom subnetting

Er zijn verschillende redenen om netwerken te verdelen in sunetten:

- Het gebruik van verschillende fysieke media zoals Ethernet, FDDI, Wan, enz…
- Voor beveiligingsdoeleinden: hosts op een ander subnet zijn niet zichtbaar.
- Bandbreedte: Door een aantal hosts te 'verplaatsen' naar een ander subnet kan op beide subnets de gemiddeld beschikbare bandbreedte meer evenredig worden verdeeld.

4.2.11 Machtsverheffing

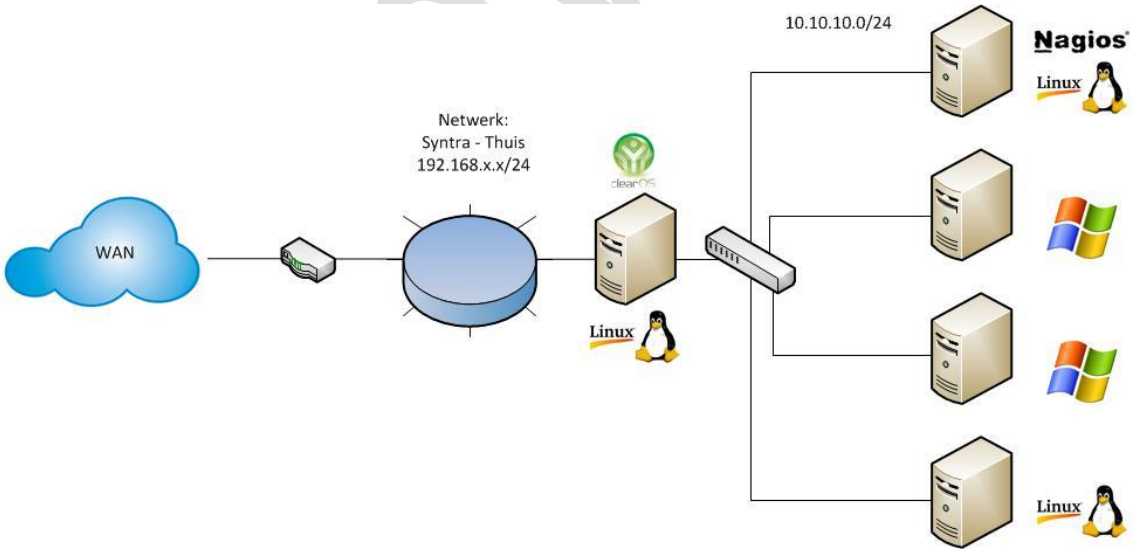
2^1	2
2^2	4
2^3	8
2^4	16
2^5	32
2^6	64
2^7	128
2^8	256
2^9	512
2^{10}	1 024
2^{11}	2 048
2^{12}	4 096
2^{13}	8 192
2^{14}	16 384
2^{15}	32 768
2^{16}	65 536
2^{17}	131 072
2^{18}	262 144
2^{19}	524 288
2^{20}	1 048 576
2^{21}	2 097 152
2^{22}	4 194 304
2^{23}	8 388 608
2^{24}	16 777 216

4.3 TCP/IP in onze C-Proef

De basisvraag die je je dient te stellen als je een LAN netwerk opzet is of je voor een klasse A, B of C netwerk kiest. In onze imaginaire KMO is het koffie dik kijken hoe het bedrijf in de toekomst zal evolueren. Voor een klasse C netwerk kiezen met de range 192.168.1.0 waarbij we 254 gebruikers zullen hebben, komt als een thuisnetwerkje over en zal niet bijdragen tot een positieve perceptie van professionalisme. We konden voor een klasse B netwerk opteren met de gebruikelijk IP-adressen 172.16.0.0 tot de range 172.31.255.255 wat ons een waaier van 1.048.576 IP-adressen geeft, verdeeld over 16 subnetten. Uiteindelijk hebben we toch voor een C klasse netwerk gekozen weliswaar met een A klasse uitstraling luisterende naar 10.10.10.0/24.

De keuze wordt gefungeerd door twee redenen. Ons virtueel netwerk heeft niet onmiddellijk toegang tot het WAN (zie illustratie). Op Syntra of thuis krijgt de Clear OS server een extern IP-adres van de DHCP server van het tweede netwerk. Voor thuis en Syntra zitten we in de range 192.168.x.x. Om duidelijk onze LAN te scheiden van het ander LAN netwerk hebben we andere IP adressen genomen om alle conflicten te vermijden en eenvoudig van thuis of vanuit Syntra onze applicatie te testen. Een twee reden is dat onze imaginaire KMO, die zoals alle florerende bedrijven in volle expansie is, kan migreren naar een groter netwerk en waarom niet van een A klasse. Lokaal verdeelt onze Clear OS – DHCP server IP adressen in 10.10.10.0/24. Zouden we in een groter geheel moeten werken dan kunnen we naar een prefix /16 of nog een /12 overgaan zonder hiervoor de IP adressen van de huidige gebruikers te moeten aanpassen.

We zijn gecharmeerd door de waaier aan mogelijkheden die Clear OS ons aanbied. In het volgend hoofdstuk wordt de installatie en het personaliseren van Clear OS voor onze C-proef toegelicht. Doch blijft een achtergrondkennis van routing belangrijk, zeker mocht iets niet werken en je wilt aan trouble shooting doen. Hierverder illustreer ik hoe onze applicatie zou werken mochten we het routen aan een klassieke linux server toevertrouwen zonder de Clear OS software te gebruiken.



In bovenstaand figuur vind je de opbouw van het totaal netwerkconcept. Als denkoefening werken we de routing van ons netwerk op de linux machines uit zonder gebruik te maken van een Clear OS server.

4.3.1 Welke routing is reeds geconfigureerd?

We bekijken op de Nagios server hoe de routing is geconfigureerd.

```
linux-357s:/home/pascal # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.10.0      *               255.255.255.0   U     0      0        0 eth0
loopback        *               255.0.0.0       U     0      0        0 lo
linux-357s:/home/pascal # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.10.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
```

4.3.2 Standaard Gateway instellen

We zien dat we zoals hierboven beschreven in de range 10.10.10.0/24 zitten. Maar om andere IP-adressen te bereiken buiten zijn standaard range wordt nog niets gerouteerd. We stellen een default gateway in langs waar we naar buiten kunnen. Ziehier de instellingen van de default gateway.

```
linux-357s:/home/pascal # route add default gw 10.10.10.120
linux-357s:/home/pascal # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.10.10.120    0.0.0.0         UG    0      0        0 eth0
10.10.10.0      *               255.255.255.0   U     0      0        0 eth0
loopback        *               255.0.0.0       U     0      0        0 lo
linux-357s:/home/pascal # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.10.120    0.0.0.0         UG    0      0        0 eth0
10.10.10.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
```

Voor alle andere IP adressen buiten ons subnet 10.10.10.0/24 gaan we via de linuxserver 10.10.10.120.

4.3.3 Instellingen van de routerende server

Dit zijn de instellingen op de routerende linux server. Hier gebruiken we uiteraard twee netwerkkaarten. Beiden met subnetmask 255.255.255.0

```
nagios-client:/home/pascal # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.10.0      *               255.255.255.0   U     0      0        0 eth1
loopback        *               255.0.0.0       U     0      0        0 lo
192.168.2.0     *               255.255.255.0   U     0      0        0 eth0
```

We bepalen de routerende functie

```
nagios-client:/home/pascal # route add -net 10.10.10.0/24 gw 10.10.10.120
```

```
nagios-client:/home/pascal # route add -net 192.168.2.0/24 gw 192.168.2.100
```

```
nagios-client:/home/pascal # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.10.0      10.10.10.120    255.255.255.0   UG    0      0        0 eth1
10.10.10.0      0.0.0.0         255.255.255.0   U     0      0        0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
192.168.2.0     192.168.2.100   255.255.255.0   UG    0      0        0 eth0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Beide netwerken kunnen elkaar bereiken.

5 ClearOS

5.1 Wat

ClearOS is een open bron firewall server gemaakt op basis van het Amerikaanse Redhat Enterprise Linux, een zeer robuust besturingssysteem. Zij hebben jarenlange ervaring opgebouwd als gespecialiseerd bedrijf in het ontwikkelen van server besturingssystemen voor netwerken. Linux is net zoals windows een besturingssysteem voor zowel servers als werkstations.
Linux ondersteunt ook windows netwerken. Het maakt net zoals windows gebruik van SMB (Service Message Block).

Waarom kiezen voor ClearOS?

In de eerste plaats voor zijn systeemeisen. Deze zijn aanmerkelijk lager dan de huidige Windows systeemeisen. Anderzijds door financiële overweging. ClearOS is open bron software applicatie wat wil zeggen dat de code wordt vrijgegeven. Dit geeft de gebruikers de mogelijkheid om de software te gebruiken aan te passen en te verbeteren. Clear Os blijft verder evolueren en wordt regelmatig aangepast. Het is hierdoor ook gratis te downloaden.
Bij sommige bedrijven moet je wel bij hun de software aankopen bij de aanschaf van een server. Maar bij die aankoop zit in de service de ondersteuning van de software en zijn configuratie.
Een derde argument is de stabiliteit. Uit ervaring blijkt dat Linux servers zeer stabiel draaien en zelden “gereset” hoeven te worden.
Als vierde het onderhoud. De systemen zijn zeer onderhoud arm en kunnen af met minder updates dan vergelijkbare producten.

ClearOS heeft volgende modules:

Windows file server, DHCP server, DNS server, print server, firewall, proxyserver, web content filtering systeem, bandbreedte beperking filter, IPSec VPN server, PPTP server, mail server, kolab server, web server, FTP server, SSH server, Back-up, MySQL database server en uitgebreide rapportage over het gebruik van het netwerk.

5.2 Benodigheden

De minimale vereisten zijn;
Basis hardware
CPU: tot 16 processors
RAM: Minimaal 512 MB
HDD: Minimaal 2 GB
Video kaart: Bijna alle video kaarten
Netwerkkaart: Een netwerkkaart is verplicht, twee voor gateway
Monitor, muis, toetsenbord: Enkel maar voor de installatie

Hardware vereisten

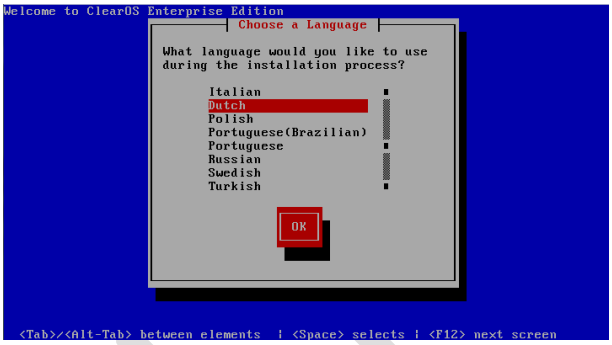
RAM / CPU	5 users	5 - 10 users	10 - 50 users	50 - 200 users
CPU	500 MHz	1 GHz	2 GHz	3 GHz
RAM	512 MB	1 GB	1,5 GB	2 GB

Hard Disk: Installatie en log heeft 1 GB nodig, optionele opslag is aan u.
RAID: Aanbevolen voor bedrijf kritische systemen.

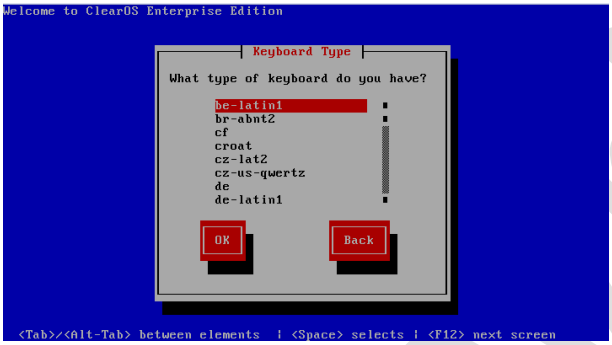
5.3 Installatie

We beginnen de installatie bij opstart van de machine met een ClearOS CD of indien we virtueel werken met een iso file.

Valideren om verder te gaan.

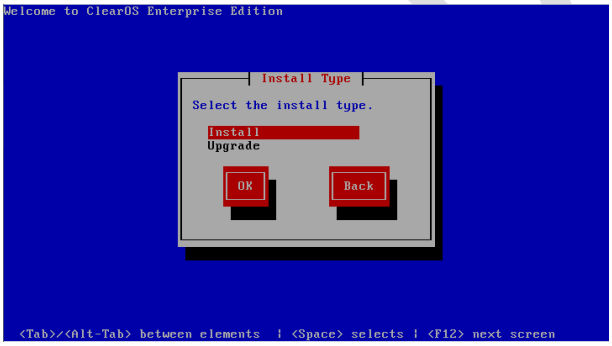


Taalkeuze.



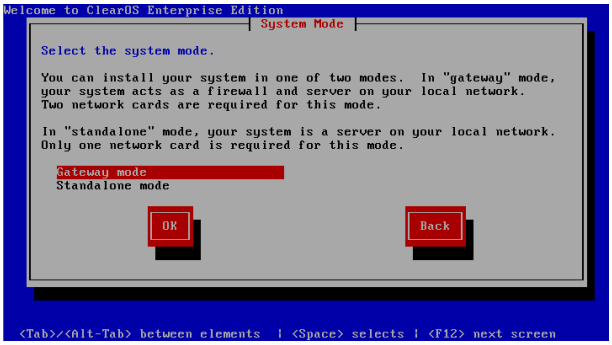
Kies het toetsenbord die je wenst te gebruiken

Kies installatie methode (meestal cd-rom).

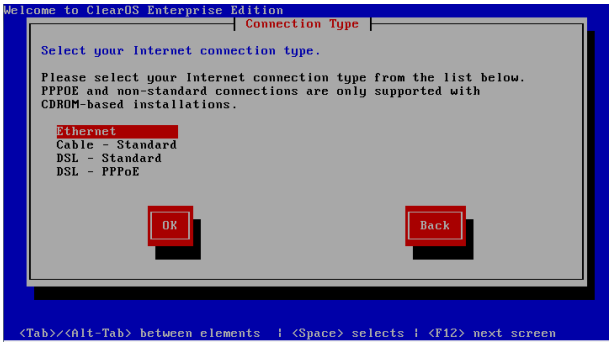


Selecteer het type installatie (meestal Install).

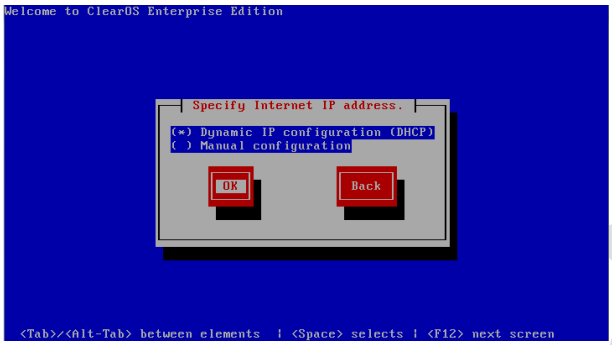
Typ ClearOS om verder te gaan en om alle harde schijven te verwijderen.



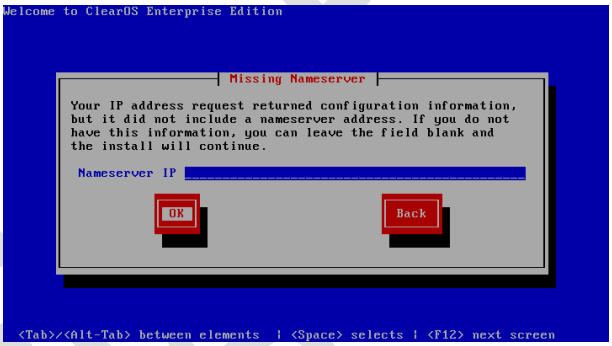
Kies Gateway mode (indien twee netwerkkaarten aanwezig).



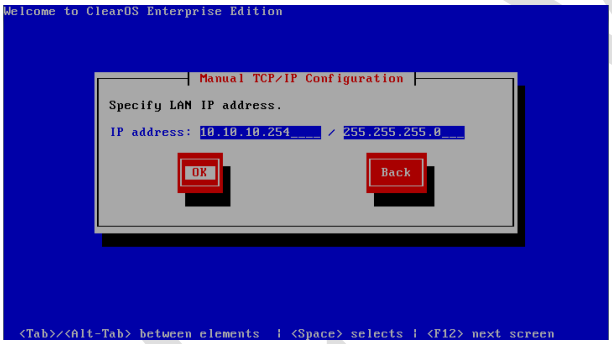
Selecteer het type netwerkverbinding (meestal Ethernet)



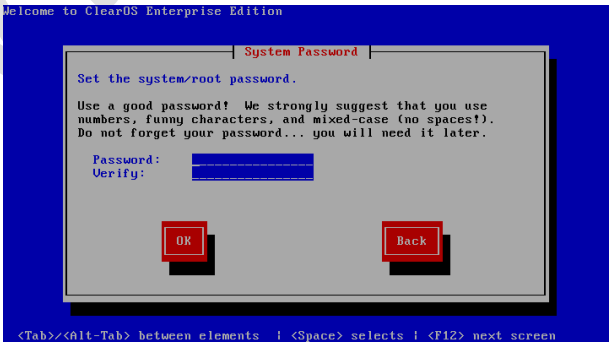
Geef internet IP adres, laat op standaard staan (DHCP) voor nu.



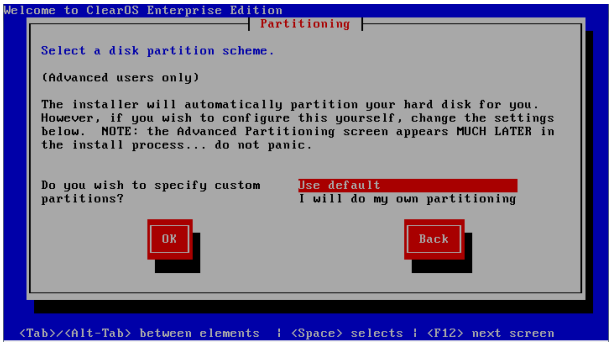
Laat momenteel de naamserver leeg.



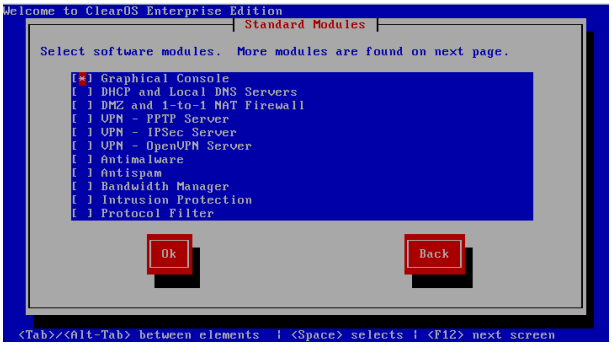
Geef LAN IP adres. Dit is je interne netwerk.



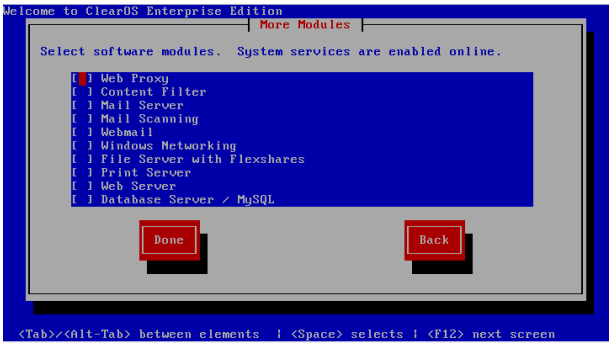
Voor een sterk systeemwachtwoord in.



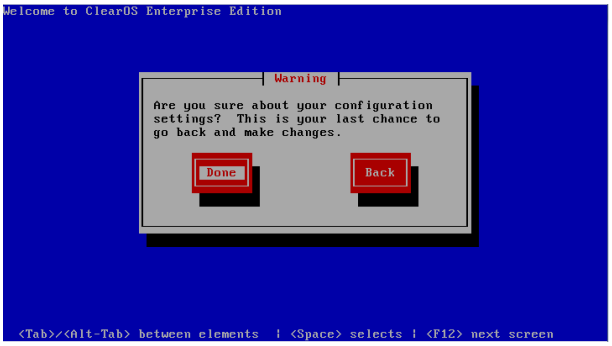
Gebruik de standaard partitie schema.



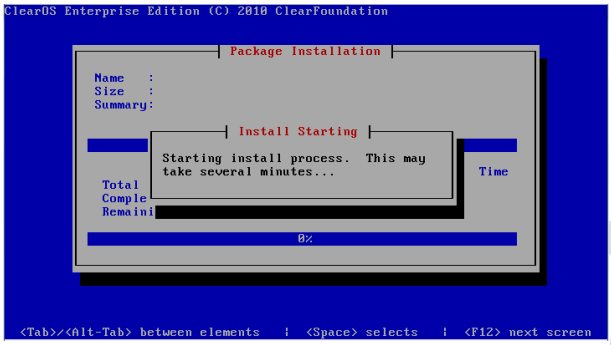
Kies ClearOS modules (vb. DHCP, …).



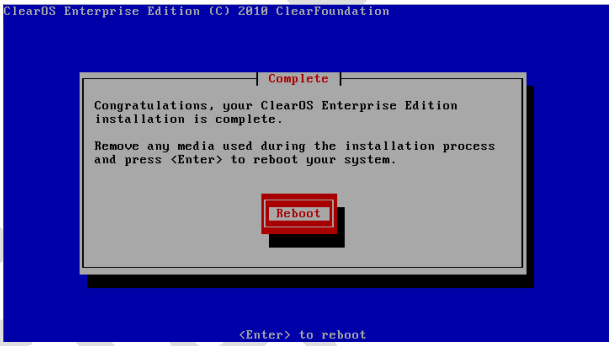
Kies meer modules (Web Server, MySQL, …)



Weet je het zeker? Klik op Done.



De installatie zal enkele minuten duren afhankelijk van uw module selectie.



Na afloop verwijder de cd / iso en Reboot.

Na de herstart krijg je volgend scherm.

5.4 Configuratie

Mocht je tijdens de installatie toch het verkeerde type of toetsenbord hebben gekozen dan kan je dit nog achteraf aanpassen. We gaan naar de Shell mode op CTRL+ALT+F2 drukken (F2-F6 command line terminals, F7 XWindow omgeving)

```
[root@system ~]# loadkeys be-latin1
Loading /lib/kbd/keymaps/i386/azerty/be-latin1.map.gz
[root@system ~]# vi /etc/sysconfig/keyboard _
```

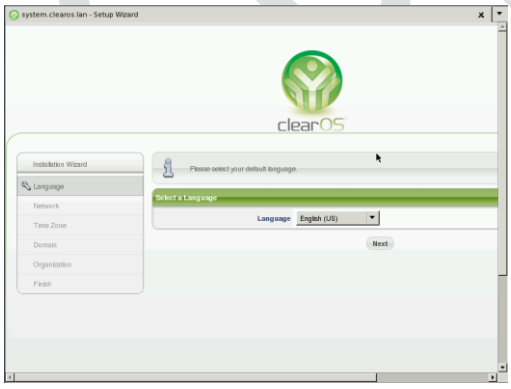
Typ “loadkeys be-latin1” waardoor het belgisch toetstenbord wordt geladen.
Om dit standaard te maken pas het bestand keyboard in “/etc/sysconfig” aan.

```
KEYBOARDTYPE="pc"
KEYTABLE="be-latin1"
~
~
~
~
~
~
```

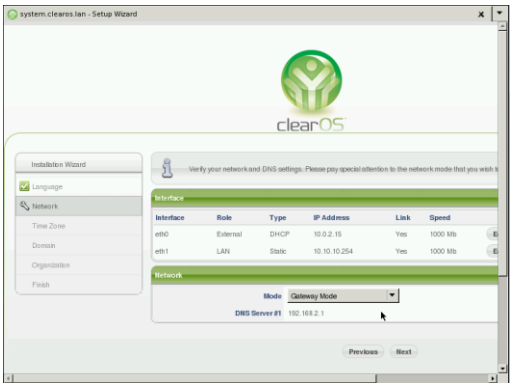
Achter KEYTABLE= verander je de “us” naar “be-latin1”

Als ClearOS een scherm en toetsenbord heeft dan kan je standalone inloggen.
Indien ClearOS geen scherm en toetsenbord heeft, dan dien je een computer in de range van Clear OS te zetten om hem via een webbrowser te bereiken. Via de webbrowser bepalen we de eerste configuratie en starten we de DHCP service.
Dit via volgend adres https://serveripaddress:81/
De ‘Secure Shell’ wordt automatisch bij aanvang mee geïnstalleerd. Hierdoor kan je ook vanaf een andere computer aan de command line.

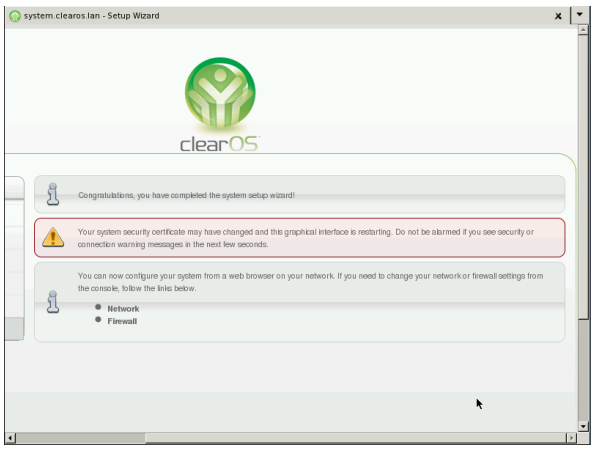
De eerste aanmelding.
Inloggen doe je met gebruiker ‘root’ en met het wachtwoord die je tijdens de installatie bepaalde.
Bij de eerste aanmelding moet je nog door een kleine configuratie heen.



Bepaal de taal.

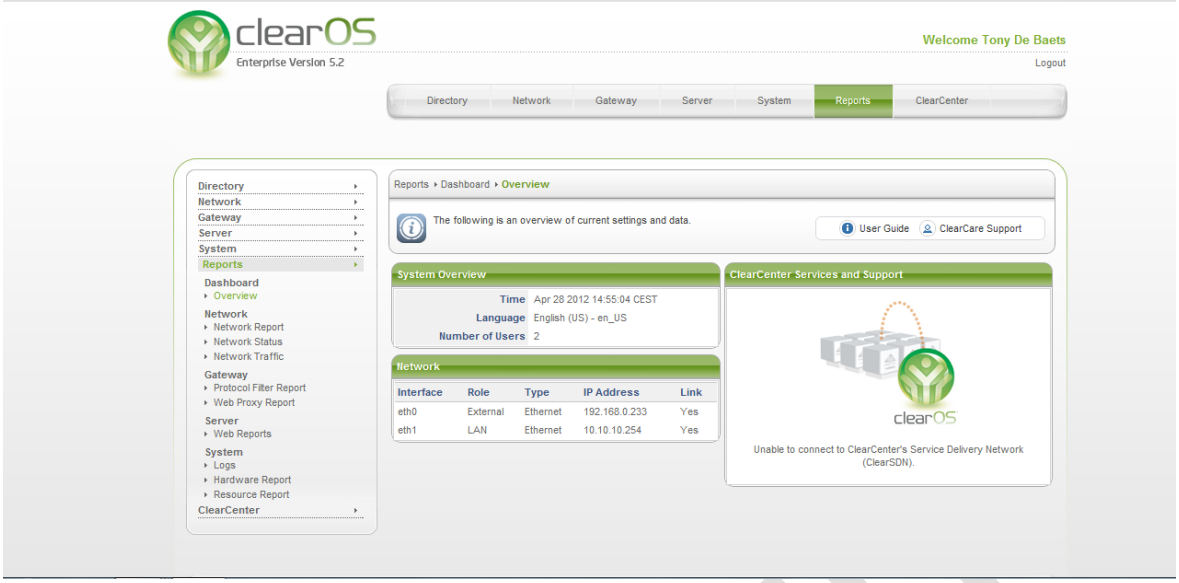


Network, bepaal Tijd Zone, domein en Organisatie

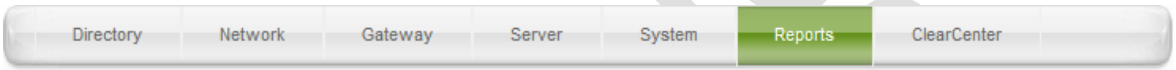


Aan het einde van de installatiewizard, raad ClearOS je aan om de configuratie voort te zetten met een standaard web browser. Dit voor elke desktop systeem in je domein.

5.4.1 Kleine rondleiding van de ClearOS



Bij inloggen kom je op de “Dashboard” pagina en heb je een overzicht van je system en krijg je een netwerk overzicht.



Boven aan de pagina vind je dan verschillende onderdelen terug.

Directory:	Configuratie van gebruikers, Domein en LDAP
Network:	Netwerkinstellingen (DHCP, DNS), Firewall en VPN
Gateway:	Antimalware, Bandwidth, protocol filter, Proxy en Filtering
Server:	File en Print, Mail, Web en MySQL
System:	Settings, Hardware, Security en Backup
Reports:	Rapporten over Netwerk, gateway, server en system
ClearCenter:	Extra modules installeren of updaten.

5.4.2 Netwerk configuratie.

Ga naar *Netwerk > Settings > Ip settings*.

Hier configureer je je netwerk, hostnaam en DNS-servers.
Via Interface kies je de gewenste kaart en druk je op 'edit'.
We hebben de mogelijkheid op volgende zaken te kiezen zoals LAN, hot LAN, Extern of DMZ.
Bij type selecteer je Statisch of DHCP, indien je van je ISP een vast IP adres krijgt of niet.
Voor ons labo-model zetten wij de eerste kaart op Extern en DHCP.
De tweede kaart komt op LAN en Statisch, geef ook een IP adres mee. Dit is onze interne netwerkkaart.

De verschillende modes zijn;

Standalone (geen firewall)	*standalone server zonder een firewall (vb. fileserver).
Standalone	*standalone server met firewall (vb. publieke web server).
Gateway Mode	*voor het aansluiten van u LAN, DMZ op het internet.

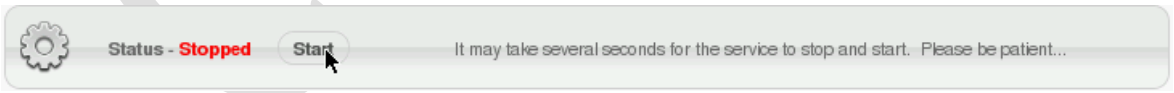
Host naam;
Een host naam is de volledige naam van uw systeem. Als je een eigen domein hebt, kunt u gebruik maken van een host naam, zoals gateway.ikke.be, mail.ikke.be

Naam/DNS Servers;
Als je de externe netwerkkaart op DHCP zet, zal de DNS-servers automatisch worden geconfigureerd.
Noot: Wegens wij ook een windows Domein controller gaan gebruiken en er voor kiezen om onze ClearOS niet in het domein te steken. Gaan we hier later nog het DNS adres meegeven van de domein controller. Zo kunnen we ook aan de servers die in ons domein komen (Applicatieserver).

DHCP;
Netwerk > Settings > DHCP

Als je de interne netwerkkaart edit kan je de volgende adressen aanpassen;
Gateway, IP range (low), IP range (high), DNS servers, WINS, TFTP en NTP server.
Standaard staat de Gateway als je eigen adres (X.X.X.254), het uitdelen van IP adressen van X.X.X.100 tot X.X.X.253 en de Lease time op 12 uur.

Indien de DHCP server nog niet draait druk je op 'Start'.
En zoals de server zelf al aangeeft, wees dus geduldig...



De volgende keer dat de server opstart zal de DHCP wel worden mee opgestart.

Vanaf het moment er computers een IP adres hebben gekregen van de DHCP staan deze in de lijst 'Dynamic Leases'. Hierbij staat ook het MAC Adres, Host naam en wanneer deze vervalt.
Onder de 'Static Leases' kan je het IP adres opgeven met het Mac adres en druk je op 'Add'.
Wanneer er een netwerkkaart met het juiste MAC adres aanmeld bij de DHCP zal deze een vast IP adres krijgen van de DHCP.

5.4.3 Gebruikersaccounts.

Directory > Accounts > Users

Klik op ‘add’ om een gebruiker toe te voegen.
Geef een gebruikersnaam, voornaam, achternaam en een paswoord in.
Je kan ook de adres gegevens bijwerken of die laten staan op dit van het bedrijf.
Bij een mailserver zal je bij ‘Mail services’ de Mailbox quota moeten instellen en een mailadres.
Andere services die de gebruiker kan gebruiken is afhankelijk van de geïnstalleerde modules en de al ingestelde configuratie.
Druk onderaan op ‘add’ en de gebruiker wordt aangemaakt.
Je kan de gebruiker onder verdelen onder groepen *Directory > Accounts > Groups*
Klik op de gewenste groep All Users, Domain Users of Domain Admins (wij kiezen voor domain admins) en selecteer de gewenste gebruikers. Druk op Update om te bevestigen.

Noot. Via *Directory > Accounts > Import/Export* kan je de gebruikerslijst exporteren.
Of ja kan ook een template downloaden en daar alle gebruikers inzetten en terug uploaden.

Ga naar *System > Settings > Administrators*
Met de beheerder manager pagina kun je de administrators aan verschillende tools toevoegen of verwijderen. Vb. Admin1 mag enkel de fileserver beheren en Admin2 enkel de webserver en zijn pagina’s.

5.4.4 Windows Networking

Server > Windows Networking > Windows Settings

De eerste keer zal je een winadmin paswoord moeten ingeven. (Dit wordt enkel gebruikt als je kiest voor PDC, maar je moet het ingeven voor je aan de andere instellingen kan.)
Ook kan je de 'Server name' en het 'Windows Domain' ingeven.
Druk op 'update' om verder te gaan.

Je hebt keuze tussen twee modes.
*Simple File and Print Server.
Deze modus wordt gebruikt voor het creëren van een basis bestands- en print server.
*Primary Domain Controller / PDC.
Hierbij moeten de volgende parameters worden gespecifieerd:

- Windows Domain
- Logon script
- Roaming profiles
- Logon drive

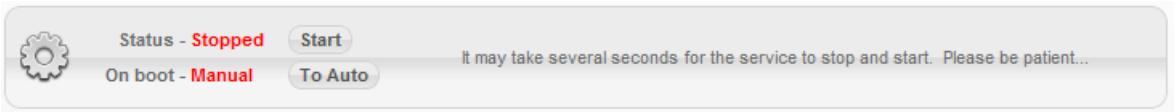
Wij kiezen hier voor Simple File and Print Server aangezien we deze enkel maar nodig hebben om onze web server te kunnen updaten.

Noot. Windows Networking is enkel beschikbaar langs de interne kant. Deze in de firewall regels actief maken als inkomende heeft geen zin.

5.4.5 Web server

Server > Web > Web Server

Met de web server beheert u uw eigen website. U kunt verschillende web applicaties naar uw server uploaden, inclusief content management systemen, forums, blogs en andere. Hiervoor moet u evt. ook de MySQL database geïnstalleerd hebben.



Indien de server nog niet draait druk je op 'Start' om hem te starten.
Om de web server mee te laten opstarten samen met de ClearOS druk je op 'To Auto'.

*Web server instellingen.
Hier kan je twee dingen aanpassen, 'Server Name' en 'SSL-enabled'.
-De servernaam is een geldige naam voor uw web server. Deze naam wordt gebruikt op een aantal weinig gebruikte error pagina's, dus het is niet zo belangrijk.
-De webserver wordt geleverd met een ingebouwde SSL-codering voor de verbeterde beveiliging. Als uw website een gebruikersnaam en wachtwoord vereist om in te loggen, dan is het een goed idee om encryptie te gebruiken.

*Virtuele host instellingen.
De webserver bevat ondersteuning voor "virtuele hosts". Dit betekent dat uw web server kan worden gebruikt voor het hosten van meer dan een website.

Om de standaard web host te configureren druk je achter de host op 'edit'.
Hierin kan je dan volgende zaken instellen: Website, server aliassen, FTP en bestandserver upload (indien geïnstalleerd), upload toegang.
Je kan ook zien welke de document root is.

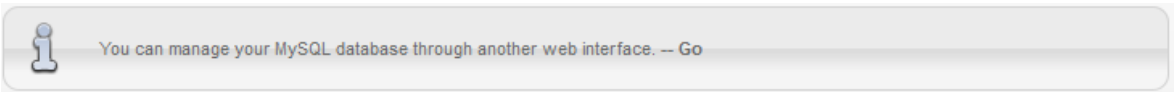
MySQL

Server > Database > MySQL

Indien de database nog niet draait druk je op 'Start' en evt. op 'To Auto' om hem automatisch mee te laten opstarten.

Indien er nog geen database wachtwoord is kan je er nu één opgeven en op 'update' klikken.

Om de MySQL database te beheren druk je op 'Go'.



Je krijgt dan de web interface van phpMyAdmin.

5.4.6 Firewall

Network > Firewall > Incoming

Op de firewall inkomende verbindingen pagina kunt u op uw server een poort of dienst openen. Bijvoorbeeld, als je jouw eigen webserver beschikbaar wilt maken voor de rest van de wereld, dan moet je poort 80 op de firewall open zetten.

In het onderdeel “Add firewall rule” kan je kiezen tussen: standaard diensten, alias / poort en alias / poort bereik.

*Standaard diensten: selecteer uit de lijst bv. http en druk op ‘Add’.
*Alias / poort: geef een alias op, selecteer of het TCP of UDP moet zijn en geef het poort nummer in. Druk dan op ‘Add’.
*Alias / poort bereik: geef een alias op, TCP of UDP, de begin poort en de eind poort. Druk op ‘Add’ om toe te voegen.

Ja kan ook externe hosts blokkeren door een alias en het IP adres in te geven en te drukken op ‘Add’.

Network > Firewall > Outgoing

Hier kan je bepaalde type uitgaand verkeer naar buiten blokkeren.

Network > Firewall > Port forwarding

Op deze pagina kan je regels aanmaken die een externe poort van de firewall door verbinden naar een poort van een interne PC in jouw locale network.

5.4.7 System

System > Resources > Services

Je kan zelf bepalen welke diensten actief zijn op jouw systeem. Als je wilt dat bepaalde diensten automatisch starten bij een herstart, zorg dan dat de 'On Boot' kolom is gezet op 'Automatic'.

System > Resources > Processes

Deze pagina geeft de real-time status van de actieve diensten op uw systeem.

System > Settings > Mail Notification

Veel programma's gebruiken e-mail om alarmen en rapportages te versturen naar de administrator. Configureer en test de uitgaande SMTP relay om er zeker van te zijn dat u deze e-mails ontvangt. Als je de SMTP server mee hebt geïnstalleerd dan kan je de standaardinstellingen laten.

Maar als je wilt kan je ook gebruik maken van de gmail dienst, dit met de volgende instellingen:

- SMTP host: smtp.gmail.com
- Port: 465
- SSL/TLS: TLS
- Username: user@gmail.com en wachtwoord
- Zender: het adres van wie je de mail ontvangt.

5.4.8 Registreer ClearOS

ClearCenter > Overview > Register System

Als je uw ClearOS registreerd dan kan je via de ‘Software Modules’ en de ‘Software Updates’ modules toevoegen en updaten.

6 NAGIOS

6.1 NAGIOS - Beheer je netwerk in één oogwenk

In onze C-proef hebben we gekozen om Nagios te gebruiken om ons netwerk te monitoren. Via verschillende checks verifiëren we de performantie van ons netwerk, de beschikbaarheid van servers, de status van draaiende services,.. In een overzichtelijk scherm worden de uitgevoerde checks gegroepeerd. Nagios kan zo ingesteld worden dat een mail of SMS wordt doorgestuurd wanneer er zich een probleem voordoet.

Nagios werd in 1999 door Ethan Galstad ontwikkeld. Zijn applicatie draaide op Unix met een c-compiler. Het heeft een massieve verdeling van het basisproduct met zich mee gebracht. En gezien het concept een open source product was, heeft het al snel aanpassingen en verbeteringen door medegebruikers gekregen. De routines worden in C , Perl of een andere scripttaal geschreven. Een routine of een plugin stuurt zijn informatie op een gestructureerde manier terug. Bij de installatie van het basispakket van Nagios worden er standaard-checks geïnstalleerd. Hierbij worden lokale checks op de Nagios-server uitgevoerd. Naast die standaard checks zijn er een waaier van plugins of checks terug te vinden op www.nagiosexchange.org. Dit is het groot voordeel van de open source filosofie van Nagios. Mensen die een check-routine hebben ontwikkeld delen die met de buitenwereld. Er is altijd wel iemand die een variante of een gelijkaardige plugin ter beschikking heeft.

De verschillende checks kan je in volgende groepen onderverdelen. Om een beeld te schetsen geef ik enkele type voorbeelden per categorie.

Hardware checks:

- check_disk: test de beschikbare ruimte op partitie of volledige harddisk
- check_load: geeft je informatie over de belasting van de CPU
- Check_swap: test de swap over de schijven

Netwerkchecks

- Check_ping: is de client te bereiken en dus nog actief
- Check_udp contoleert de goede werking van de transportlaag op basis van UDP

Applicatie checks

- Check_by_ssh: laat toe om de informatie ingekapseld volgens ssh-beveiliging in te lezen
- Check_procstate: is een applicatie running

Service checks

- Hierbij bestaat er een waaier aan mogelijkheden zoals check_dns; check_dhcp; check_pop, check_msql

Client checks

- Check_nagios laat toe om de goede werking van een nagios client te controleren bv. Via NRPE
- Check_nt laat toe een server of een NT client te testen

Door een logica of een hiërarchie in je checks in te bouwen kan je logische bouwstenen creëren. Er is een verschil tussen een host is unreachable of een host is down. Door middel van een klassieke ping commando zal je niet onmiddellijk dit verschil kunnen detecteren.

Een check geeft je eerst een status weer met al dan niet een waarde erbij. Bij de installatie bepaal je wanneer een drempel kritisch wordt overschreden of tout court gevaarlijk wordt. Op het overzicht scherm verandert je check visualisatie van groen naar rood of nog naar oranje. Zo zie je in een oogwenk of de status van de check OK – Warning – Critical is. Je bepaalt zelf of een waarde overschrijding al dan niet kritisch is en of er een bericht naar buiten wordt verstuurd.Dit laatste is heel handig om zodanig een 24/24h service te verlenen zonder hiervoor permanent gemobiliseerd te worden.

Je kan Nagios volledig op maat opbouwen. Je monitoring service zal zo groot, complex en efficiënt zijn als dat je zelf bepaalt. Services kunnen op je locale machine draaien of worden als een plugins of daemon op een andere server of client geïnstalleerd. Hierdoor is het mogelijk om windows machines in je monitoring service op te nemen. In onze C-proef superviseren we Linux alsook Windows machines. Al die verschillende elementen, checks en services worden in een overzichtelijk dashboard opgenomen.

Onze C-proef is geen finaliteit van een ‘’type installatie’. Een installatie zal leven, aangepast en bijgestuurd worden. Onze hoofdbekommernis is in eerste instantie :

- Is ons systeem werkbaar in een productieomgeving
- Is het flexibel en overzichtelijk
- En heeft het de mogelijkheid om preventieve acties te ondernemen

6.2 Server requierments

De enige eis voor het runnen van Nagios Core is een machine met Linux (of UNIX-variant) en toegang tot het netwerk.

Een Nagios server dient aan volgende specificaties te voldoen. Zoals je ziet is bepalend hoeveel hosts er worden gemonitord.

Hosts	CPU's	CPU Snelheid	Geheugen	Schijfruimte
< 100	1	800Mhz+	512Mb	5Gb
100 – 500	1	1Ghz+	1Gb+	10Gb
500 – 1000	1+	3Ghz+	1Gb+	20Gb
> 1000	1+	3Ghz+	2Gb+	40Gb

6.3 NAGIOS – Installatie

We installeren Nagios monitoring service op een (virtuele) Linux machine. Op het internet vind je een waaier aan sites die je bij de installatie begeleiden. Mijn voorkeur gaat naar :

http://www.thegeekstuff.com/2008/05/nagios-30-jumpstart-guide-for-red-hat-overview-installation-and-configuration/

In de bibliografie kan je andere interessante linken terugvinden. In functie van de versie van linux die je gebruikt (OpenSuse – RedHat) is de installatie iets verschillend. Proefondervindelijk kan ik afraden om Nagios via Yast (voor OpenSuse) te installeren. Er worden directories en subdirectory's aangemaakt op andere locaties dan in de standaard nagios-litteratuur zijn beschreven. Als je achteraf een supplementaire plugin installeert, wordt die niet in rekening gebracht want hij staat op een locatie die Nagios via Yast niet gebruikt. Dit is heel verwarrend want dingen die je denkt in het juiste bestand aan te passen worden niet in rekening gebracht.

6.3.1 Installatie

1. Alvorens de installatie te starten downloaden we eerst volgende compilers
   - gcc-core.tar.bz2
   - gnu_compilers_v2.tar.bz2
   - openssl-0.9.8c.tar.gz

2. Naaste apache2 installeren we via YAST volgende programma's. Onderstaande programma's zijn nodig bij de mapping-functie van nagios.
   - Gd
   - Gd-devel
   - Png
   - Png-devel
   - Jpeg
   - Jpeg-devel
   - Zlib
   - Zlib-devel
   - Php5-gd
   - Php5-nmstring

3. We downloaden vanuit nagios.org en plaatsen het in /home/<user>/Downloads
   - nagios-3.3.1.tar.gz
   - nagios-plugins-1.4.15.tar.gz

4. We installeren de compilers met het commando **tar -xvf …..** en controlleren of de gewenste compilers zijn geïnstalleerd
   - **rpm –qa | grep gcc**
   - **rpm –qa gd**

5. Nagios gebruikers en groepen creëren

- **useradd nagios**
- **passwd nagios**
- **groupadd nagcmd**
- **usermod –G nagcmd nagios**
- **usermod –G nagcmd apache**

6. Nagios installeren vanuit /home/<user>/Downloads
   - **tar -xzf nagios-3.3.1.tar.gz**
   - **cd nagios**
   - **./configure --with-command-group=nagcmd**
   - **make all**
   - **make install**
   - **make install-init**
   - **make install-config**
   - **make install-comandmode**

Bij de installatie krijg je volgende info

```
*** Configuration summary for nagios 3.3.1 07-25-2011 ***:

 General Options:
 -------------------------
        Nagios executable:  nagios
        Nagios user/group:  nagios,nagios
       Command user/group:  nagios,nagcmd
            Embedded Perl:  no
             Event Broker:  yes
        Install ${prefix}:  /usr/local/nagios
                Lock file:  ${prefix}/var/nagios.lock
   Check result directory:  ${prefix}/var/spool/checkresults
           Init directory:  /etc/rc.d
  Apache conf.d directory:  /etc/apache2/conf.d
             Mail program:  /usr/bin/mail
                  Host OS:  linux-gnu

 Web Interface Options:
 ------------------------
                 HTML URL:  http://localhost/nagios/
                  CGI URL:  http://localhost/nagios/cgi-bin/
 Traceroute (used by WAP):  /usr/sbin/traceroute
```

7. Configuratie van de web interface met daarbij de instelling van het passwoord van de gebruiker
   - **make install-webconf**
   - **htpasswd –c /usr/local/nagios/etc/htpasswd.users nagiosadmin**

8. Installatie van de nagios plugins vanuit /home/<user>/Downloads
   - **tar -xzf nagios-plugins-1.4.15.tar.gz**
   - **cd nagios-plugins-1.4.15**
   - **./configure --with-nagios-user=nagios --with-nagios-group=nagios**
   - **make**
   - **make install**

9. Start Nagios

Nagios toevoegen aan de startroutine

- **Chkconfig –add nagios**
- **Chkconfig nagios on**

Controlleren of er geen errors zijn bij het opstarten van nagios

- **/usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg**

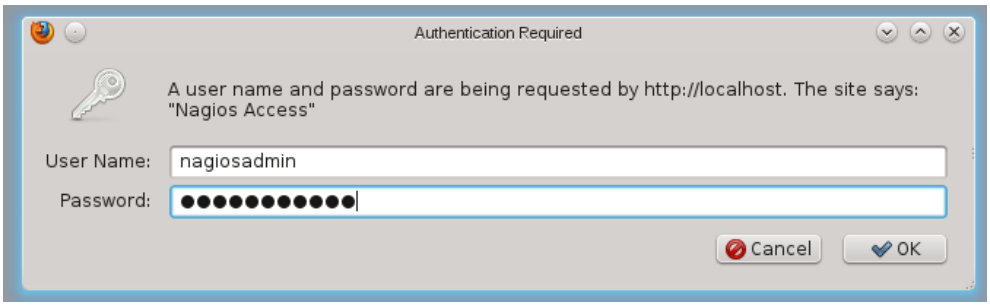
```
Processing object config file '/usr/local/nagios/etc/objects/timeperiods.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/templates.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/localhost.cfg'...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking services...
        Checked 8 services.
Checking hosts...
        Checked 1 hosts.
Checking host groups...
        Checked 1 host groups.
Checking service groups...
        Checked 0 service groups.
Checking contacts...
        Checked 1 contacts.
Checking contact groups...
        Checked 1 contact groups.
Checking service escalations...
        Checked 0 service escalations.
Checking service dependencies...
        Checked 0 service dependencies.
Checking host escalations...
        Checked 0 host escalations.
Checking host dependencies...
        Checked 0 host dependencies.
Checking commands...
        Checked 24 commands.
Checking time periods...
        Checked 5 time periods.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Nagios starten

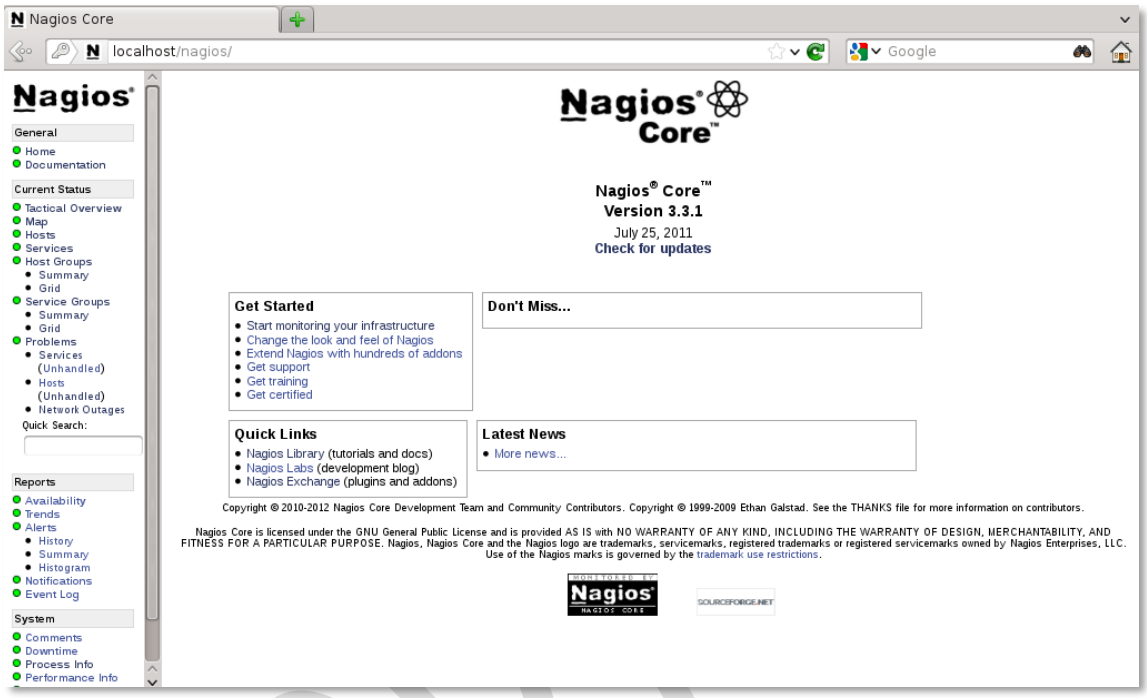
- **service nagios start**
- **rcapache2 start**

Webinterface controlleren

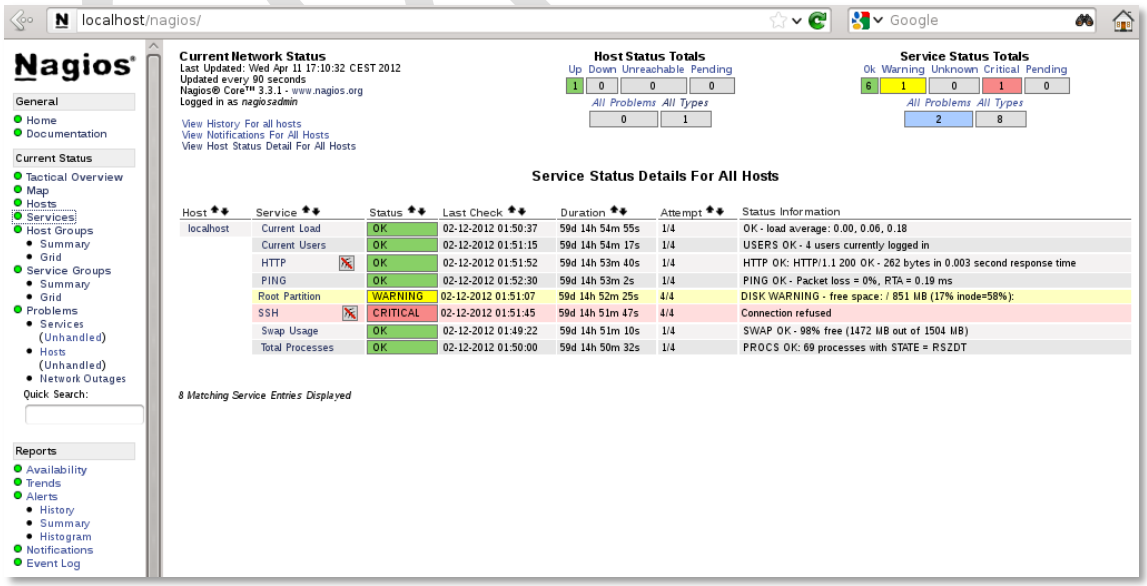
- http://localhost/nagios



We zitten in de basisconfiguratie van nagios

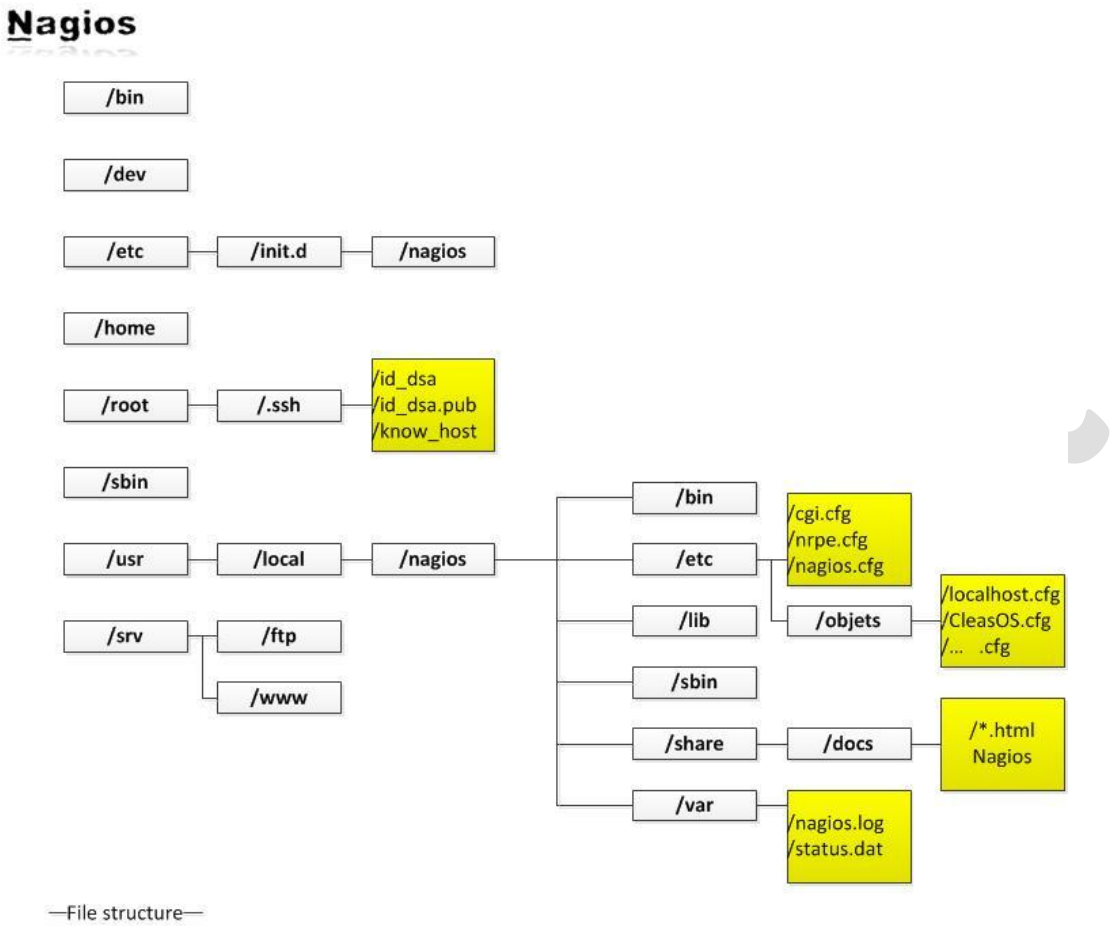


Met één host en de standaard services



6.3.2 Wat zit waar

In het onderstaand overzicht vind je de locatie en de bestanden terug die voor de configuratie belangrijk zijn.



—File structure—

De bestanden die zich in **/root/.ssh** bevinden houden de verschillende keys bij voor externe toegang tot dit of andere machines. Hierover vind je meer informatie bij sshd check (hfdst 6.4.6).

In **/usr/local/nagios/etc** vind je de main bestanden van nagios. De passwoorden en de gebruikers die toegang hebben tot nagios. En het **nagios.cfg** bestand. Hier zal je de topologie van je netwerkt bepalen. Hoeveel hosts monitoren we, hoe zijn ze aan elkaar gelinkt. In het **cgi.cfg** bestand configureer je de mapping van je netwerk.

In **/usr/local/nagios/etc/objets** worden de hosts individueel aangemaakt die door **nagios.cfg** worden opgeroepen. Voor ieder host zal je bepalen welke checks er worden uitgevoerd.

/usr/local/nagios/bin vind je de executable files. Hier zullen wij niet direct iets aan veranderen

/usr/local/nagios/lib of **/usr/local/nagios /libexe** groeperen alle checks die bij de basisinstallatie mee zijn geïnstalleerd. Je kan dit zien als een bibliotheek van checks

/usr/local/nagios/share hier worden de logo's en html pagina's gegroepeerd

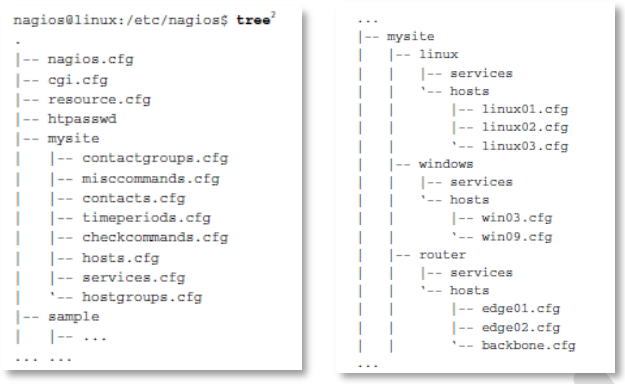
In de **/usr/local/nagios/var/nagios.log** vind je alle teruggestuurde info van de lopende checks

In de **/usr/local/nagios/var/status.dat** heb je alle informatie van de aangemaakte hosts

6.3.3 Relatie tussen nagios.cfg en /objects bestanden

De ‘core’ applicatie zit in het **nagios.cfg** bestand. Vanuit **/usr/local/nagios/etc/nagios.cfg** worden de gemonitorde hosts opgeroepen. Die bevinden zich in **/usr/local/nagios/etc/objets/**

Om een geheel mooi overzichtelijk te houden, en zeker voor latere uitbreidingen, is het belangrijk om zaken die bij elkaar horen te groepen. Dit kunnen geografische groepen zijn of hosts met dezelfde OS. Volgende directory structuur kunnen we hiervoor gebruiken .



6.3.4 Basisapplicatie

Bij de basis installatie wordt enkel de localhost gemonitord. In nagios.cfg wordt de localhost.cfg opgeroepen die zich in de directory **/usr/local/nagios/etc/objets/** bevindt.

Wat wordt in een /object/*.cfg bestand aangemaakt? Een *.cfg bestand heeft volgende indeling:

Define host – Define Hostgroup – Define Service

Define host :

hier wordt de naam en het IP adres van de host gespecifieerd. Hoeveel checks dienen te gebeuren alvorens we overgaan naar een OK staat. Wanneer worden de checks uitgevoerd (24/24 of enkel tijdens de kantooruren). Wanneer mag een melding naar buiten worden gestuurd bij een probleem). En wat is voor ons belangrijk warning, down, unreachable, recovery (OK na een error) of flapping.

```
define host{
   host_name                       linux01
   hostgroups                      linux-servers
   alias                           Linux File Server
   address                         192.168.1.9
   check_command                   check-host-alive
   max_check_attempts              3
   check_period                    24x7
   contact_groups                  localadmins
   notification_interval           120
   notification_period             24x7
   notification_options            d,u,r,f
   parents                         router01
}
```

Host Group:

Het kan handig zijn om verschillende hosts met dezelfde eigenschappen in één groep te stoppen. Zo worden gegevens gegroepeerd en dien je de uit te voeren checks maar één keer aan te maken.

```
define hostgroup{
   hostgroup_name  linux-servers
   alias           Linux Servers
   members         linux01,linux02
}
```

```
define hostgroup{
       hostgroup_name  linux-servers ; The name of the hostgroup
       alias           Linux Servers ; Long name of the group
       members         localhost, linux-client     ; Comma separated list of hosts that belong to this group
       }
```

Services:

Je kan bepalen wanneer een services wordt uitgevoerd, wie je wenst te verwittigen als er zich een probleem voordoet, welke service – check je wenst uit te voeren.

```
define service{
    host_name                       linux01
    service_description             PING
    check_command                   check_ping!100.0,20%!500.0,60%
    max_check_attempts              3
    normal_check_interval           5
    retry_check_interval            1
    check_period                    24x7
    notification_interval           120
    notification_period             24x7
    notification_options            w,u,c,r,f
    contact_groups                  localadmins
}
```

Vervolgens bepaal je de services die je wenst uit te voeren

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        }


# Define a service to check the disk space of the root partition
# on the local machine.  Warning if < 20% free, critical if
# < 10% free space on partition.

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Root Partition
        check_command                   check_local_disk!10%!5%!/
        }



# Define a service to check the number of currently logged in
# users on the local machine.  Warning if > 20 users, critical
# if > 50 users.

define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Current Users
        check_command                   check_local_users!20!50
        }


# Define a service to check the number of currently running procs
# on the local machine.  Warning if > 250 processes, critical if
```

6.3.5 Controle voor opstart van Nagios

Zoals eerder aangehaald is Nagios een webbased applicatie. Apache dient op de monitoring server te draaien.

We controlleren of we alles goed aangemaakt hebben met volgend commando. Je ziet dat de verschillende hosts mee worden opgeroepen.

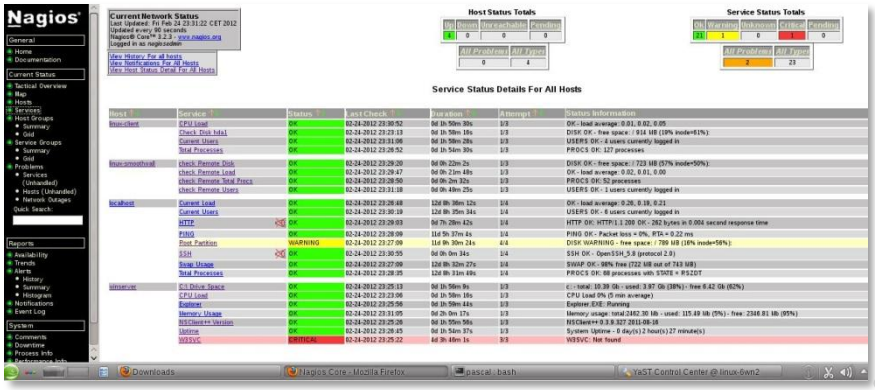
/usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg

```
nagios-monitor:/ # /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 3.2.3
Copyright (c) 2009-2010 Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 10-03-2010
License: GPL

Website: http://www.nagios.org
Reading configuration data...
   Read main config file okay...
Processing object config file '/usr/local/nagios/etc/objects/commands.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/contacts.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/timeperiods.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/templates.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/localhost.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/windows.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/linuxclient.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/clearOS.cfg'...
Processing object config file '/usr/local/nagios/etc/objects/switch.cfg'...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking services...
        Checked 28 services.
Checking hosts...
        Checked 5 hosts.
Checking host groups...
        Checked 4 host groups.
Checking service groups...
        Checked 0 service groups.
Checking contacts...
        Checked 1 contacts.
Checking contact groups...
        Checked 1 contact groups.
Checking service escalations...
        Checked 0 service escalations.
Checking service dependencies...
        Checked 0 service dependencies.
Checking host escalations...
        Checked 0 host escalations.
Checking host dependencies...
        Checked 0 host dependencies.
```

```
Checking commands...
        Checked 29 commands.
Checking time periods...
        Checked 5 time periods.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
nagios-monitor:/ #
```

Zijn er geen errors of warnings dan kunnen we Nagios opstarten met : **service nagios start**

6.3.6 Overzicht van de lopende host met de uitgevoerde checks



6.3.7 Hoe moet je de verschillende waardes interpreteren

- We krijgen een groene OK terug als de uitgelezen waarde in het vooropgestelde tolerantieveld zit en alles normaal is
- Een gele WARNING als een eerste drempel wordt overschreden maar de kritische drempel is nog niet overschreden
- Een rode CRITICAL als de uitgelezen waarde onder de critical waarde zit of als de check niet kan uitgevoerd worden.
- Een oranje UNKNOWN als de waarde die uitgelezen wordt niet correct geïnterpreteerde kan worden

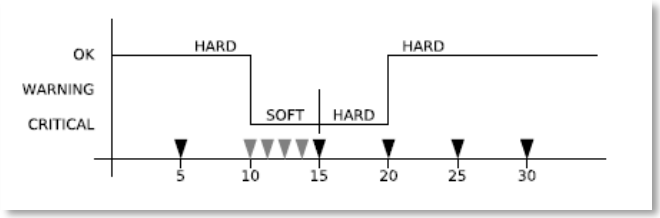
Host	Service	Status	Last Check	Duration	Attempt	Status Information
Clear_OS	CPU Load	OK	04-02-2012 17:24:41	0d 0h 41m 13s	1/3	OK - load average: 1.04, 0.95, 0.83
	Check Disk	OK	04-02-2012 17:25:43	0d 0h 40m 7s	1/3	DISK OK - free space: / 4753 MB (73% inode=96%):
	Current Users	OK	04-02-2012 17:17:11	0d 0h 38m 39s	1/3	USERS OK - 1 users currently logged in
	Total Processes	OK	04-02-2012 17:18:39	0d 0h 37m 11s	1/3	PROCS OK: 88 processes
linksys-srw224p	PING	OK	04-02-2012 17:25:07	0d 3h 5m 43s	1/3	PING OK - Packet loss = 0%, RTA = 0.67 ms
	Port 1 Bandwidth Usage	UNKNOWN	04-02-2012 17:21:35	15d 20h 5m 11s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	CRITICAL	04-02-2012 17:24:32	15d 20h 6m 29s	3/3	(Return code of 127 is out of bounds - plugin may be missing)

In de kolom Attempt kan je nagaan hoeveel keren de check werd uitgevoerd alvorens een hard state wordt doorgestuurd.

In het *.cfg bestand bepaal je na hoeveel tijd een volgende check dient te gebeuren. Is de waarde dezelfde als de vorige keer dan is alles ok. Je hebt een HARD state en de volgende check gebeurt in ons geval na 5 min.

Ga je van een OK naar een critical waarde dan gebeuren de daaropvolgende inlezingen sneller (retry_check_interval) en een aantal keer (max_check_attempts) alvorens die tijdelijke overgang van soft state naar een hard state te valideren. Een overgang die in een soft state blijft hangen heet **flapping.** In ons bovenstaand geval zie je bij Attempt dat bij de eerste van de 3 checks al een hard state werd doorgegeven. Voor Unknown en critical is na de 3 poging van de 3 een hard staat doorgegeven.

```
define service{
   host_name               proxy
   service_description     DNS
   ...
   normal_check_interval 5
   retry_check_interval  1
   max_check_attempts    5
   ...
}
```



Als na een korte tijdsspanne bij een check de overgangen heel wisselvallig zijn; van cirtical naar ok en omgekeerd dan zal er een wolkje bij die check komen. Hiermee illustreert Nagios dat die service niet stabiel is.

6.4 Nagios – Checks en services op clients

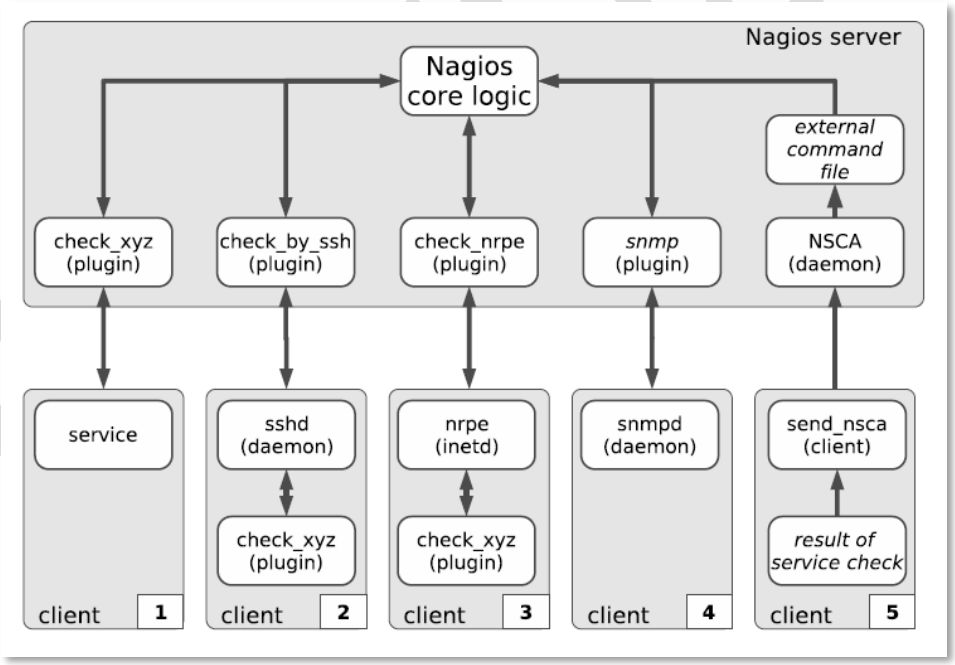
Naast de standaard checks die op de localhost werden geïnstalleerd, kunnen we ook informatie gaan opvragen op andere machines. Hiervoor bestaan er verschillende mogelijkheden. In onze C-proef hebben we de 4 varianten uitgewerkt.

Voor ClearOS werken we partieel met een check_xyz plugin. Dit om de goede werking van bv. De DHCP te controleren . Daarnaast gebruiken we ook NRPE om zaken als CPU-load, HD bezetting en aantal users op een andere Linux machine te bekijken.

Voor een windows machines gebruiken we NSClient++. Dit is een plugin die op de windows machines wordt geïnstalleerde . De NSClient++ bezorgt de gegevens in een gestructureerde formaat aan Nagios terug.

Verder heb ik de ClearOS-server via SSHD gemonitord. Dit op basis van private- en public keys. Het nadeel was dat je de check als root diende uit te voeren, wat misschien voor security niet echt wenselijk is. Het voordeel is wel dat je geen speciale daemon meer op de client moest installeren. SHHD staat al standaard op een Linux machine. Zo wordt de ClearOS in onze C-proef als nog via een NRPE plugin uitgevoerd. Toch illustreer ik verder de ssh-variante als check want toen we Smoothwall als DHCP en Firewall gebruikten was dit de enige manier om zijn services te monitoren.

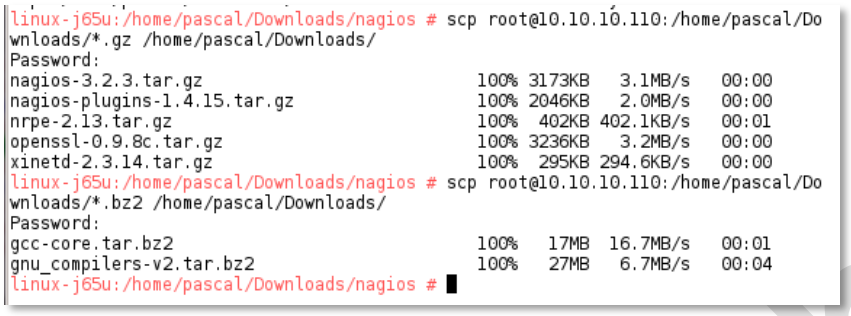
Mocht de tijd ons niet ontbreken hadden we de Cisco switch van Syntra via SNMP willen monitoren.



6.4.1 Installatie van NRPE

6.4.1.1 Op Linux Client

Bij de standaard Nagios installatie hebben we reeds verschillende plugins en compilers gedownload. Een eerste mogelijkheid is dat we ze kopiëren vanuit de Nagios Monitor server naar de Linux Client machine via het **scp** commando.



1. Zoals bij de installatie van nagios installeren we eerst de verschillende compilers.
   - **gcc-core.tar.bz2**
   - **gnu_compilers_v2.tar.bz2**
   - **openssl-0.9.8c.tar.gz**

   Hebben we een Linux OpenSuse client dan kunnen we ook de compilers via Yast installeren.

2. Vervolgens installeren we NRPE en Nagios-plugins. Een handige link hierbij is: http://www.thegeekstuff.com/2008/06/how-to-monitor-remote-linux-host-using-nagios-30/

   We gebruiken:
   - **nagios-plugins-1.4.15.tar.gz**
   - **nrpe-2.13.tar.gz**

3. We maken nagios als gebruiker aan
   - **useradd nagios**
   - **passwd nagios**

4. Installatie van nagios plugin vanuit /home/<user>/Downloads
   - **tar -xvfz nagios_plugins-1.4.15.tar.gz**
   - **cd nagios-plugins-1.4.15.tar.gz**
   - **export LDFAGS=ldl**
   - **./configure --with-nagios-user=nagios --with-nagios-group=nagios**
   - **make**
   - **make install**
   - **chown nagios.nagios /usr/local/nagios**
   - **chown –R nagios.nagios /usr/local/nagios/lib/**

5. Installatie van NRPE vanuit /home/<user>/Downloads

- **tar -xvfz nrpe-2.13.tar.gz**
- **cd nrpe-2.13**
- **./configure**
- **make all**
- **make install-plugin**
- **make install-daemon**
- **make install-daemon-config**
- **make install-xinetd**
-

6. Instelling om nrpe als daemon te laten draaien
   Hierbij zullen we onze monitor server definiëren en een specifieke poort openzetten

   I. In het bestand **/etc/xinetd.d/nrpe** geven we het IP-adres van de Nagios Monitoring Server

      only_from = 127.0.0.1 *10.10.10.110* (ip-adres van monitoring server)

   II. In het bestand **/etc/services** bepalen we de poort die we openzetten voor nrpe

      nrpe 5666/tcp # NRPE

      In de locale firewall zullen we die poort eveneens openzetten

   III. We starten de service xinetd op. Hiermee laten we toe dat we communiceren met een andere server
      Service xinetd restart

   IV. Controlleren of de NRPE luistert
      netstat –at | grep nrpe
      Met als resultaat
      tcp 0 0 *:nrpe *:*

   V. Controlleren of de NRPE draait
      /usr/local/nagios/lib/check_nrpe –H localhost
      Met als resultaat
      NRPE v2.13

7. Controleren of lokale checks functioneren

```
linux-j65u:/home/pascal/Downloads/nrpe-2.13 # cd /
linux-j65u:/ # /usr/local/nagios/lib/check_users -w 5 -c 10
USERS OK - 3 users currently logged in |users=3;5;10;0
linux-j65u:/ # /usr/local/nagios/lib/check_load -w 15,10,5 -c 30,25,20
OK - load average: 0.00, 0.01, 0.05|load1=0.000;15.000;30.000;0; load5=0.010;10.000;25.000;0; load15=0.050;5.000;20.000;0;
```

6.4.1.2 Op Linux Monitoring Server NRPE installeren

1. Installatie van nrpe vanuit /home/<user>/Downloads
   - **tar -xvfz nrpe-2.13.tar.gz**
   - **cd nrpe-2.13**
   - **./configure**
   - **make all**
   - **make install-plugin**
2. Controlleren of we onze client kunnen bereiken

   /usr/local/nagios/lib/check_nrpe –H 10.10.10.120

   Met als resultaat

   NRPE v2.13

6.4.1.3 Host en Services voor Linux Client definiëren

We maken een linuxclient.cfg bestand aan met volgende host en de services gegevens.

```
    I    linuxclient.cfg                                                    Row 1    Col 1    0:14  Ctrl-K H

define host{
        name                            linux-box       ; The name of this host template
        use                             generic-host    ; This template inherits other values from the generic-host template
        check_period                    24x7            ; By default, Linux hosts are checked round the clock
        check_interval                  5               ; Actively check the host every 5 minutes
        retry_interval                  1               ; Schedule host check retries at 1 minute intervals
        max_check_attempts              10              ; Check each Linux host 10 times (max)
        check_command                   check-host-alive ; Default command to check Linux hosts
        notification_period             workhours       ; Linux admins hate to be woken up, so we only notify during the day
                                                        ; Note that the notification_period variable is being overridden from
                                                        ; the value that is inherited from the generic-host template!
        notification_interval           120             ; Resend notifications every 2 hours
        notification_options            d,u,r           ; Only send notifications for specific host states
        contact_groups                  admins          ; Notifications get sent to the admins by default
        register                        0               ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }

# We define a generic printer template that can be used for most printers we monitor

define host{
        use                     linux-box
        host_name               linux-client
        alias                   linux client
        address                 10.10.10.120    ; Inherit default values from the generic-host template
        }



# Local service definition template - This is NOT a real service, just a template!

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-client
        service_description             CPU Load
        check_command                   check_nrpe!check_load
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-client
        service_description             Current Users
        check_command                   check_nrpe!check_users
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-client
        service_description             Total Processes
        check_command                   check_nrpe!check_total_procs
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-client
        service_description             Check Disk
        check_command                   check_nrpe!check_hda1
        }
```

6.4.2 Clear OS client

Bij ClearOS (RedHat) zouden we compilers via Yum kunnen installeren.

Download de gewenste compilers met

yum install gcc gcc-c++ autoconf automake

yum install opensll-devel

Of volgen we de installatie procedure waarbij de plugins en compilers overzetten via het scp-commando (analoog aan onze Linux Client installatie).

We volgen dezelfde stappen als bij de installatie van Linux Client

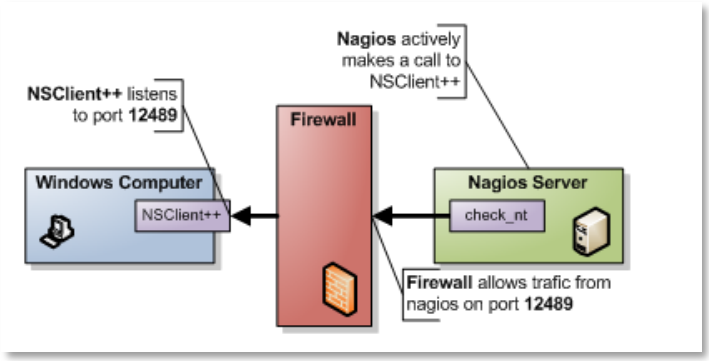
We maken een clearOS.cfg bestand op onze monitoring server aan met de volgende informatie

```
   I    clearOS.cfg                                                    Row 1    Col 1    0:20  Ctrl-K H
define host{
        name                            linux-box2      ; The name of this host template
        use                             generic-host    ; This template inherits other values from the generic-host template
        check_period                    24x7            ; By default, Linux hosts are checked round the clock
        check_interval                  5               ; Actively check the host every 5 minutes
        retry_interval                  1               ; Schedule host check retries at 1 minute intervals
        max_check_attempts              10              ; Check each Linux host 10 times (max)
        check_command                   check-host-alive ; Default command to check Linux hosts
        notification_period             workhours       ; Linux admins hate to be woken up, so we only notify during the day
                                                        ; Note that the notification_period variable is being overridden from
                                                        ; the value that is inherited from the generic-host template!
        notification_interval           120             ; Resend notifications every 2 hours
        notification_options            d,u,r           ; Only send notifications for specific host states
        contact_groups                  admins          ; Notifications get sent to the admins by default
        register                        0               ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }

# We define a generic printer template that can be used for most printers we monitor

define host{
        use                     linux-box2
        host_name               Clear_OS
        alias                   Clear OS
        address                 10.10.10.254    ; Inherit default values from the generic-host template
        }


define hostgroup{
        hostgroup_name          Clear_OS
        alias                   Clear OS
        members                 Clear_OS
        }
```

```
# Local service definition template - This is NOT a real service, just a template!

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       Clear_OS
        service_description             CPU Load
        check_command                   check_nrpe!check_load
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       Clear_OS
        service_description             Current Users
        check_command                   check_nrpe!check_users
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       Clear_OS
        service_description             Total Processes
        check_command                   check_nrpe!check_total_procs
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       Clear_OS
        service_description             Check Disk
        check_command                   check_nrpe!check_hda1
        }
```

6.4.3 Installatie van NSClient++

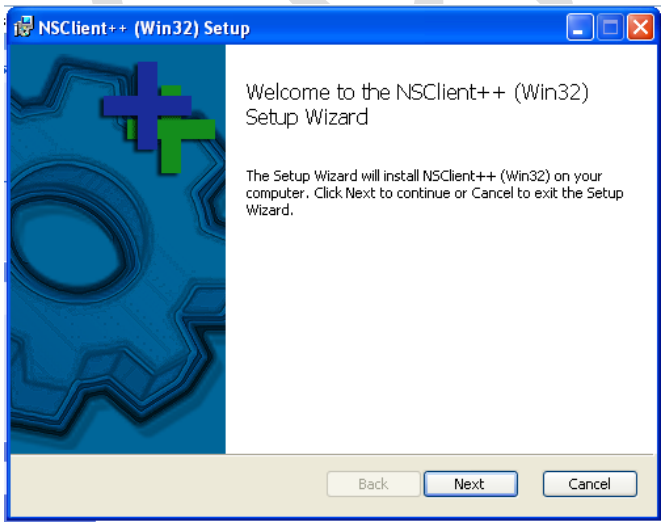
Om Windows Servers of andere Windows machines te monitoren

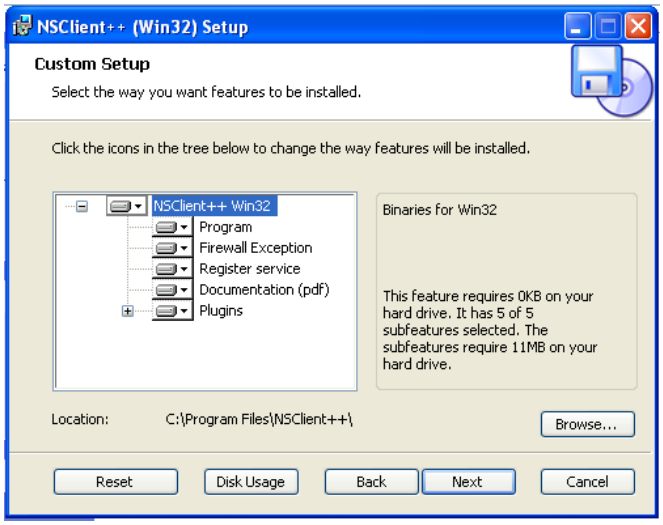


NSClient++ is een daemon die op de Windows machine draait. NSClient++ structureert zijn gecollecteerde gegevens zodat Nagios ze kan verwerken. Nagios zal gegevens van de windows computer opvragen. NSClient++ luistert naar de gestelde vragen en stuurt zijn antwoord naar de nagios monitoring-server terug.

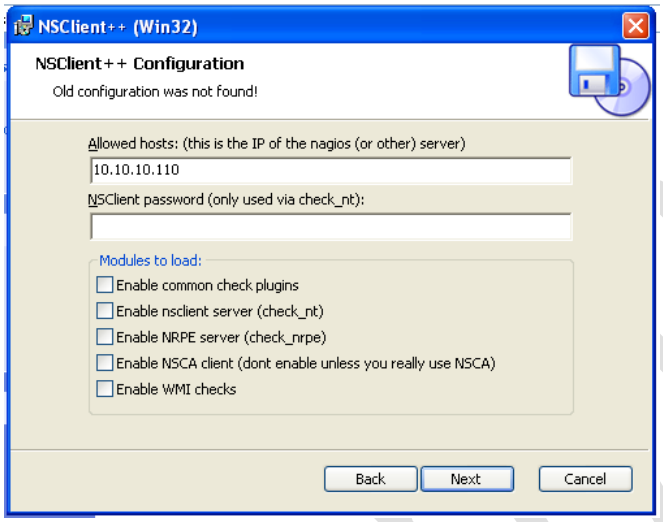
Volgende file dien je op je windows machine te downloaden.

We beginnen de installatie

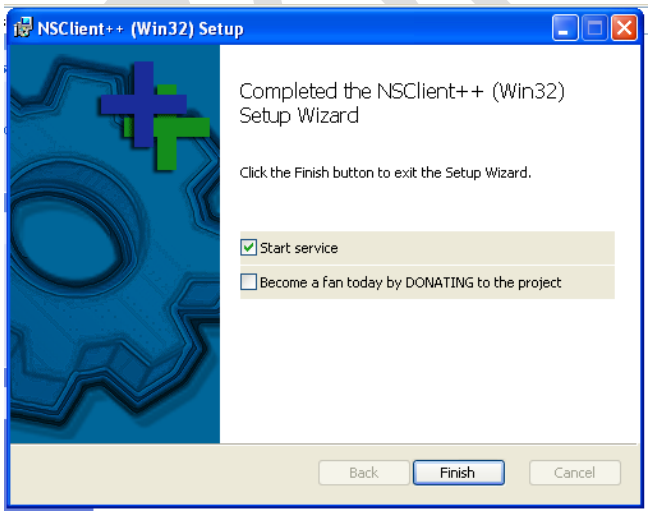




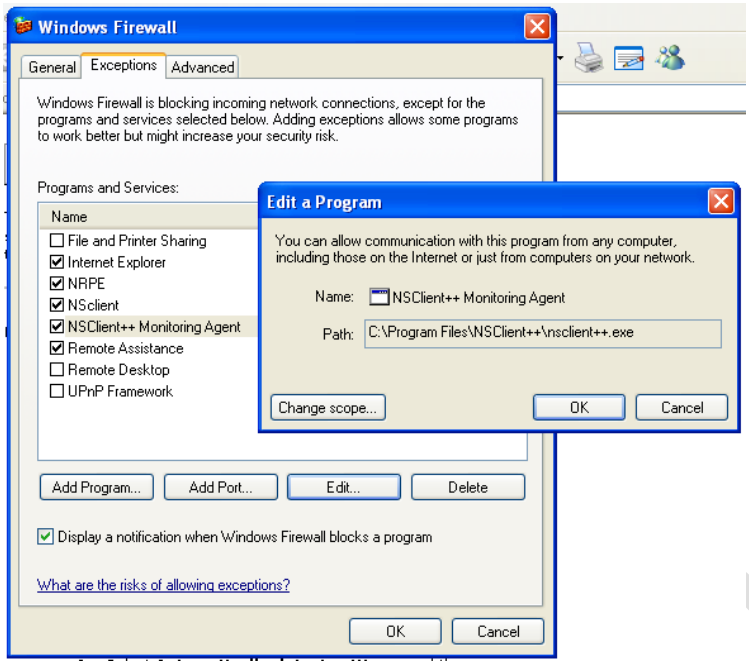
We installeren de full versie



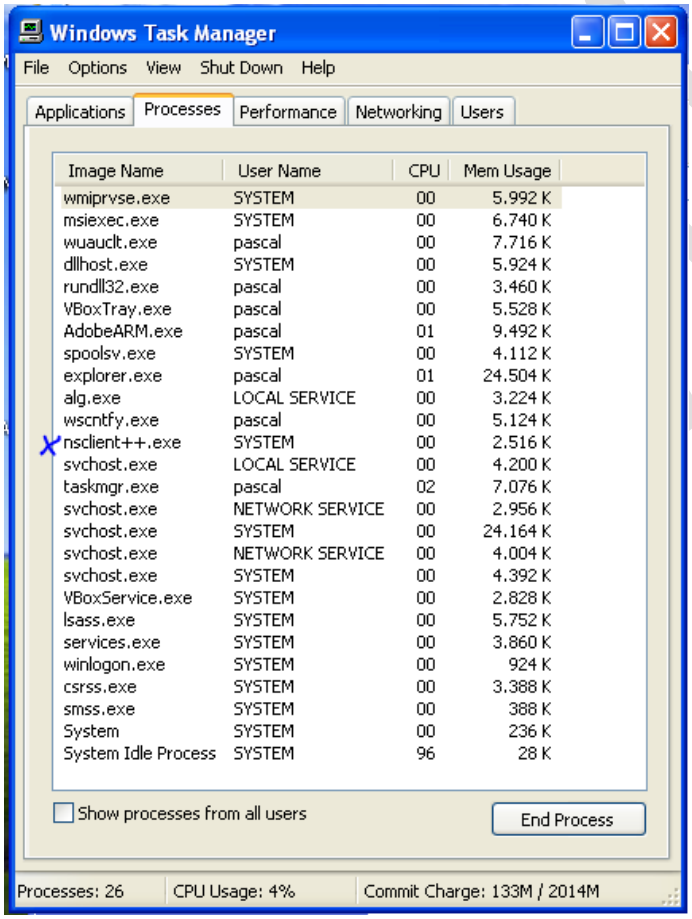
We definiëren welke monitoring server we toestemming geven om onze host te monitoren



Installatie is voltooid



We controleren of er uitzonderingen zijn toegevoegd die de juiste poorten openzet.



NSClient++ draait tussen de andere processen

Configuratie bij onze Nagios Monitor

We maken een bestand windows.cfg aan waarbij volgende services definiëren

```
   I    windows.cfg (Modified)                                                Row 51   Col 1    0:38  Ctrl-K H

define host{
        use             windows-server          ; Inherit default values from a template
        host_name       winserver               ; The name we're giving to this host
        alias           My Windows Server       ; A longer name associated with the host
        address         10.10.10.130            ; IP address of the host
        }

define hostgroup{
        hostgroup_name  windows-servers ; The name of the hostgroup
        alias           Windows Servers ; Long name of the group
        }

define service{
        use                     generic-service
        host_name               winserver
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }

define service{
        use                     generic-service
        host_name               winserver
        service_description     Uptime
        check_command           check_nt!UPTIME
        }

define service{
        use                     generic-service
        host_name               winserver
        service_description     CPU Load
        check_command           check_nt!CPULOAD!-l 5,80,90
        }

define service{
        use                     generic-service
        host_name               winserver
        service_description     Memory Usage
        check_command           check_nt!MEMUSE!-w 80 -c 90
        }



define service{
        use                     generic-service
        host_name               winserver
        service_description     C:\ Drive Space
        check_command           check_nt!USEDDISKSPACE!-l c -w 80 -c 90
        }

define service{
        use                     generic-service
        host_name               winserver
        service_description     Explorer
        check_command           check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
        }

define service{
        use                     generic-service
        host_name               winserver
        service_description     IEXPLORE - Browser
        check_command           check_nt!PROCSTATE!-d SHOWALL -l IEXPLORE.exe
        }
```

6.4.4 DHCP werking controleren

Om de goede werking van de DHCP-services te volgen, hebben we volgende services aan de localhost toegevoegd.

De controle komt vanuit de localhost en hij vraagt aan de ClearOS of hij nog IP adressen uitdeelt (zonder een IP adres te distribueren). Hij vraagt aan de DHCP server of hij in staat is een IP-adres te distribueren.

```
define service{
        use                             local-service
        host_name                       localhost
        service_description             DHCP
        check_command                   check_dhcp
        }
```

6.4.5 Overzicht van nagios.cfg

Hier bepalen we welke host nagios oproept. Terug te vinden in de /objects/*.cfg bestanden.

```
    I    nagios.cfg

# LOG FILE
# This is the main log file where service and host events are logged
# for historical purposes.  This should be the first option specified
# in the config file!!!

log_file=/usr/local/nagios/var/nagios.log



# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
cfg_file=/usr/local/nagios/etc/objects/linuxclient.cfg
#cfg_file=/usr/local/nagios/etc/objects/smoothwall.cfg
cfg_file=/usr/local/nagios/etc/objects/clearOS.cfg
```

Overzicht van de bestanden die we oproepen

We controleren nagios startup met[1]

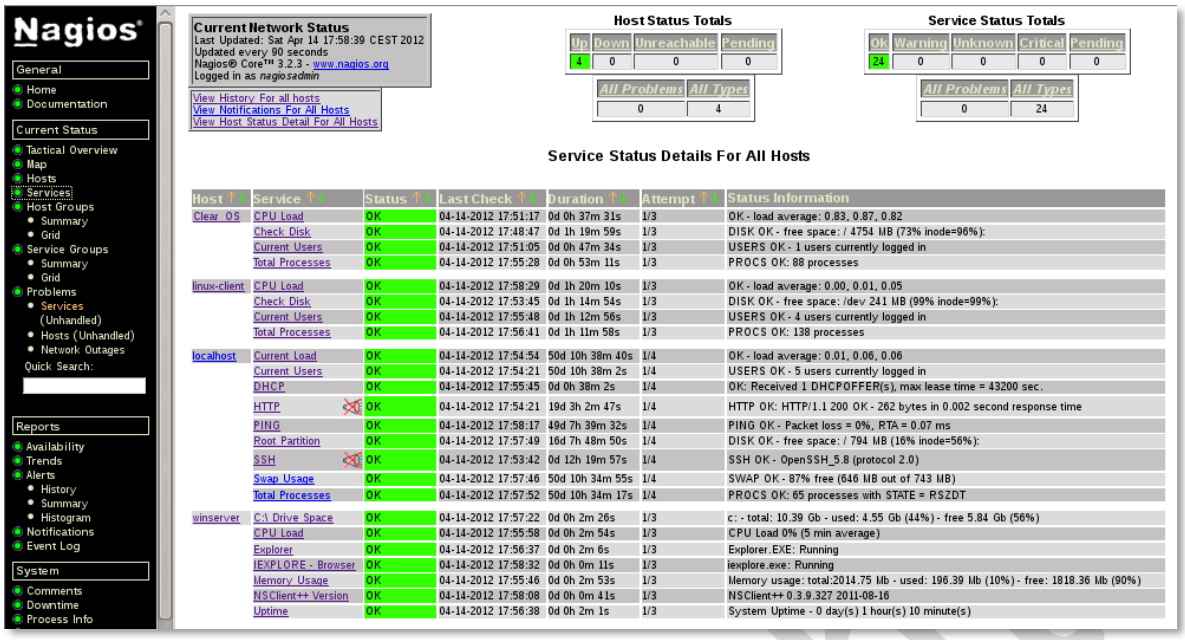
- **/usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg**
- **Service nagios start**

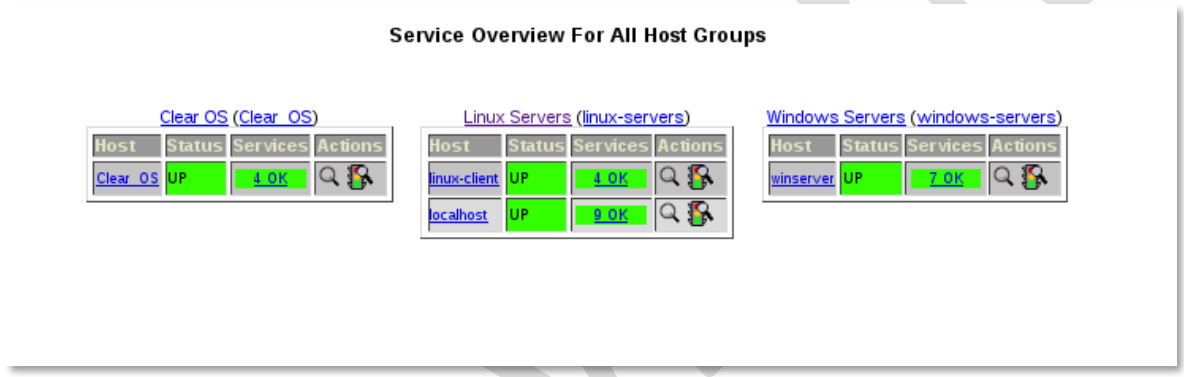
Met volgende schermen in **http://localhost/nagios**

Of vanuit een andere PC

http://<nagiosserveripadress>/nagios

[1] In hoofdstuk 6.8 hebben we hiervoor een batch file geschreven

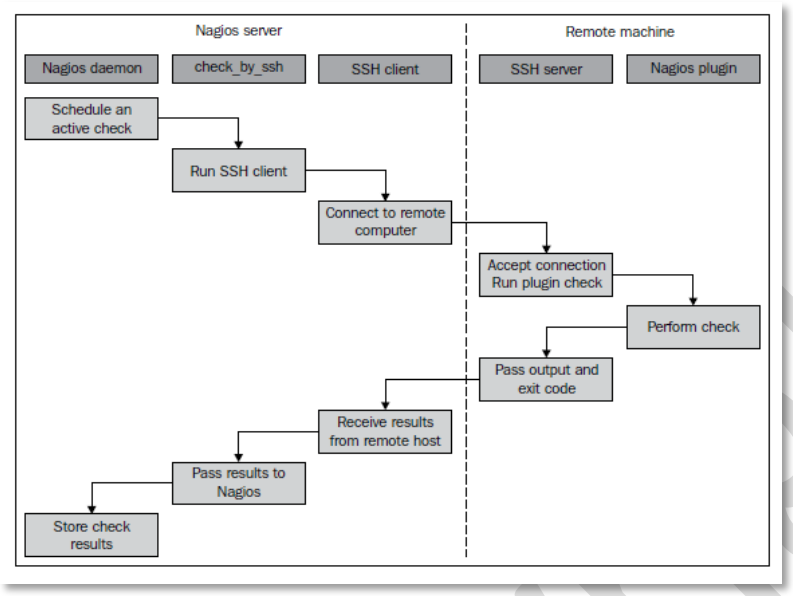

Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log
System
Comments
Downtime
Process Info
Current Network Status
Last Updated: Sat Apr 14 17:58:39 CEST 2012
Updated every 90 seconds
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
4 0 0 0
All Problems All Types
0 4
Service Status Totals
Ok Warning Unknown Critical Pending
24 0 0 0 0
All Problems All Types
0 24
Service Status Details For All Hosts
Host Service Status Last Check Duration Attempt Status Information
Clear_OS CPU Load OK 04-14-2012 17:51:17 0d 0h 37m 31s 1/3 OK - load average: 0.83, 0.87, 0.82
Check_Disk OK 04-14-2012 17:48:47 0d 1h 19m 59s 1/3 DISK OK - free space: / 4754 MB (73% inode=96%):
Current_Users OK 04-14-2012 17:51:05 0d 0h 47m 34s 1/3 USERS OK - 1 users currently logged in
Total_Processes OK 04-14-2012 17:55:28 0d 0h 53m 11s 1/3 PROCS OK: 88 processes
linux-client CPU Load OK 04-14-2012 17:58:29 0d 1h 20m 10s 1/3 OK - load average: 0.00, 0.01, 0.05
Check_Disk OK 04-14-2012 17:53:45 0d 1h 14m 54s 1/3 DISK OK - free space: /dev 241 MB (99% inode=99%):
Current_Users OK 04-14-2012 17:55:48 0d 1h 12m 56s 1/3 USERS OK - 4 users currently logged in
Total_Processes OK 04-14-2012 17:56:41 0d 1h 11m 58s 1/3 PROCS OK: 138 processes
localhost Current_Load OK 04-14-2012 17:54:54 50d 10h 38m 40s 1/4 OK - load average: 0.01, 0.06, 0.06
Current_Users OK 04-14-2012 17:54:21 50d 10h 38m 2s 1/4 USERS OK - 5 users currently logged in
DHCP OK 04-14-2012 17:55:45 0d 0h 38m 2s 1/4 OK: Received 1 DHCPOFFER(s), max lease time = 43200 sec.
HTTP OK 04-14-2012 17:54:21 19d 3h 2m 47s 1/4 HTTP OK: HTTP/1.1 200 OK - 262 bytes in 0.002 second response time
PING OK 04-14-2012 17:58:17 49d 7h 39m 32s 1/4 PING OK - Packet loss = 0%, RTA = 0.07 ms
Root_Partition OK 04-14-2012 17:57:49 16d 7h 48m 50s 1/4 DISK OK - free space: / 794 MB (16% inode=56%):
SSH OK 04-14-2012 17:53:42 0d 12h 19m 57s 1/4 SSH OK - OpenSSH_5.8 (protocol 2.0)
Swap_Usage OK 04-14-2012 17:57:46 50d 10h 34m 55s 1/4 SWAP OK - 87% free (646 MB out of 743 MB)
Total_Processes OK 04-14-2012 17:57:52 50d 10h 34m 17s 1/4 PROCS OK: 65 processes with STATE = RSZDT
winserver C:\ Drive_Space OK 04-14-2012 17:57:22 0d 0h 2m 26s 1/3 c: - total: 10.39 Gb - used: 4.55 Gb (44%) - free 5.84 Gb (56%)
CPU_Load OK 04-14-2012 17:55:58 0d 0h 2m 54s 1/3 CPU Load 0% (5 min average)
Explorer OK 04-14-2012 17:56:37 0d 0h 2m 6s 1/3 Explorer.EXE: Running
IEXPLORE - Browser OK 04-14-2012 17:58:32 0d 0h 0m 11s 1/3 iexplore.exe: Running
Memory_Usage OK 04-14-2012 17:55:46 0d 0h 2m 53s 1/3 Memory usage: total:2014.75 Mb - used: 196.39 Mb (10%) - free: 1818.36 Mb (90%)
NSClient++ Version OK 04-14-2012 17:58:08 0d 0h 0m 41s 1/3 NSClient++ 0.3.9.327 2011-08-16
Uptime OK 04-14-2012 17:56:38 0d 0h 2m 1s 1/3 System Uptime - 0 day(s) 1 hour(s) 10 minute(s)


Service Overview For All Host Groups
Clear OS (Clear_OS)
Host Status Services Actions
Clear_OS UP 1 OK
Linux Servers (linux-servers)
Host Status Services Actions
linux-client UP 4 OK
localhost UP 9 OK
Windows Servers (windows-servers)
Host Status Services Actions
winserver UP 7 OK

6.4.6 Controle via SSHD

In variante zullen we Clear OS met sshd monitoren ipv NRPE.

Vanuit de Nagios server wordt een check bepaald. Via ssh wordt hij op de remote server uitgevoerd. De Remote server stuurt zijn antwoord naar de nagios server terug via ssh. Nagios server archiveert en verwerkt het antwoord.



De volledige configuratie van ssh-check gebeurt vanuit de Nagios Server. We maken als nagios user een public/private key aan met het commando **ssh-keygen –t dsa**

De Authorized key dient in **/root/.ssh/** van ClearOS weggeschreven te worden. Via scp kan je een bestand vanuit je locatie naar een andere machine wegschrijven. Dit met het commando:

scp /home/nagios/.ssh/id_dsa.pub root@10.10.10.254:/root/.ssh/authorized_keys

```
nagios@nagios-monitor:/> ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/nagios/.ssh/id_dsa):
/home/nagios/.ssh/id_dsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nagios/.ssh/id_dsa.
Your public key has been saved in /home/nagios/.ssh/id_dsa.pub.
The key fingerprint is:
b7:6e:f4:9b:92:9c:92:58:82:da:85:46:fc:1b:46:a3 nagios@nagios-monitor
The key's randomart image is:
+--[ DSA 1024]----+
|                 |
|                 |
|   .             |
|    o o          |
|   . * .S .      |
|    E * ....     |
|   + o * +.+     |
|  . . o o.* ..   |
|         o..o.   |
+-----------------+
nagios@nagios-monitor:/> scp /home/nagios/.ssh/id_dsa.pub root@10.10.10.254:/root/.ssh/authorized_keys
root@10.10.10.254's password:
id_dsa.pub                                                    100%  611     0.6KB/s   00:00
```

Vervolgens dienen we op beide machines sshd te herstarten om de key's te actualiseren.

Service sshd restart

We kunnen controleren of we via Nagios Monitoring Server de gewenste gegevens uit ClearOS kunnen inlezen

```
nagios@nagios-monitor:/> ssh root@10.10.10.254 /usr/local/nagios/libexec/check_users -w 5 -c 10
USERS OK - 1 users currently logged in |users=1;5;10;0
nagios@nagios-monitor:/> ssh root@10.10.10.254 /usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/disk
DISK OK - free space: / 4754 MB (73% inode=96%);| /=1752MB;5488;6174;0;6861
nagios@nagios-monitor:/> ssh root@10.10.10.254 /usr/local/nagios/libexec/check_procs -w 100 -c 150
PROCS OK: 87 processes
```

Als dit lukt maken we vervolgens een cfg bestand aan met de uit te voeren checks. Hiervoor heb ik enkele specifieke commando's in commands.cfg aangemaakt.

```
    I    objects/commands.cfg                                          Row 149  Col 1    7:14  Ctrl-K H
#
#### check SSH ##############
# 'check sshd commands'
define command{
        command_name    check_remote_users
        command_line    ssh  root@10.10.10.254 /usr/local/nagios/libexec/check_users -w 5 -c 10
        }
define command{
        command_name    check_remote_load
        command_line    ssh root@10.10.10.254 /usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20
}

define command{
        command_name    check_remote_disk
        command_line    ssh root@10.10.10.254 /usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/disk
}
define command{
        command_name    check_remote_total_procs
        command_line    ssh root@10.10.10..254 /usr/local/nagios/libexec/check_procs -w 100 -c 150
}
```

In ClearOS.cfg zijn volgende elementen terug te vinden

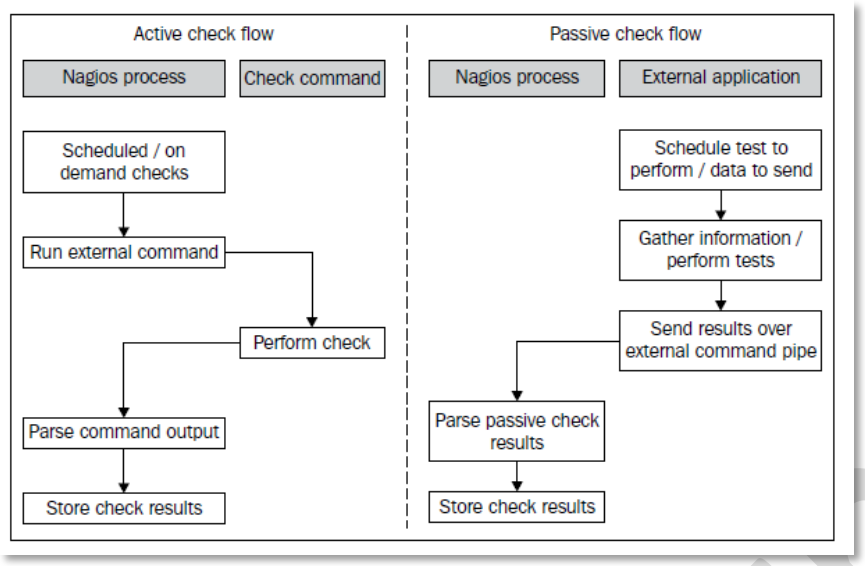
```
define host{
        name                            linux-smooth    ; The name of this host template
        use                             generic-host    ; This template inherits other values from the generic-host template
        check_period                    24x7            ; By default, Linux hosts are checked round the clock
        check_interval                  5               ; Actively check the host every 5 minutes
        retry_interval                  1               ; Schedule host check retries at 1 minute intervals
        max_check_attempts              10              ; Check each Linux host 10 times (max)
        check_command                   check-host-alive ; Default command to check Linux hosts
        notification_period             workhours       ; Linux admins hate to be woken up, so we only notify during the day
                                                        ; Note that the notification_period variable is being overridden from
                                                        ; the value that is inherited from the generic-host template!
        notification_interval           120             ; Resend notifications every 2 hours
        notification_options            d,u,r           ; Only send notifications for specific host states
        contact_groups                  admins          ; Notifications get sent to the admins by default
        register                        0               ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }

# We define a generic printer template that can be used for most printers we monitor

define host{
        use                     linux-smooth
        host_name               linux-clearOS
        alias                   ClearOS via SSH
        address                 10.10.10.254    ; Inherit default values from the generic-host template
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-clearOS
        service_description             check Remote Load
        check_command                   check_remote_load
        }
define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-clearOS
        service_description             check Remote Disk
        check_command                   check_remote_disk
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-clearOS
        service_description             check Remote Users
        check_command                   check_remote_users
        }

define service{
        use                             generic-service         ; Inherit default values from the generic-service definition
        host_name                       linux-clearOS
        service_description             check Remote Total Procs
        check_command                   check_remote_total_procs
        }
```

Hierbij de vergelijking tussen de verschillende checks.

ClearOS wordt met NRPE uitgevoerd – Linux-ClearOS via SSH

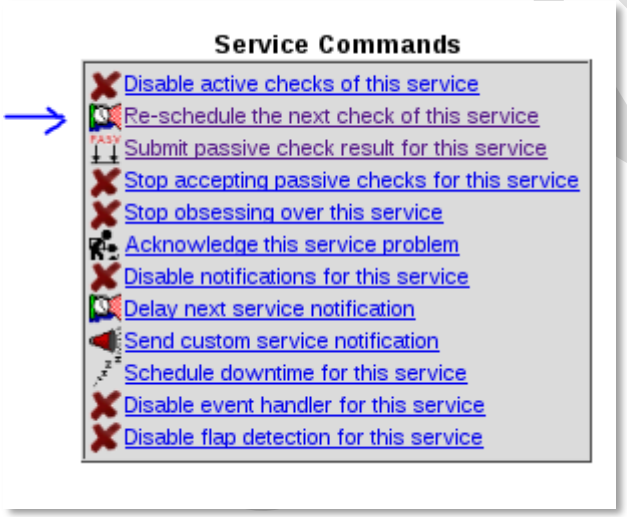
Host	Service	Status	Last Check	Duration	Attempt	Status Information
Clear_OS	CPU Load	OK	04-14-2012 20:11:17	0d 2h 52m 43s	1/3	OK - load average: 0.99, 0.95, 0.86
	Check Disk	OK	04-14-2012 20:08:47	0d 3h 35m 11s	1/3	DISK OK - free space: / 4754 MB (73% inode=96%):
	Current Users	OK	04-14-2012 20:11:05	0d 3h 2m 46s	1/3	USERS OK - 1 users currently logged in
	Total Processes	OK	04-14-2012 20:05:28	0d 3h 8m 23s	1/3	PROCS OK: 88 processes
linux-clearOS	check_Remote_Disk	OK	04-14-2012 20:10:57	0d 0h 2m 58s	1/3	DISK OK - free space: / 4754 MB (73% inode=96%):
	check_Remote_Load	OK	04-14-2012 20:11:21	0d 0h 2m 39s	1/3	OK - load average: 0.91, 0.93, 0.86
	check_Remote_Total_Procs	OK	04-14-2012 20:11:44	0d 0h 2m 22s	1/3	PROCS OK: 87 processes
	check_Remote_Users	OK	04-14-2012 20:12:03	0d 0h 1m 53s	1/3	USERS OK - 1 users currently logged in

6.5 Wat is het verschil met Active en Passieve Check

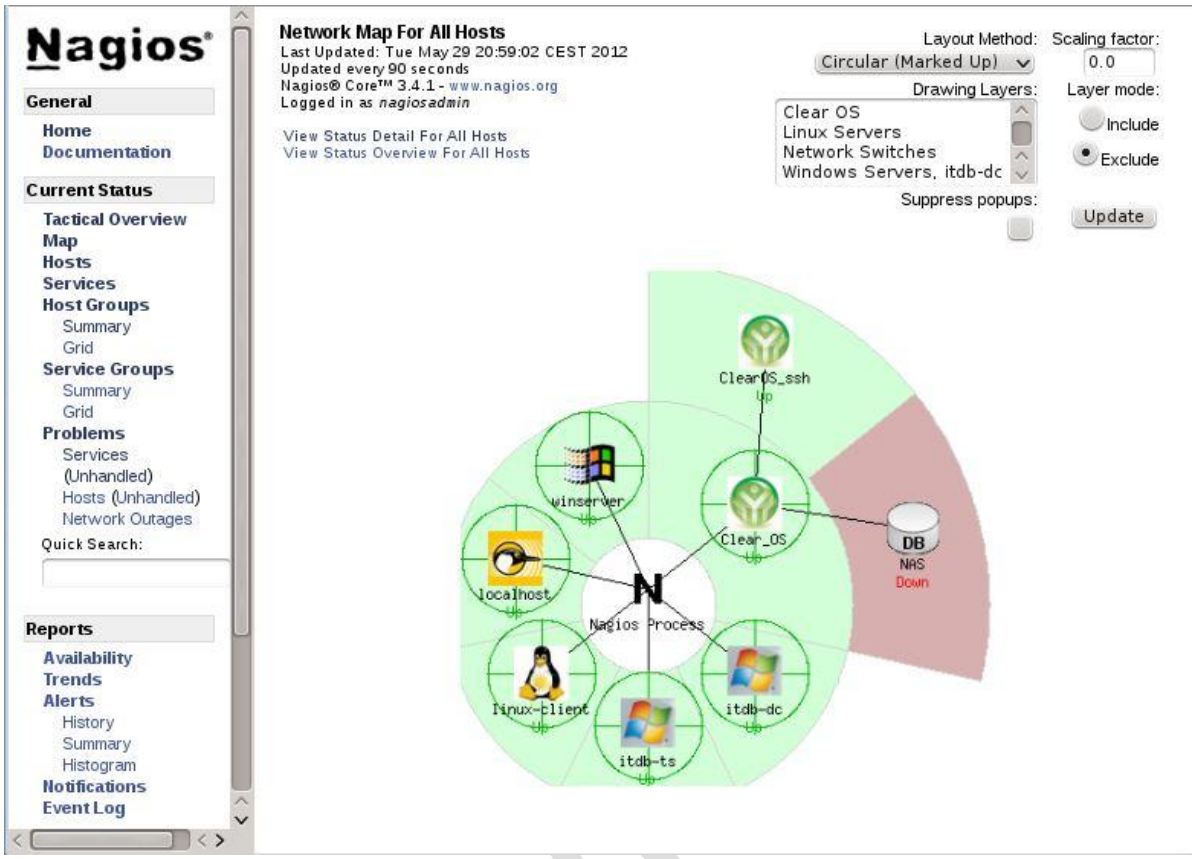


Een active check gebeurt wanneer nagios monitoring server zelf een check gaat opvragen. Bij een passieve check luistert de nagios monitroing server naar een check resultaat die binnenkomt.

Bij een installatie kan het handig zijn om vlugger een antwoord binnen te krijgen. Gebruik volgend link. Hierbij wachten we de ingestelde tijdsinterval niet af.



6.6 Personaliseren van Nagios

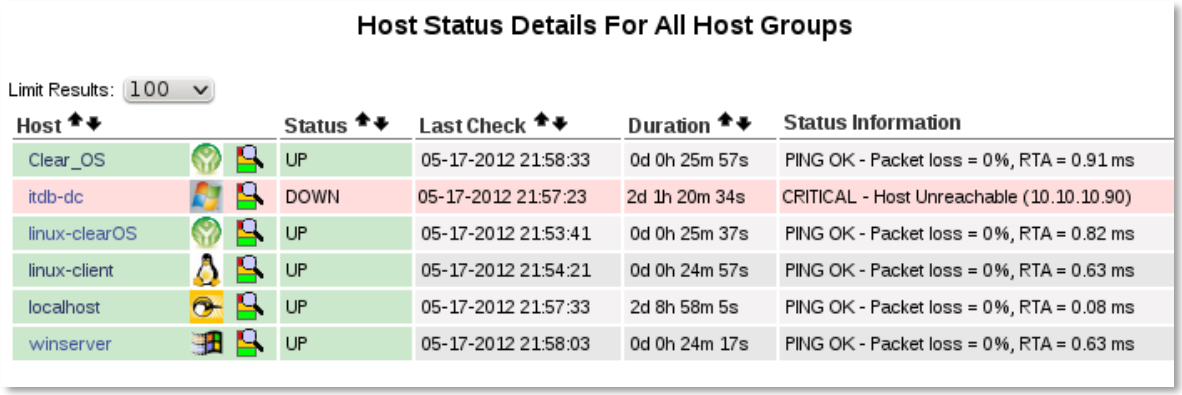


We kunnen in Nagios d.m.v. **MAP** een overzicht van de gemonitorde configuratie visualiseren. In ons geval monitoren we een kleine KMO. Via één centrale switch spreken we de verschillende toestellen aan vandaar de stervormige structuur. Mochten we over verschillende switchen communiceren of nog een tree of een forest-structuur in ons domein hebben dan worden de vertakkingen overzichtelijk gevisualiseerd. Met de informatie unreachable of down kan je beter begrijpen waarom een deelnemer niet meer aanspreekbaar is.

In ons geval bevinden de standard iconen-images zich op : **/usr/local/nagios/share/images/logos.** Je bepaalt in de *.cfg file bij **define host** welk logo je wenst te visualiseren voor die deelnemer.

```
define host{
        use             windows-server  ; Inherit default values from a template
        host_name       winserver       ; The name we're giving to this host
        alias           My Windows Server       ; A longer name associated with the host
        address         10.10.10.130    ; IP address of the host
        icon_image      win40.png
        statusmap_image win40.png
        }
```

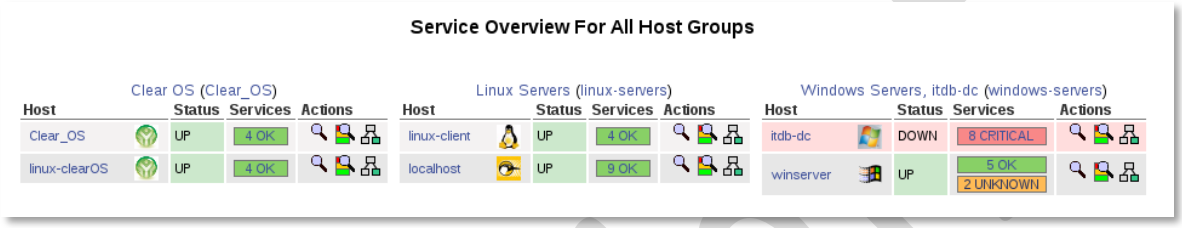
De iconen worden vanaf nu in alle verschillende schermen meegenomen.



Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
Clear_OS	UP	05-17-2012 21:58:33	0d 0h 25m 57s	PING OK - Packet loss = 0%, RTA = 0.91 ms
itdb-dc	DOWN	05-17-2012 21:57:23	2d 1h 20m 34s	CRITICAL - Host Unreachable (10.10.10.90)
linux-clearOS	UP	05-17-2012 21:53:41	0d 0h 25m 37s	PING OK - Packet loss = 0%, RTA = 0.82 ms
linux-client	UP	05-17-2012 21:54:21	0d 0h 24m 57s	PING OK - Packet loss = 0%, RTA = 0.63 ms
localhost	UP	05-17-2012 21:57:33	2d 8h 58m 5s	PING OK - Packet loss = 0%, RTA = 0.08 ms
winserver	UP	05-17-2012 21:58:03	0d 0h 24m 17s	PING OK - Packet loss = 0%, RTA = 0.63 ms



Service Overview For All Host Groups

Clear OS (Clear_OS)

Host	Status	Services	Actions
Clear_OS	UP	4 OK	
linux-clearOS	UP	4 OK	

Linux Servers (linux-servers)

Host	Status	Services	Actions
linux-client	UP	4 OK	
localhost	UP	9 OK	

Windows Servers, itdb-dc (windows-servers)

Host	Status	Services	Actions
itdb-dc	DOWN	8 CRITICAL	
winserver	UP	5 OK 2 UNKNOWN	

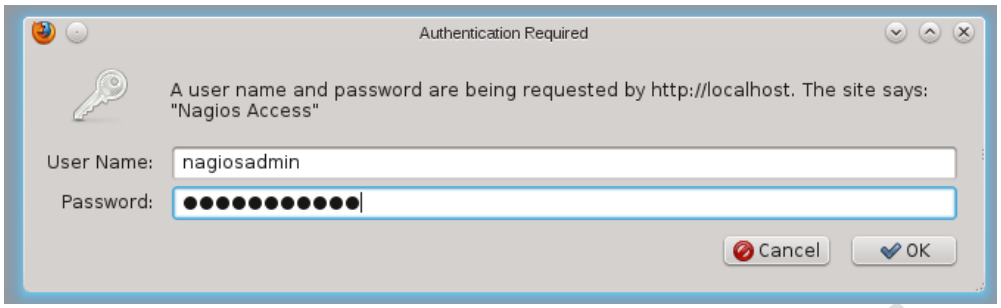
Met **parents** kan je een hiërarchie opzetten

```
define host{
        name                            linux-smooth    ; The name of this host template
        use                             generic-host    ; This template inherits other values from the generic-host template
        check_period                    24x7            ; By default, Linux hosts are checked round the clock
        check_interval                  5               ; Actively check the host every 5 minutes
        retry_interval                  1               ; Schedule host check retries at 1 minute intervals
        max_check_attempts              10              ; Check each Linux host 10 times (max)
        check_command                   check-host-alive ; Default command to check Linux hosts
        notification_period             workhours       ; Linux admins hate to be woken up, so we only notify during the day
                                                        ; Note that the notification_period variable is being overridden from
                                                        ; the value that is inherited from the generic-host template!
        notification_interval           120             ; Resend notifications every 2 hours
        notification_options            d,u,r           ; Only send notifications for specific host states
        contact_groups                  admins          ; Notifications get sent to the admins by default
        register                        0               ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }

# We define a generic printer template that can be used for most printers we monitor

define host{
        use                     linux-smooth
        host_name               ClearOS_ssh
        alias                   ClearOS via SSH
        address                 10.10.10.254    ; Inherit default values from the generic-host template
        icon_image              clearos.jpg
        statusmap_image         clearos2.png
        parents                 Clear_OS
        }
```

6.7 Welke beveiligingen voorzien we in onze installatie.

6.7.1 Passwoorden bij Nagios

Standaard wordt de toegang tot Nagios Apache webapplicatie beveiligd door wachtwoorden.



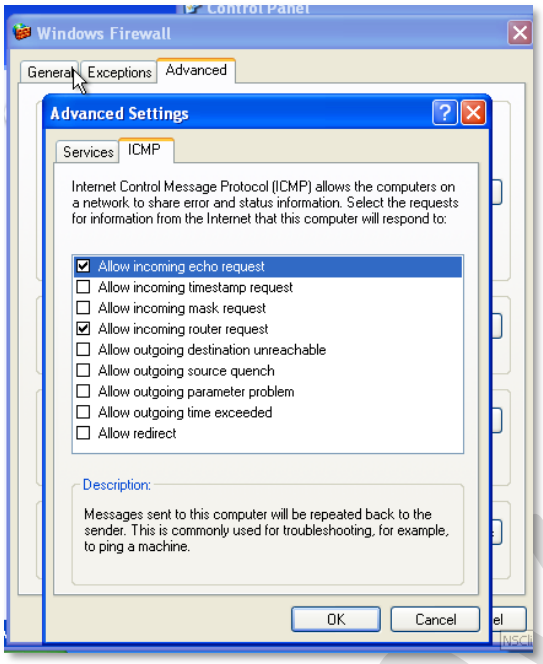
De instelling om de security policy aan te passen gebeurt in volgend bestand **/usr/local/nagios/etc/cgi.cfg**

6.7.2 Firewall beveiliging opzetten

Verder worden bij al onze machines de Firewall geactiveerd. Om een correcte interactie te hebben met de nagios- monitoring server hadden we voordien de poort voor NRPE gedefinieerd.

NRPE poort 5666/tcp

Door de firewall op de windows machine actief te zetten komt de klassieke ping-commando niet meer binnen. Hierbij dien je volgende settings op de windows machine aan te passen.



6.8 Trouble Shooting bij Nagios

Bij de installatie hebben we natuurlijk verschillende probleempjes moeten trotseren. Hieronder een kleine oplijsting ervan.

- SSH Warning – Probleem met de key
  - **joe /root/.ssh/known_hosts**
  - Verwijder de key in de file
  - **service sshd restart**

- check_NRPE – Could not complete SSL handshake
  - controleren in **/etc/xinetd.d/nrpe** of het IP-adres van de monitoring server juist is opgegeven **only_from=127.0.0.1 10.10.10.110**
  - controleer het IP-adres van de monitoring server
  - **service xinetd restart**

- log files consulteren om een probleem te begrijpen
  - **tail –f /var/log/messages**

- nog een handigheidje. We maken een batch file aan om nagios te testen.
  - **joe /home/<user>/nagiostest**

```
#!/bin/bash
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

We geven de juiste rechten zodat hij door iedere user kan uitgevoerd worden

- **chmod a+x nagiostest**

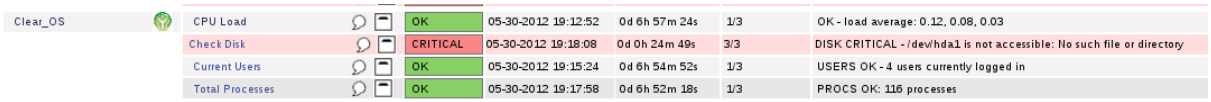
En het path toevoegen zodat hij vanuit iedere directory kan worden aangesproken

- **cd /usr/bin/**
- **ln –s /home/<user>/nagiostest nagiostest**

of

- kopieer de batch file naar de folder /user/bin

- Info check_disk van nrpe client komt niet binnen.



Clear_OS	CPU Load	OK	05-30-2012 19:12:52	0d 6h 57m 24s	1/3	OK - load average: 0.12, 0.08, 0.03
	Check Disk	CRITICAL	05-30-2012 19:18:08	0d 0h 24m 49s	3/3	DISK CRITICAL - /dev/hda1 is not accessible: No such file or directory
	Current Users	OK	05-30-2012 19:15:24	0d 6h 54m 52s	1/3	USERS OK - 4 users currently logged in
	Total Processes	OK	05-30-2012 19:17:58	0d 6h 52m 18s	1/3	PROCS OK: 116 processes

De status van de disk uit Clear Os wordt verkeerdelijk gelezen. Door het commando df te gebruiken vind je de locatie en benaming van de disk-devices.

```
[root@system etc]# df
Bestandssysteem      1K-blokken     Gebruikt Beschikbaar Gebruikt% Aangekoppeld op
/dev/sda3            149384896    2588952 139085148    2% /
/dev/sda1                77749      11414      62321   16% /boot
tmpfs                   972212          0     972212    0% /dev/shm
```

Op ClearOS (nrpe client) passen we volgend bestand aan **/usr/local/nagios/etc/nrpe.cfg**

Initiele gegevens

```
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10
command[check_load]=/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20
command[check_hda1]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/hda1
command[check_zombie_procs]=/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/local/nagios/libexec/check_procs -w 150 -c 200
```

Vervangen door

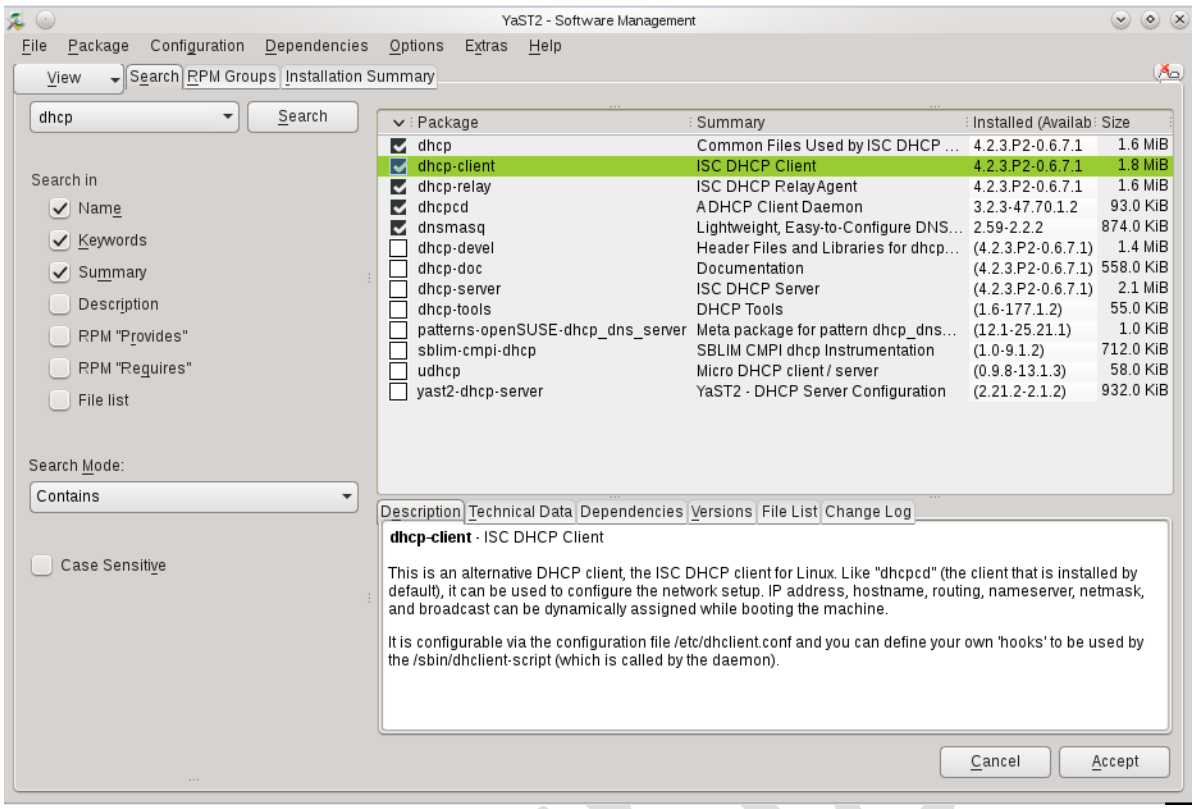
```
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10
command[check_load]=/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20
command[check_hda1]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/sda3
command[check_zombie_procs]=/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/local/nagios/libexec/check_procs -w 150 -c 200
```

Service xinetd restart en zoals je onderstaand kan zien wordt de informatie nu correct ingelezen en doorgestuurd

Controle vanuit de monitoring server.

```
linux-nagios-monitor:/home/pascal # /usr/local/nagios/lib/check_nrpe -H 10.10.10.254 -c check_hda1
DISK CRITICAL - /dev/hda1 is not accessible: No such file or directory
linux-nagios-monitor:/home/pascal # /usr/local/nagios/lib/check_nrpe -H 10.10.10.254
NRPE v2.13
linux-nagios-monitor:/home/pascal # /usr/local/nagios/lib/check_nrpe -H 10.10.10.254 -c check_hda1
DISK OK - free space: / 135825 MB (98% inode=99%);| /=2528MB;116706;131294;0;145883
```

- DCHP service komt niet binnen bij nagios als als rcSuSEfirewall actief is
  Installatie van DCHP client via Yast2 om het probleem te verhelpen.



7 Domain Controller

7.1 Wat?

Domein Controller
Een domeincontroller is een server in een computernerwerk van Micosoft Windows die centraal beheert wie er toegang tot welke stukken van het domein mag hebben. Dit in tegenstelling tot het werkgroep-model, waarbij gebruikers en toegang op iedere individuele computer ingesteld moeten worden.

File Server
Een fileserver (of bestandsserver) is een computer die Network Attached Storage ter beschikking stelt aan clients. Veel gebruikte protocollen zijn FTP, NFS, SMB.
Bestandsservers kunnen RAID gebruiken om de snelheid en betrouwbaarheid van het lezen en schrijven te vergroten.

Backup-server
Het onderdeel Windows Server Backup in Windows Server 2008 bestaat uit een Microsoft Management Console Module en opdrachtregelprogramma's die samen een complete oplossing vormen voor het maken en terugzetten van back-up's.
Met Windows Server Backup kunt u een back-up maken van een volledige server (alle volumes), geselecteerde volumes of de systeemstatus. U kunt volumes, mappen, bestanden, bepaalde toepassingen en de systeemstatus herstellen. En in een noodgeval, bijvoorbeeld als een vaste schijf uitvalt, kunt u uw volledig systeem op een nieuwe vaste schijf terugzetten met behulp van een volledige serverback-up en de Windows Herstelomgeving.

!Noot: het is niet aangeraden om de fileserver en de back-up server op de domeincontroller te zetten. Toch wegens wij op klein labo model werken gaan we wegens plaatsgebrek van een extra server dit toch doen om de nodige uitleg te geven.

7.2 Benodigheden

De systeemvereisten voor Windows Server 2008 R2 zijn als volgt:

Component	Vereiste
Processor	Minimaal: een processor met 1,4 GHz (x64 processor) of 1,3 GHz (Dual Core). Opmerking: Een Intel Itanium 2-processor is vereist voor Windows Server 2008 R2 voor Itanium-systemen.
Geheugen	Minimum: 512 MG RAM. Maximum: 8 GB (Stichting) of 32 GB (standaard) of 2 TB (Enterprise, Datacenter, en Itanium-systemen).
Vereisten voor schijfruimte	Minimum: 32 GB of groter. Opmerking: Computers met meer dan 16 GB RAM-geheugen zal meer schijfruimte voor pagin, hibernate, en dump bestanden vereisen.
Grafish	Super VGA (800 x 600) of hogere resolutie.
Andere	DVD Drive, Toetsenbord en Microsoft Mouse (of compatibel aanwijsapparaat), internettoegang (tegen betaling).

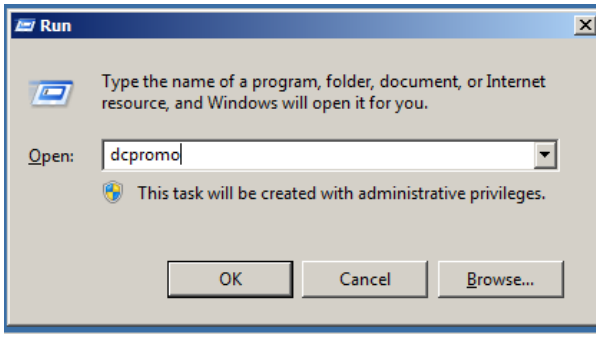
!Let op: Deze eisen zijn afhankelijk van de verschillende toepassingen en functies die u wilt installeren.

7.3 Installatie

Standaard installatie van een windows server 2008 kan je vinden in het boek “Inleiding Windows Server 2008” van Gunther Van Bleyenbergh hoodstuk 2 Installatie en configuratie.
Of via de mediaclip 2-1 De installatie van Windows Server 2008 op
http://www.academicservice.nl/site/downloadsinleidingwindowsserver2008.html

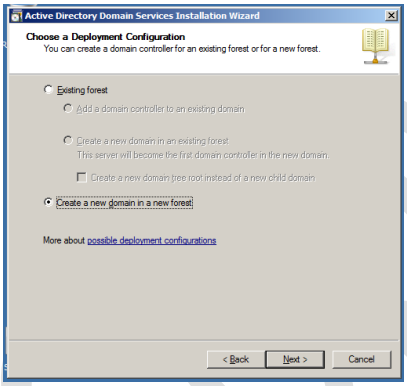
7.3.1 Installatie van de Domein Controller.

Voor je begint met het installeren van de Domein Controller zorg je ervoor dat je computer een vast IP adres heeft of dat de DHCP een vast IP adres geeft aan deze computer. Wij zorgen ervoor dat ClearOS een vast IP geeft aan onze DC.
Geef je computer een unieke naam volgens de normen van een netwerkbeheerder.
Zijnde volgens: wat is het, waar staat hij, waarvoor moet het dienen.
Dus voor ons 'ptco-dc'

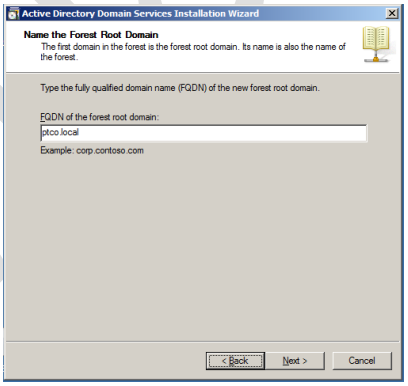


Type in de 'run-box' dcpromo.

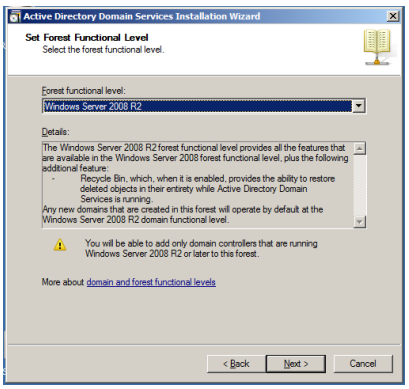
Je krijgt een scherm "Welkom bij de Active Directory Domein Service Installatie wizard". Klik evt. de box geavanceerde mode installatie.



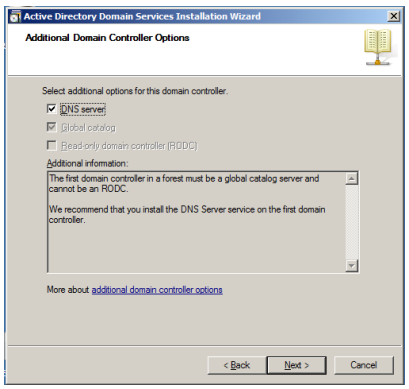
Op het volgende scherm kies je voor het aanmaken van een nieuw forest. Indien je al een bovenliggend domein hebt kan je kiezen voor de uitbreiding van een forest.



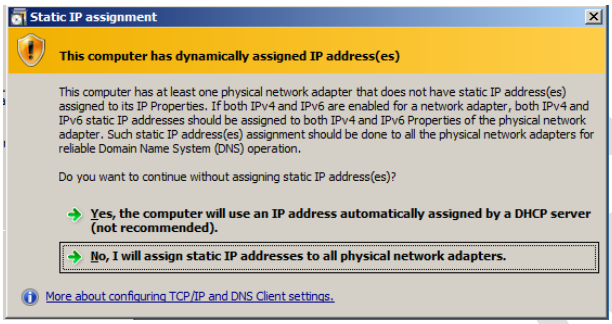
Geef een domein naam op. In onze virtuele toepassing ptco.local. Als je geavanceerde modus selecteerde Domein Netbios naam



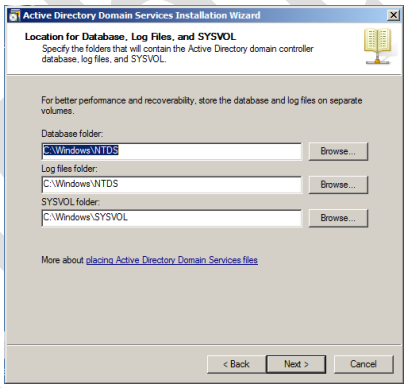
Geef het forest functioneel niveau. Aangezien onze tweede windows server ook een srv 2008 R2 zal zijn geven we hier dus de voorkeur aan 'Windows Server 2008 R2'.
Indien je weet dat een van je onderliggende server een srv 2003 zal zijn geef je hier dan ook de 'Windows Server 2003' mee.



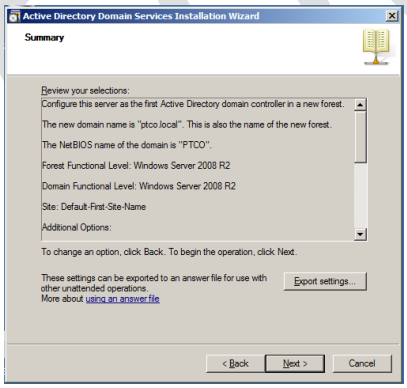
De wizard zal de DNS controleren en indien nodig deze aangeven om me te installeren.



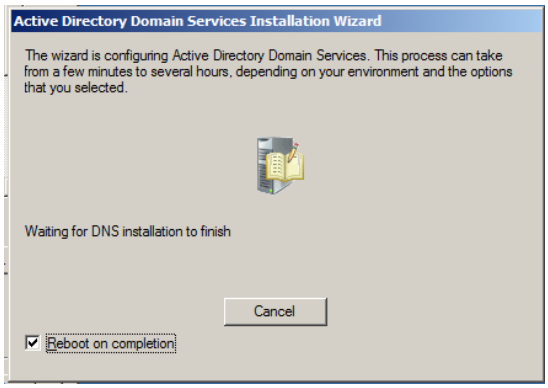
!Indien je geen vast IP adres hebt opgegeven zal je hier een bericht van krijgen om of een vast IP te geven of deze op dynamisch te laten staan.
!Indien er geen bovenliggende Windows DNS server is gevonden zal je hier ook een bericht over krijgen. Op de vraag of je verder wilt gaan klik je gewoon 'Ja'.



Op het volgende scherm kan je selecteren in welke map de database, log bestanden en de SYSVOL moet komen. Wij gaan deze niet veranderen en laten deze in de Windows map staan.



Geef een wachtwoord op voor de herstel administrator.
Nu krijg je een overzicht van wat je net hebt opgegeven. Klik op 'volgende' om de installatie te beginnen.



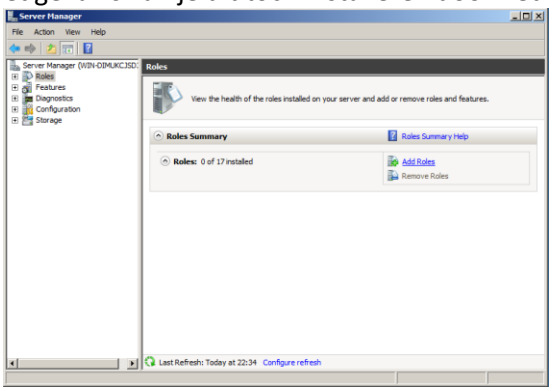
De installatie loopt en op het venster kan je evt. opgeven om te heropstarten na installatie.

*Na de herstart zie je dat de computer in een domein zit. Bij het aanmelden zie je voor de aanmeldingsnaam het domein staan. Zijnde “domeinnaam\gebruikersnaam”.
*Onder de administrative tools zul je merken dat volgende is geinstalleerd:

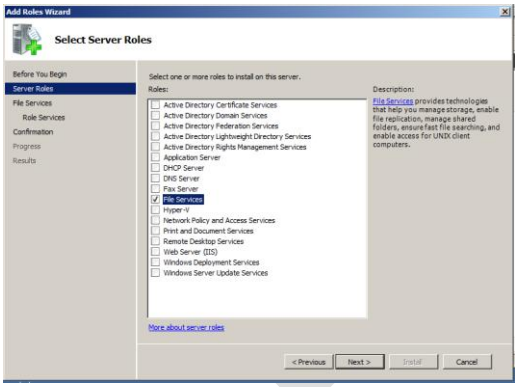
- Active Directory: Domein en vertrouwensrelaties
- Active Directory: Sites en services
- Active Directory: Gebruikers en computers
- Active Directory: Administratief centrum
- Active Directory-module voor powershell
- DNS
- Group Policy Management
- ADSI Edit

7.3.2 Installatie van de File Server.

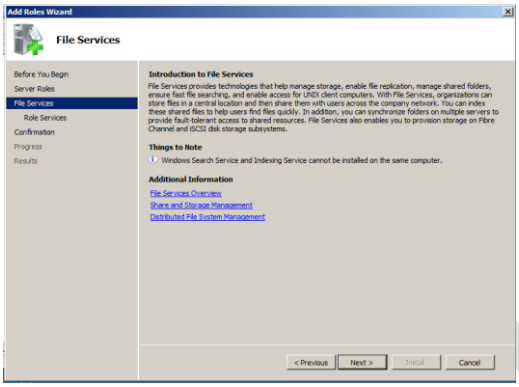
Normaal is de installatie van de file services al gebeurd bij het installeren van de DC. Indien dit niet het geval is kan je dit toch installeren door het volgende te doen.



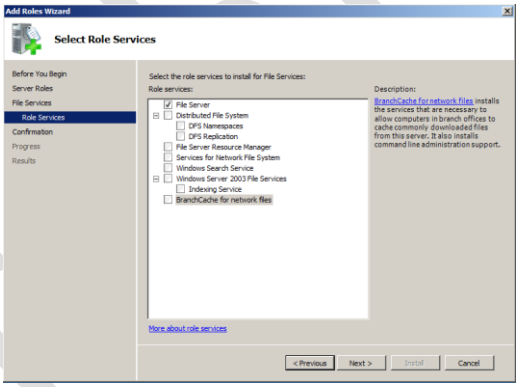
Start de server manager.
Ga naar roles > 'Add Roles'



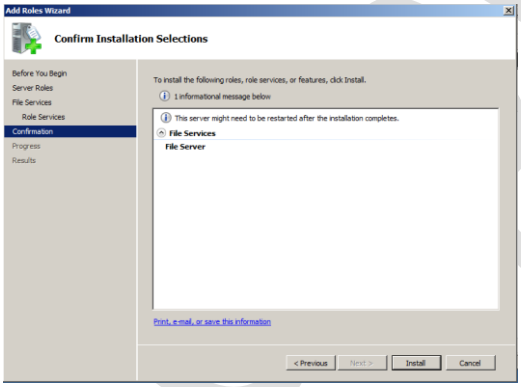
Selecteer de roles die je wil toevoegen > File Services.



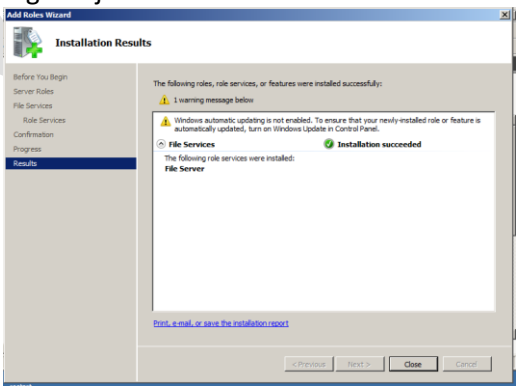
Bij het Introductie scherm krijg je nog wat meer informatie.



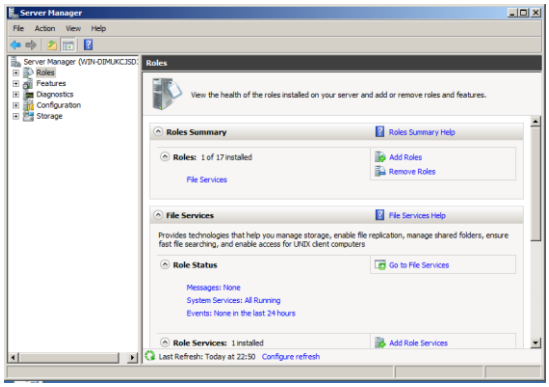
De Files Services staan al geselecteerd, indien nodig kan je extra services selecteren.



Klik op 'Install'.

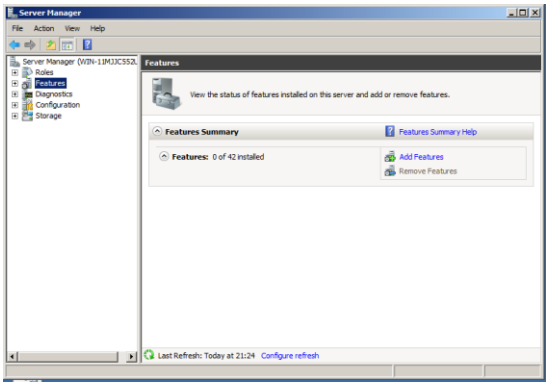


Na de installatie zie je in de server manager dat de role is toegevoegd.

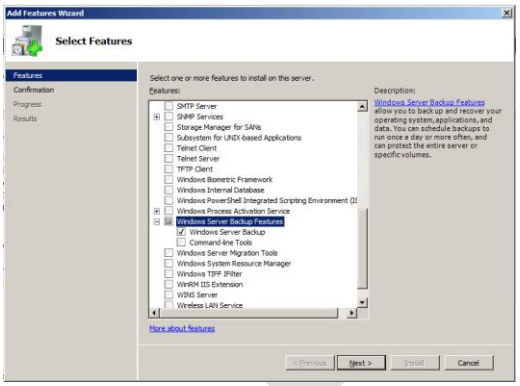


Indien je een extra services bij een geïnstalleerde role wil toevoegen druk je 'Add Role Service'.

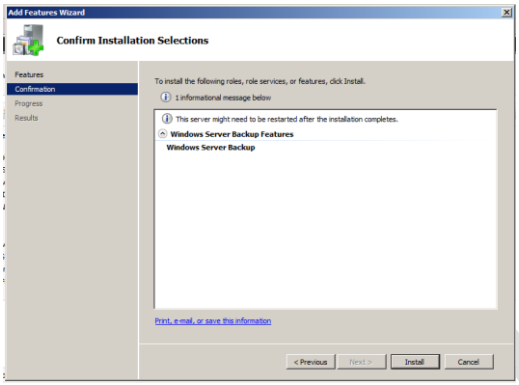
7.3.3 Installatie Backup Server.



Start de server manager.
Ga naar features > 'Add Features'.



Selecteer de features die je wil toevoegen > Windows Server Backup Features.



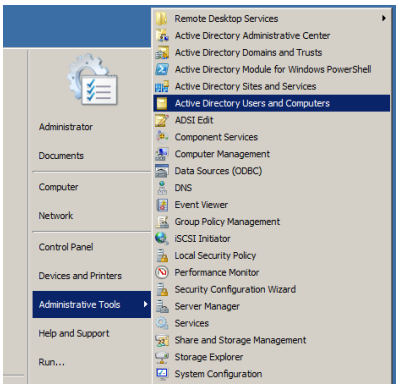
Klik op 'Install'.

Na de installatie zie je in de server manager dat de features is toegevoegd.

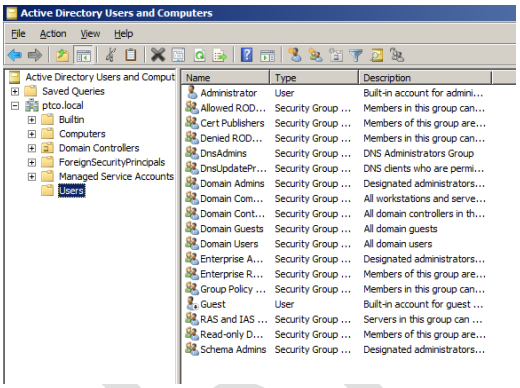
7.4 Configuratie

7.4.1 Configuratie Domein Controller.

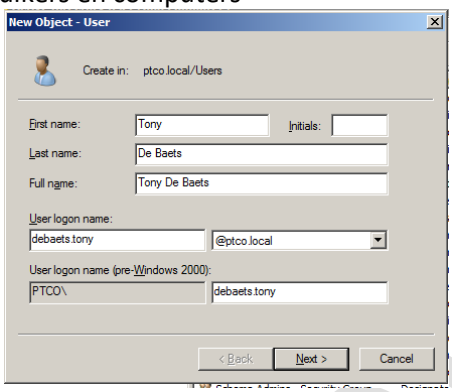
7.4.1.1 Gebruikers toevoegen.



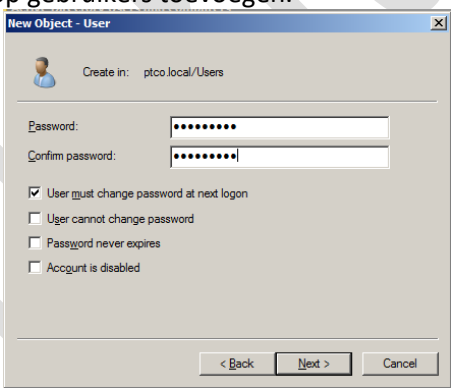
Ga naar Administratief tools > Active Directory: Gebruikers en computers



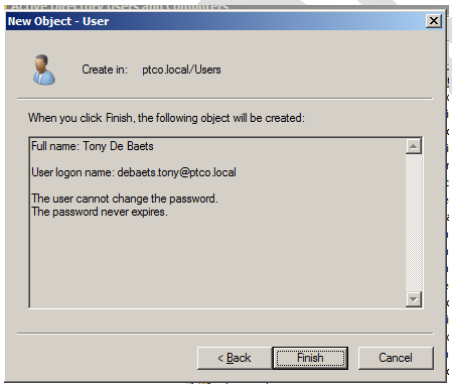
Onder je domein zie je gebruikers staan. Klik op gebruikers toevoegen.



Geef de naam en de aanmeldingsnaam.



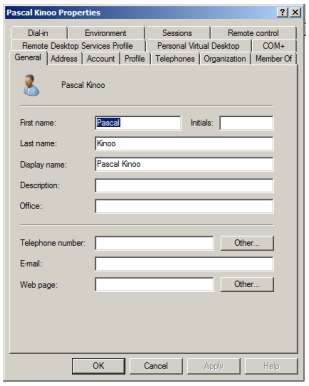
Geef een wachtwoord en selecteer evt. de extra opties. Gebruiker moet wachtwoord veranderen bij volgende aanmelding, wachtwoord vervalt nooit, ….



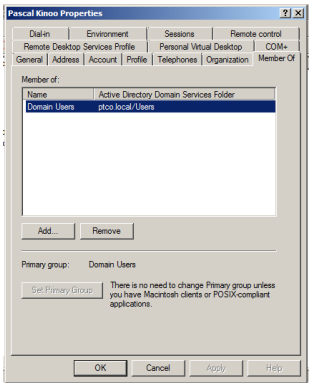
Klik op 'Finish' om de gebruiker op te slaan.

!Noot: Indien je een groot aantal gebruikers moet toevoegen kan je gebruik maken van een script met een database bestand waarin alle gebruikers staan met evt. extra gegevens vb. lidnummer, telefoonnummer, adres, ...

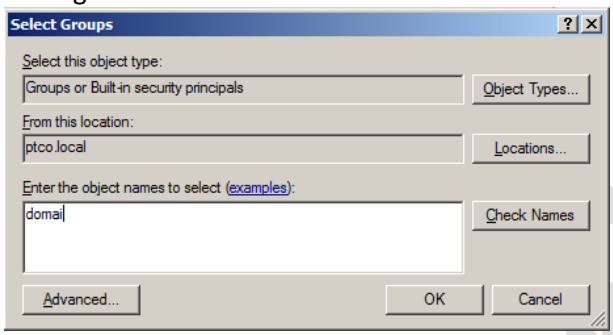
7.4.1.2 Gebruiker Domein Administrator maken.



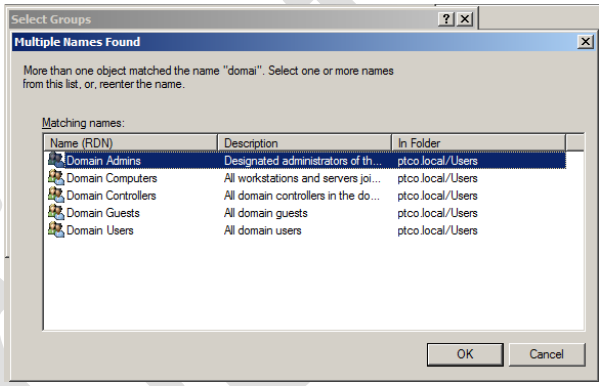
Dubbelklik op één van de twee gebruikers die we net hebben toegevoegd om de eigenschappen op te vragen.



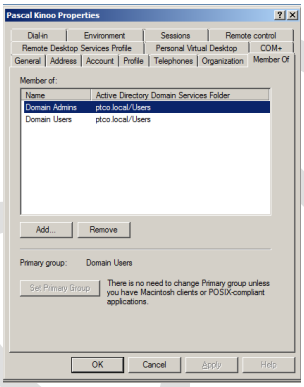
Ga naar het tabblad 'Member Of' en klik op 'Add'.



Geef de naam van de groep waarin ze lid mogen worden.



In ons geval 'Domain Admins'.



Klik op 'OK' om te bevestigen.

Maak evt. een Organisatie Unit aan om de gebruikers in te zetten.
Vb. Boekhedouding, Magazijn, Verkopers, …

7.4.1.3 *Rechten toekennen.*

Ga naar 'Group Policy Management'
Ga naar je domein onder 'Domains'
Klik met de rechtermuisknop op de OU waar je de rechten wilt van toekennen
Als er nog object inzit klik 'Create a GPO in this domain, and link it here'
Geef de nieuwe GPO een naam
Klik met de rechtermuisknop op het object en klik 'Edit'
Nu kan je voor dit object de rechten aanpassen naar wens.

Wij gaan volgende rechten aanpassen.
User configuration > Policies > Administrative Templates > Desktop > Desktop

*Desktop Wallpaper	
Wallpaper Name:	\\ptco-dc\Shared\logo.png
Wallpaper Style:	Center
*Enable Active Desktop	Enable
*Allow only bitmapped wallpaper	Disabled

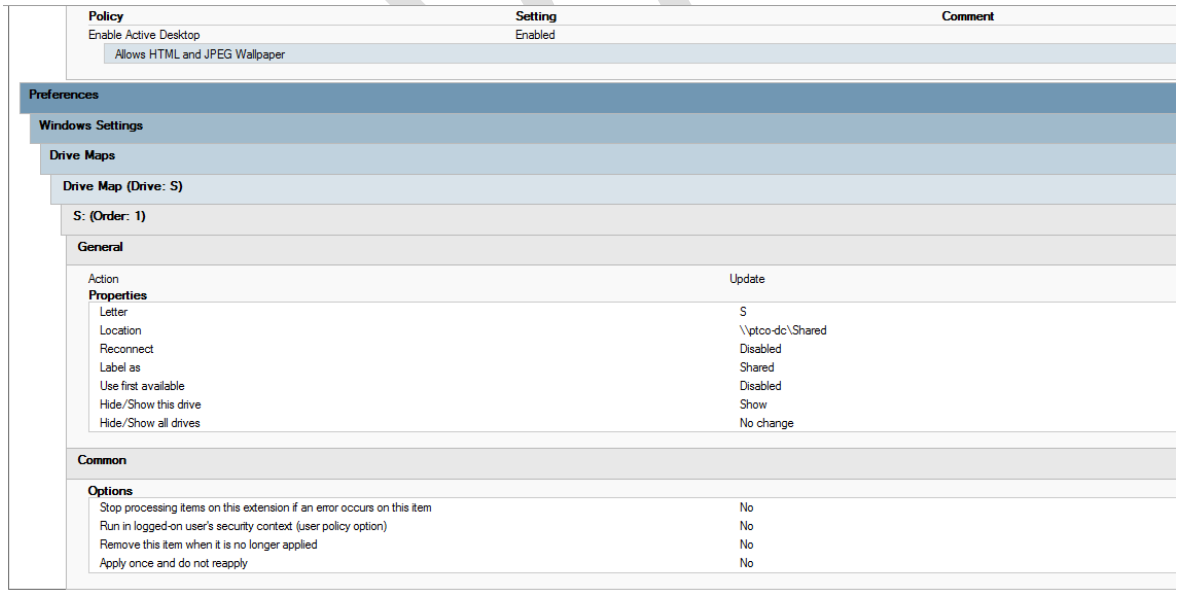
User configuration > Policies >Preferences > Windows Settings > Drive Maps

*Letter	S
*Location	\\ptco-dc\Shared
*Hide/show this drive	Show
De rest mag je laten staan zoals het staat.	

Met deze twee rechten zal de gebruiker ons logo op zijn desktop krijgen en wordt er een connectie gemaakt met de 'Shared' folder die wordt gezien als een extra drive nl. s:/

Als je op een object staat kan je naar de tap 'Settings' en krijg je samenvatting van alle rechten die je hebt toegekend. Met de rechter muisknop kan je deze dan opslaan als htm pagina.

Onderstaande is een deel van de pagina.



Policy	Setting	Comment
Enable Active Desktop	Enabled	
Allows HTML and JPEG Wallpaper		

Preferences

Windows Settings

Drive Maps

Drive Map (Drive: S)

S: (Order: 1)

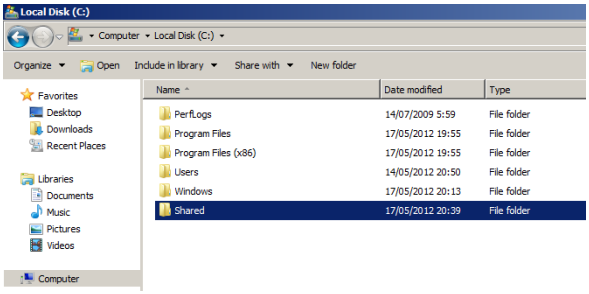
General

Action	Update
Properties	
Letter	S
Location	\\ptco-dc\Shared
Reconnect	Disabled
Label as	Shared
Use first available	Disabled
Hide/Show this drive	Show
Hide/Show all drives	No change

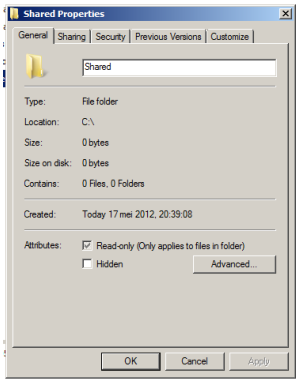
Common

Options	
Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

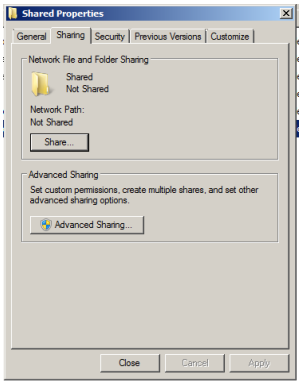
7.4.2 Configuratie File Server



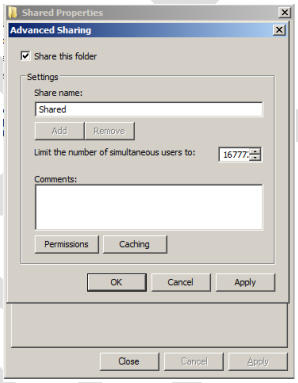
Ga naar deze computer en maak een nieuwe map aan Vb. Shared



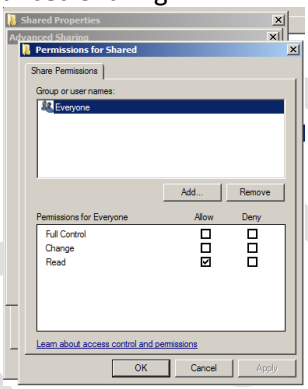
Vraag de eigenschappen van deze folder op.



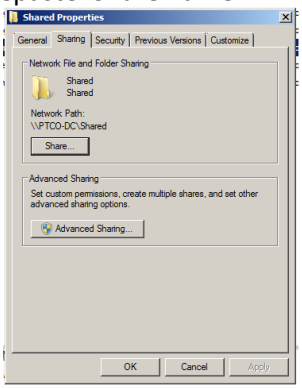
Ga naar het tabblad ‘Sharing’.
Klik op ‘Advanced Sharing’.



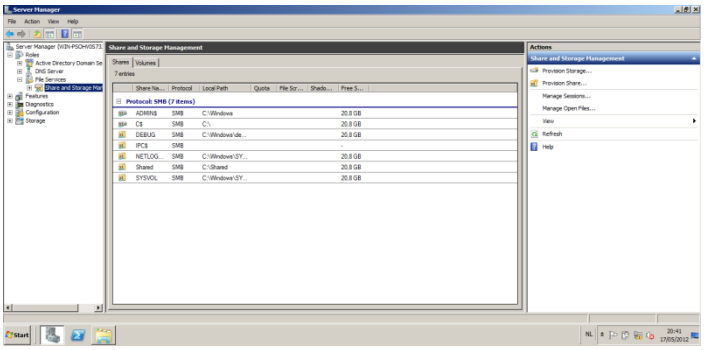
Selecteer ‘Share this folder’.
Geef een gepaste ‘Share name’ in.



Klik op de ‘permissions’.
Selecteer ‘Everyone’ en klik op ‘Full Control’.

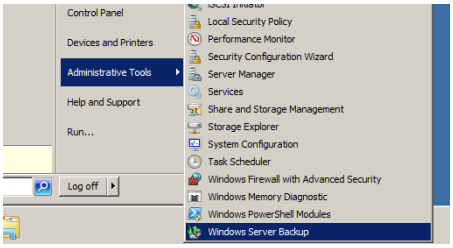


Druk 2x op OK om dit te bevestigen.
Bij de ‘Properties’ zie je nu dat de map wordt gedeeld.

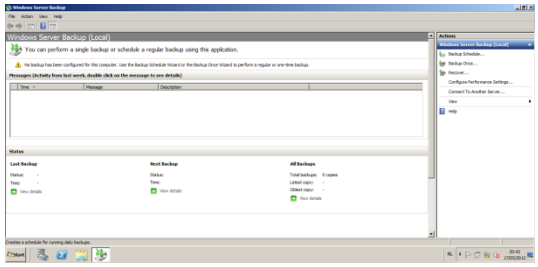


*Je kan dit controleren in de server manager.
Onder role file services heb je de ‘Share and Storage Management’ waar alle shares staan.

7.4.3 Configuratie BackUp Server



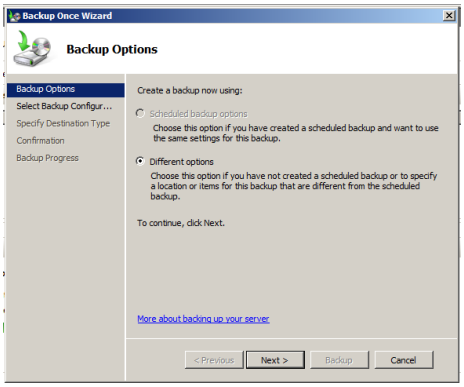
Ga naar Administratief tools > Windows Server Backup



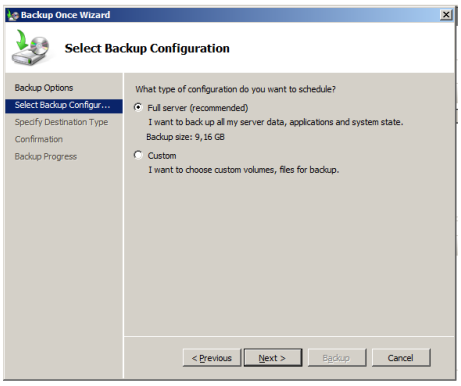
Rechts in het venster staan de verschillende acties die je kan selecteren.
Zoals Back-up schema, eenmalige backup, herstel.

!Wij gaan eerst een eenmalige backup doen van het volledige systeem en gaan een schema instellen van onze gedeelde map 'Shared'.

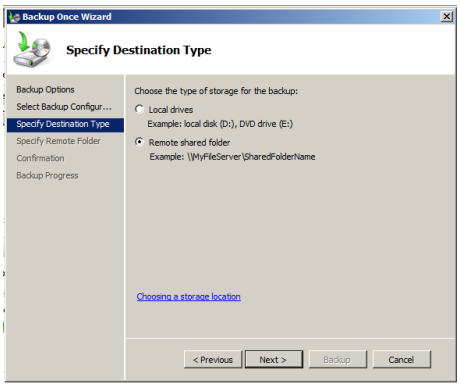
7.4.3.1 Eenmalige Back-up.



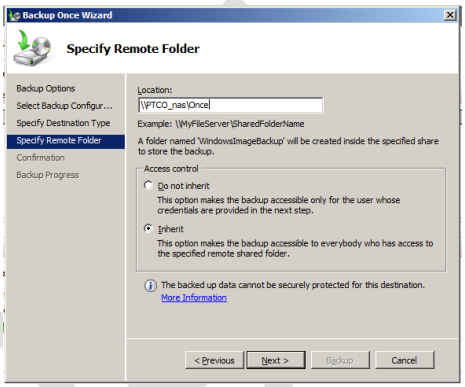
We hebben enkel maar de keuze voor Different options.



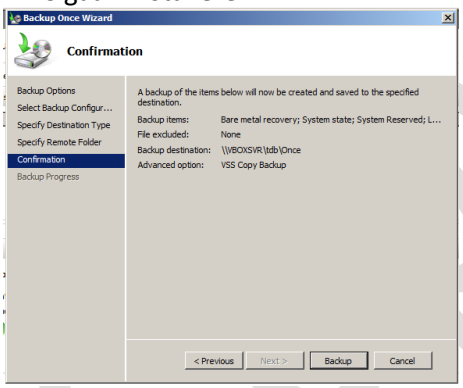
We kiezen hierna voor 'Full Server'.



'Remote Shared Folder' wegens we deze op onze NAS gaan installeren.

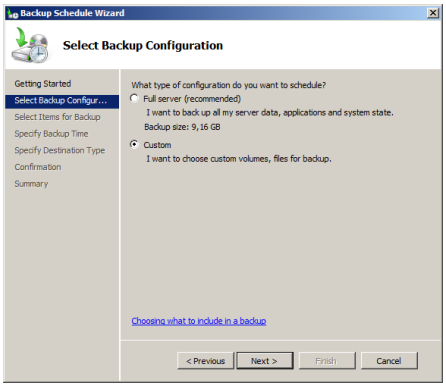


Geef het netwerkadres van de map op de NAS.

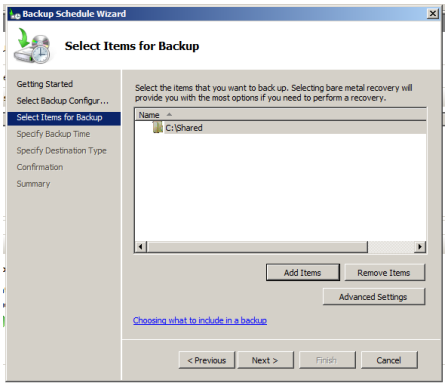


Klik op 'Backup' om deze te starten.

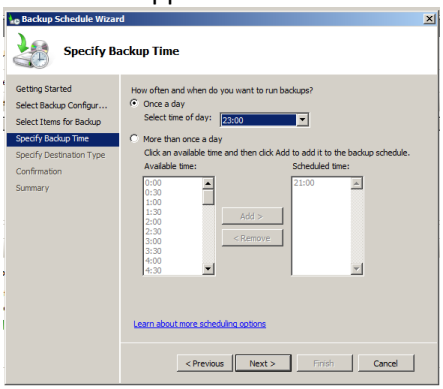
7.4.3.2 Back-up met een schema.



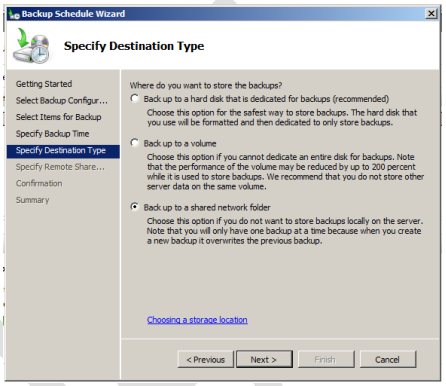
Klik op 'Custom'. Wegens we hier nu maar 1 map willen back-uppen.



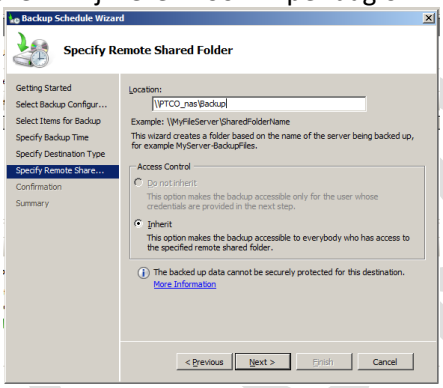
Via 'Add Items' selecteer je de map(pen).



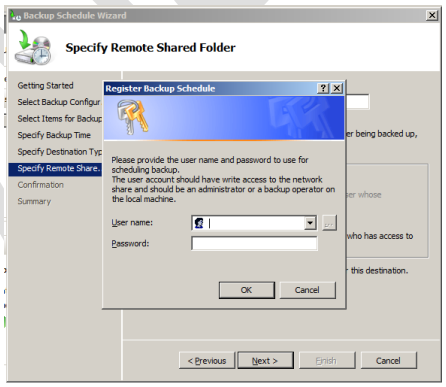
Geef de tijd(en) wanneer de back-up moet gebeuren. Wij kiezen voor 1x per dag om 23u.



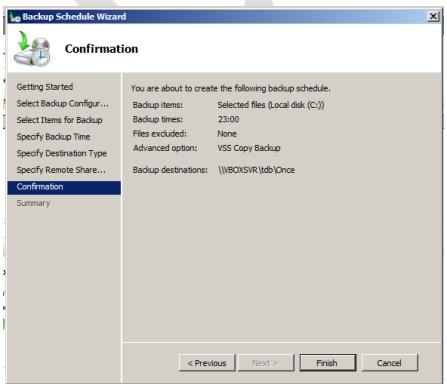
We nemen terug de 'Shared Network Foder'.



Geef het netwerkadres van de map op de NAS.



Geef een gebruiker in die de back-ups mag uitvoeren.



Klik op 'Finish' om het Back-up schema aan te maken.

!I.p.v. de 'Shared Network Foder' kan je ook kiezen voor 'een harde schijf die speciaal is bedoeld voor back-ups' of 'back-up op een volume'.

8 Remote Desktop Services

8.1 Wat?

Remote Desktop Services in Windows Server 2008 R2, voorheen bekend als Terminal Services in Windows Server 2008 en eerdere versies, is een van de onderdelen van Microsoft Windows (zowel server als client versies) waarmee een gebruiker tot applicaties en toegang tot de gegevens op een externe computer via een netwerk, met behulp van de Remote Desktop Protocol (RDP).
Terminal Services is Microsoft's implementatie van thin-client terminal server computing, waar Windows-applicaties, of zelfs het volledige bureaublad van de computer waarop Terminal Services, toegankelijk worden gemaakt voor een externe client machine.
Met Terminal Services wordt alleen de user interface van een applicatie gepresenteerd op de klant. Elke invoer wordt doorgestuurd over het netwerk naar de server, waar alle toepassingen de uitvoering plaatsvindt.
Microsoft veranderde de naam van Terminal Services om naar Remote Desktop Services met de release van Windows Server 2008 R2 in oktober 2009.

8.2 Benodigheden

De systeemvereisten voor Windows Server 2008 R2 zijn als volgt:

Component	Vereiste
Processor	Minimaal: een processor met 1,4 GHz (x64 processor) of 1,3 GHz (Dual Core). Opmerking: Een Intel Itanium 2-processor is vereist voor Windows Server 2008 R2 voor Itanium-systemen.
Geheugen	Minimum: 512 MG RAM. Maximum: 8 GB (Stichting) of 32 GB (standaard) of 2 TB (Enterprise, Datacenter, en Itanium-systemen).
Vereisten voor schijfruimte	Minimum: 32 GB of groter. Opmerking: Computers met meer dan 16 GB RAM-geheugen zal meer schijfruimte voor pagin, hibernate, en dump bestanden vereisen.
Grafish	Super VGA (800 x 600) of hogere resolutie.
Andere	DVD Drive, Toetsenbord en Microsoft Mouse (of compatibel aanwijsapparaat), internettoegang (tegen betaling).

!Let op: Deze eisen zijn afhankelijk van de verschillende toepassingen en functies die u wilt installeren.

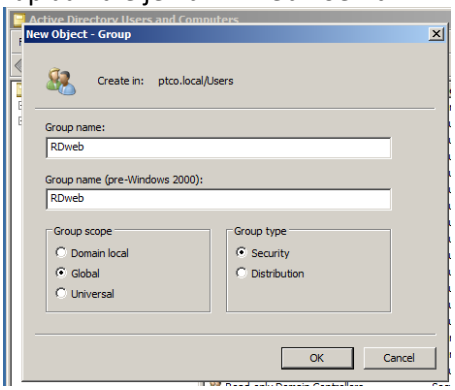
8.3 Installatie

Standaard installatie van een windows server 2008 kan je vinden in het boek “Inleiding Windows Server 2008” van Gunther Van Bleyenbergh hoodstuk 2 Installatie en configuratie.
Of via de mediaclip 2-1 De installatie van Windows Server 2008 op
http://www.academicservice.nl/site/downloadsinleidingwindowsserver2008.html

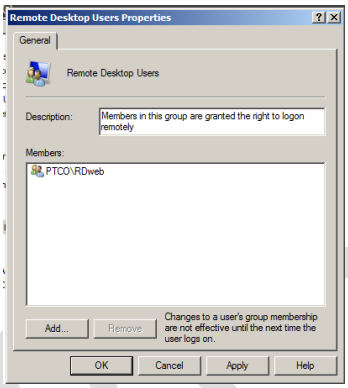
8.3.1 Installatie Remote Desktop Services.

Voor je begint met het installeren van de Remote Desktop Services zorg je ervoor dat je computer een vast IP adres heeft of dat de DHCP een vast IP adres geeft aan deze computer. Wij zorgen ervoor dat ClearOS een vast IP geeft aan onze DC.
Geef je computer een unieke naam volgens de normen van een netwerkbeheerder.
Zijnde volgens: wat is het, waar staat hij, waarvoor moet het dienen.
Dus voor ons 'ptco-rdweb'

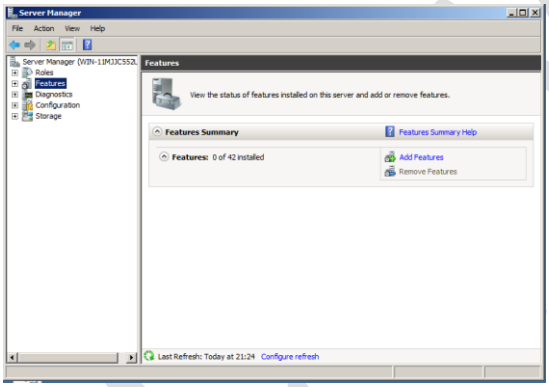
Op de Domain Controller maak in de Active Directory: Gebruikers en computers onder gebruikers een map aan die je vb. RDweb noemt.



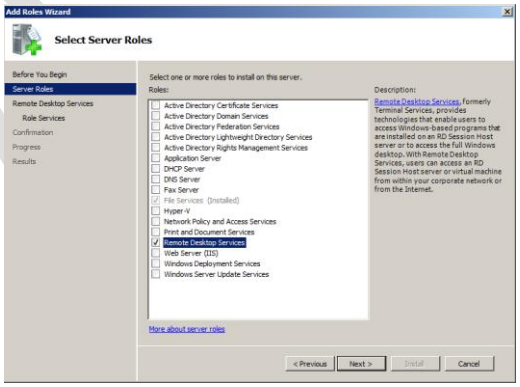
Op de Domain Controller maak in de Active Directory onder gebruikers een map aan die je vb. RDweb noemt.



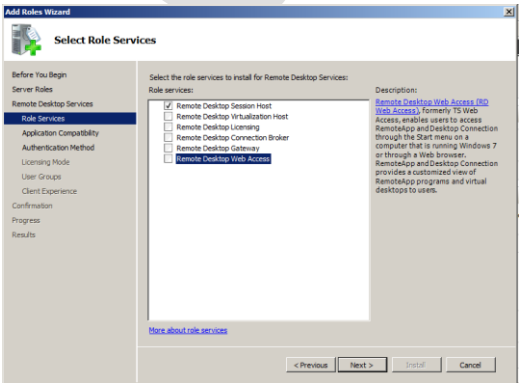
Op de RDweb server ga in de Server Manager naar configuratie > Local Users and Groups > Groups. Selecteer de 'Remote Desktop Users Properties' groep en voeg de groep RDweb toe.



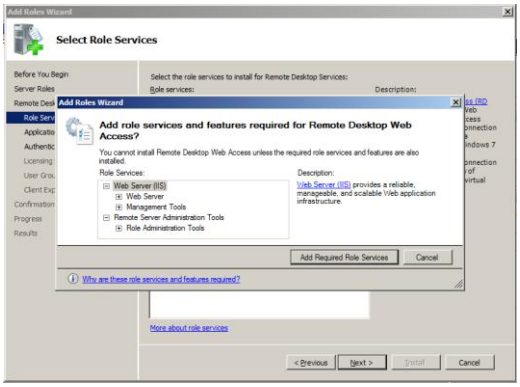
Start de server manager.
Ga naar roles > 'Add Roles'



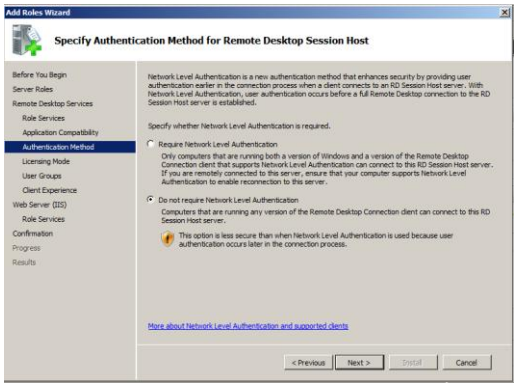
Selecteer 'Remote Desktop Services



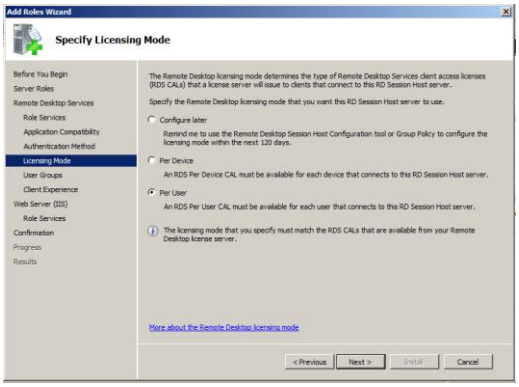
De service 'Remote Desktop Session Host' staat al geselecteerd. Selecteer ook de 'Remote Desktop Web Access'.



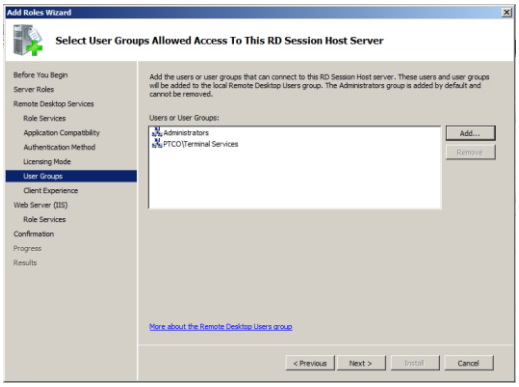
Er moeten bijkomende IIS Services worden geïnstalleerd. Klik dus op 'Add Required Role Services'.



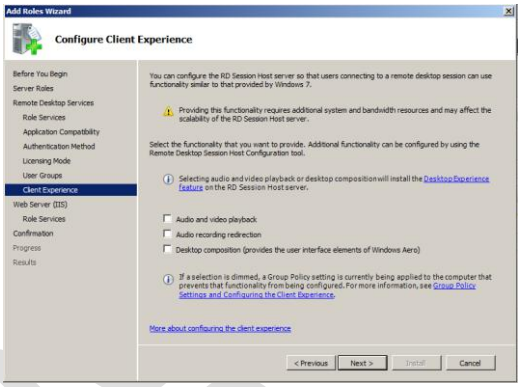
Selecteer welke verificatie op netwerkniveau je wilt.



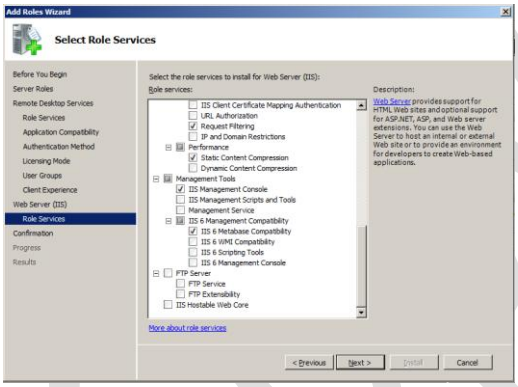
Afhankelijk van u licentie die je hebt selecteer ‘Per Dedvice’ of ‘Per User’.



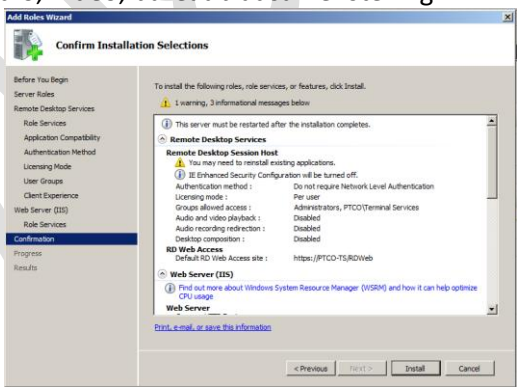
Kies welke groep gebruikers er connectie mogen maken met de ‘RD Session Host server’.



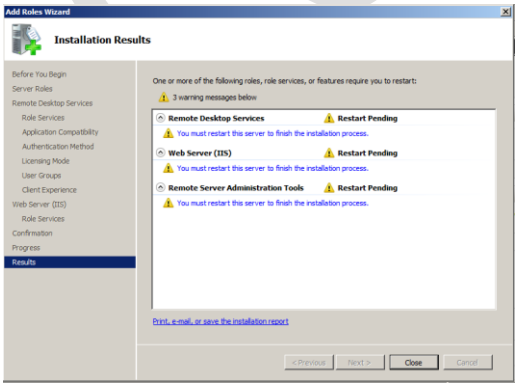
Selecteer de functie die je extra wilt aanbieden; Audio, Video, bureaubladsamenstelling.



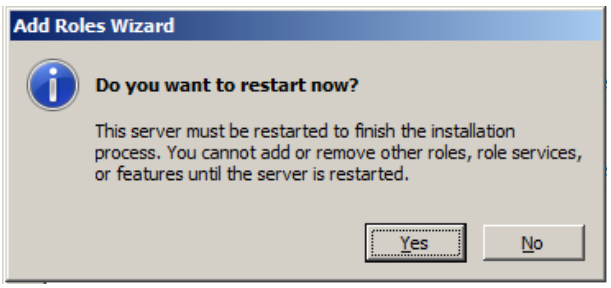
Selecteer de services voor de IIS.



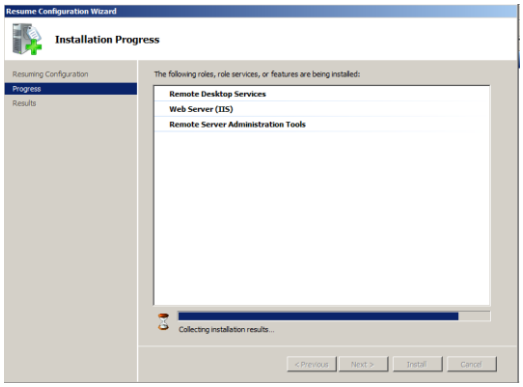
Samenvatting van de geselecteerde services. Klik op ‘install’ om verder te gaan.



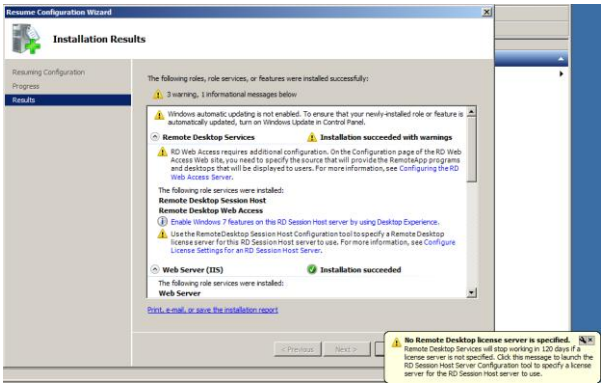
Na de installatie heb je een paar waarschuwingen.



En herstart de server.

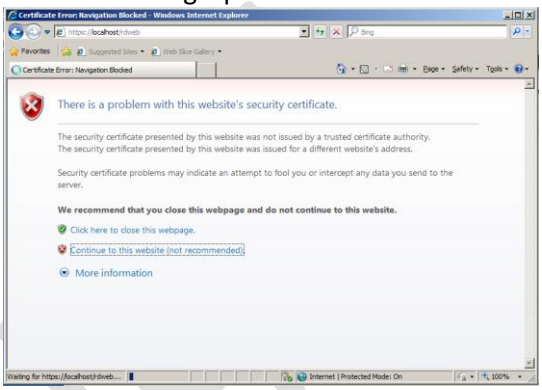


Na de herstart gaat de installatie nog een klein stukje verder.

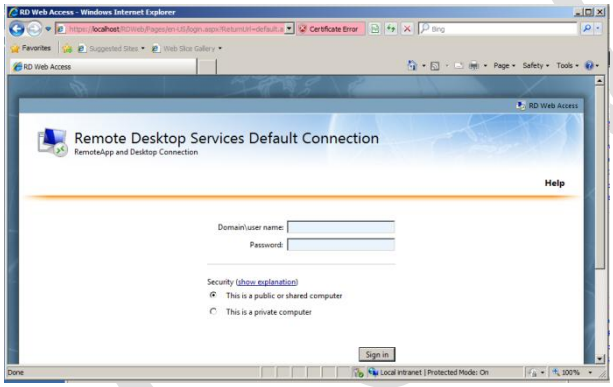


Na de herstart heb je nog een paar meldingen. Eén daarvan is dat er geen 'Remote Desktop License server' is gespecifieerd.

Start je webbrowser en typ "localhost" om te controleren of de IIS goed draait.

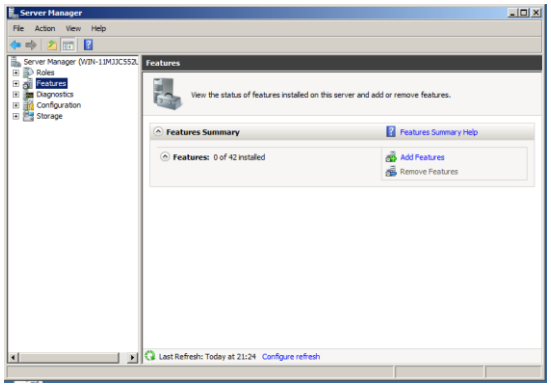


Via "https://localhost/rdweb" krijg je een melding om het certificaat vertrouwen. Vertrouw dit.

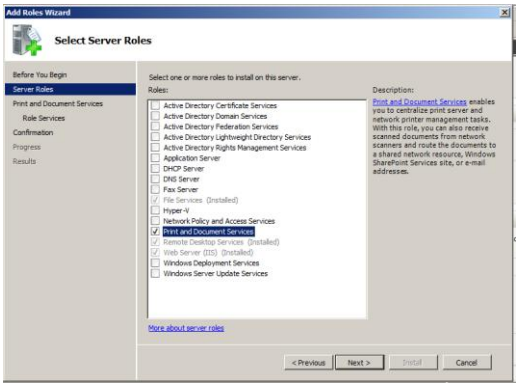


En je komt op de pagina van RD web.

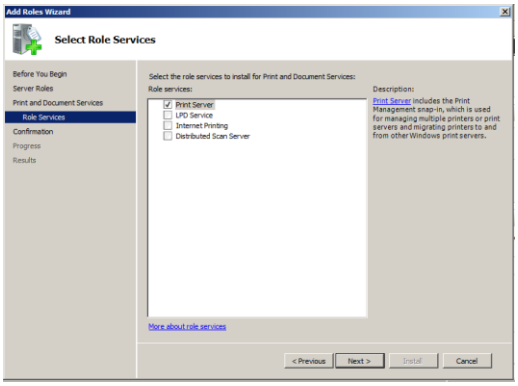
8.3.2 Installatie Print and Document Services.



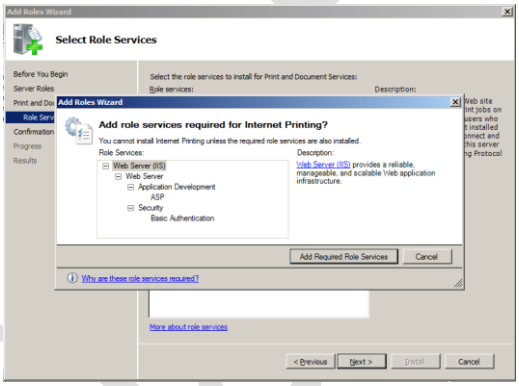
Start de server manager.
Ga naar roles > 'Add Roles'



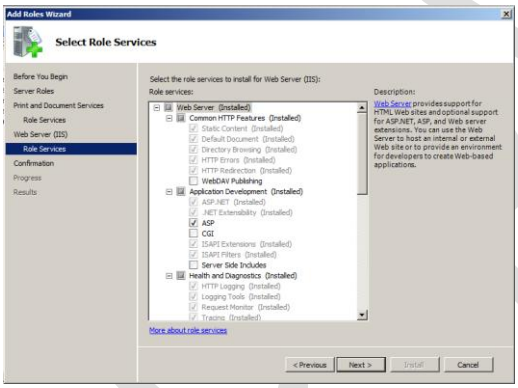
Selecteer 'Print and Document Services'



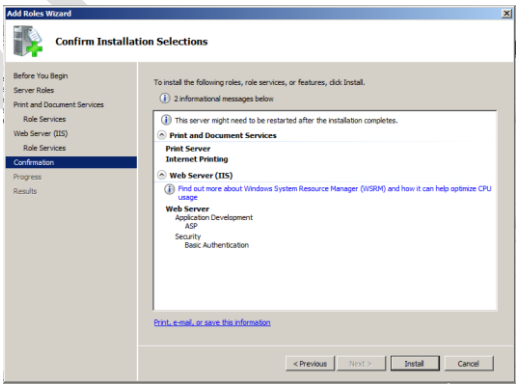
De services 'Print Server' is al geselecteerd.
Selecteer ook de services 'Internet Printing'



Er moeten bijkomende IIS Services worden geïnstalleerd. Klik dus op 'Add Required Role Services'.



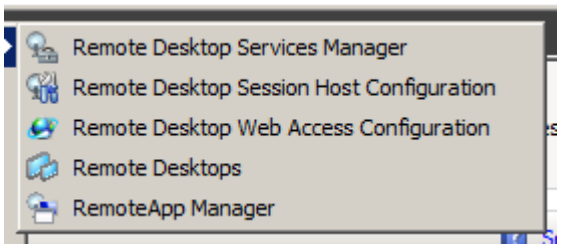
Selecteer de services voor de IIS.



Samenvatting van de geselecteerde services.
Klik op 'install' om verder te gaan.

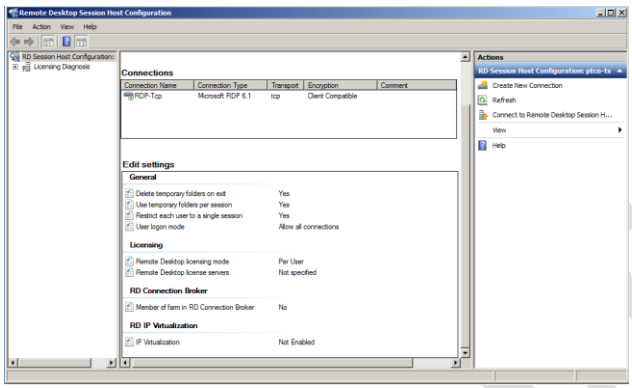
8.4 Configuratie

8.4.1 Configuratie Remote Desktop Services.

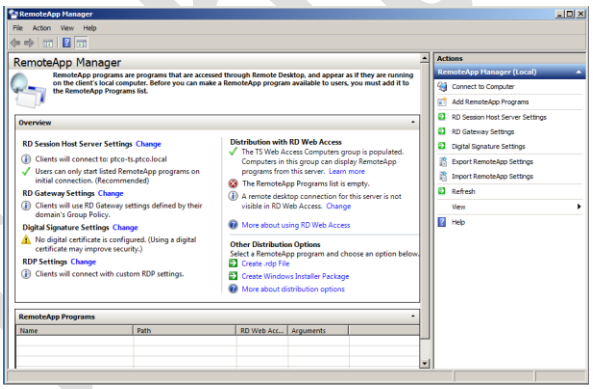


*Onder de administrative tools zul je merken dat in het menu ‘Remote Desktop Services’ volgende is geinstalleerd:

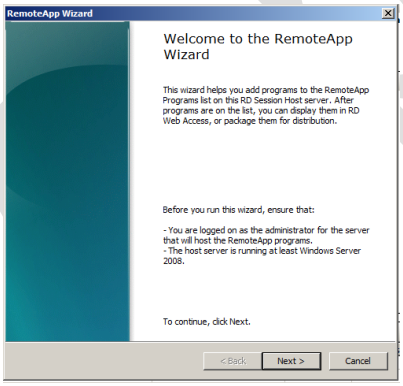
- Remote Desktop Web Access Configuration
- RemoteApp Manager



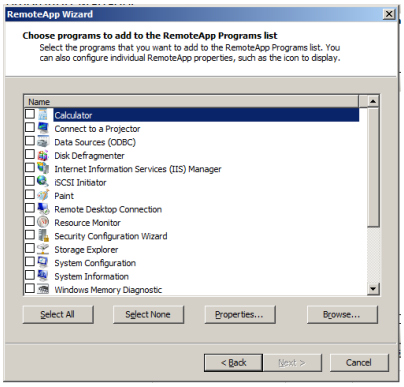
In de Remote Desktop Session Host Configuration kan je onder andere je ‘Licensing’ aanpassen zoals de RD license server.



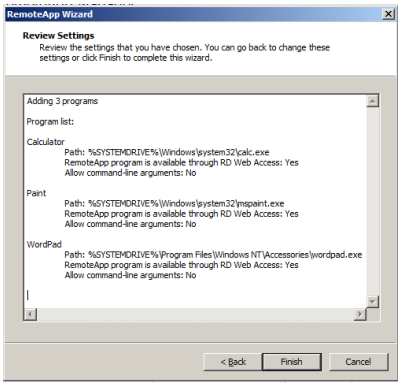
Via de RemoteApp Manager kan je selecteren welke programma’s er beschikbaar worden gesteld.



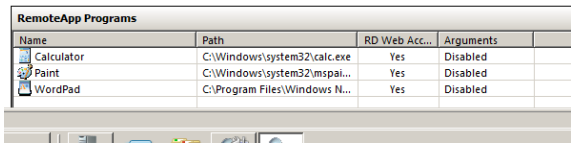
Klik rechts op ‘Add remoteApp Programma’ om de wizard te starten.



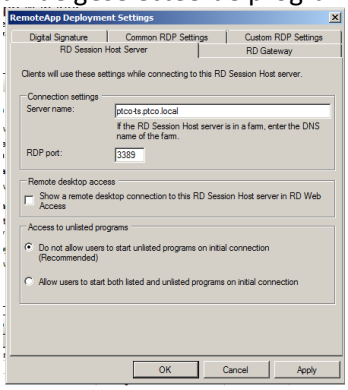
Selecteer welke programma’s beschikbaar mogen worden gesteld.



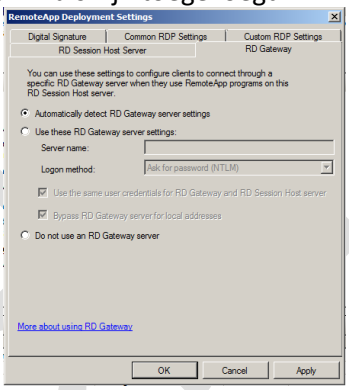
Overzicht van de geselecteerde programma's.



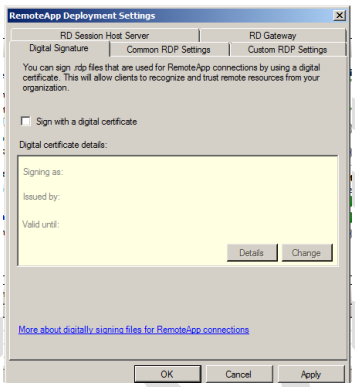
De programma's zijn toegevoegd.



Via de 'RemoteApp Deployment Settings' kan je de RDP poort veranderen. Deze staat standaard op 3389.

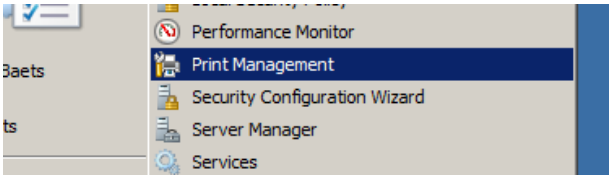


Via de 'RD Gateway Settings' kan je de gateway specifieren of hem op automatisch laten staan.

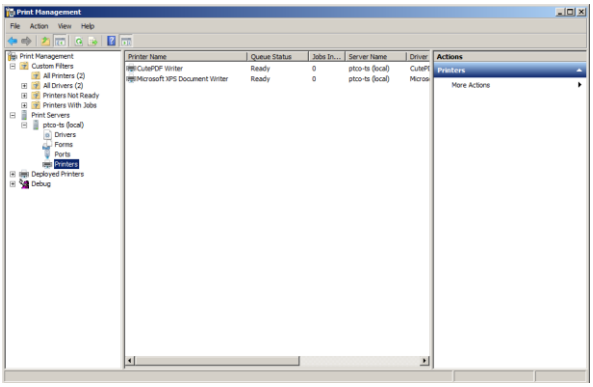


De 'Digital Signature Settings' kan je u certificaat invoegen zodat uw webbrowser geen foutmelding meer geeft.

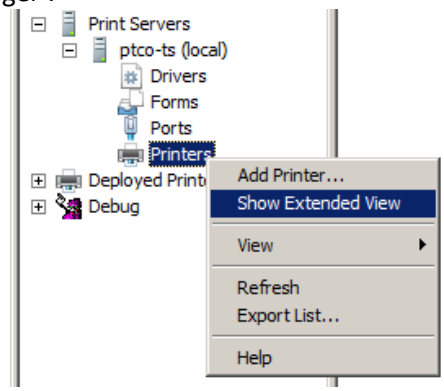
8.4.2 Configuratie Print and Document Services.



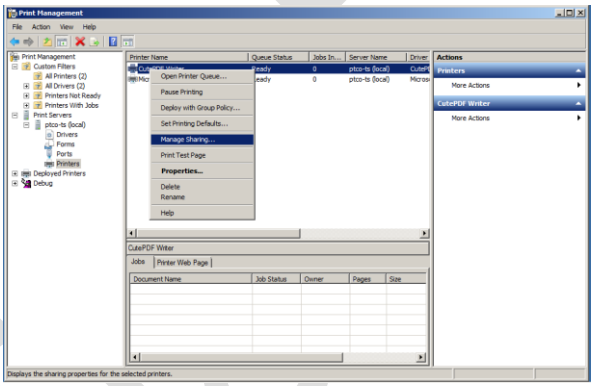
Onder Administrative Tools klik je op ‘Print Manager’.



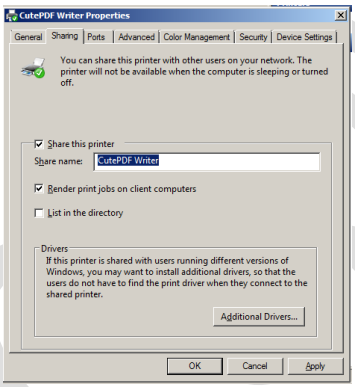
Ga naar Print Servers > Printers



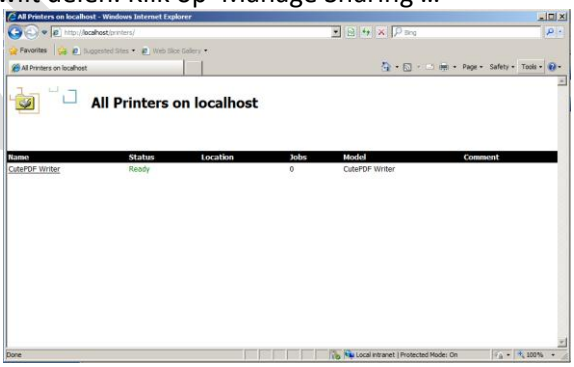
Je kan evt kiezen voor de ‘Extended View’ te tonen.



Klik met de rechtermuisknop op de printer die je wilt delen. Klik op ‘Manage Sharing …’



Selecteer ‘Share this printer’ en druk op ‘OK’



Ga in je browser naar ‘localhost/printers’ en zoals je ziet is deze printer ook gedeeld via het net.

9 Gebruik van de RD Services en Print Services

9.1 Benodigheden

Vereisten voor een clientcomputer.
Om RD Web Access te gebruiken, moeten clientcomputers ten minste Internet Explorer 6.0 uitvoeren en een versie van Extern bureaubladverbinding (RDC die minstens Remote Desktop Protocol (RDP) 6.1 ondersteunt.

Verbinding met extern bureaublad 6.1 ondersteunt RDP (Remote Desktop Protocol) versie 6.1.
RDC 6.1 :wordt meegeleverd bij de volgende besturingssystemen:

- Windows Server 2008
- Windows Vista met Service Pack 1 (SP1)
- Windows XP met Service Pack 3 (SP3)

De versie van RDC in Windows 7 en Windows Server 2008 R2 ondersteunt RDP 7.0.
De RDC-versie die u gebruikt, bepaalt welke functies van RD Web Access voor u beschikbaar zijn.

De besturing van de ActiveX Client voor extern bureaublad-services moet zijn ingeschakeld.
De ActiveX-besturing wordt meegeleverd met RDC 6.1 en de versie van RDC in Windows 7 en Windows Server 2008 R2.

9.2 Inleiding van het gebruik

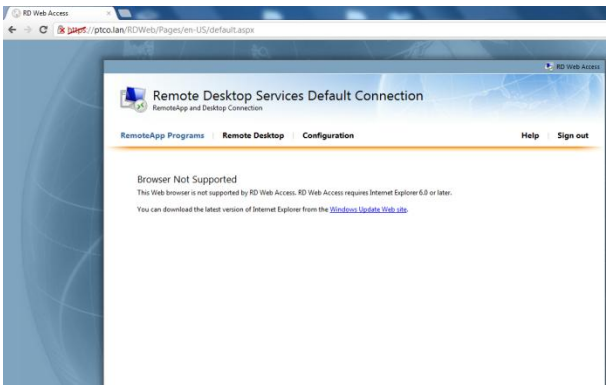
We hebben onze Clear OS geconfigureerd voor het gebruik van een webserver. Hier kunnen we dan onze eigen website op draaien en een aparte pagina maken die via een login en wachtwoord toegang geeft tot de links naar onze interne servers.
Hiervoor moeten dan wel de juiste poorten ge forward worden

- Poort 85 >> Nagios
- Poort 443 >> RDweb
- Poort 81 >> Clear OS webconfig
-

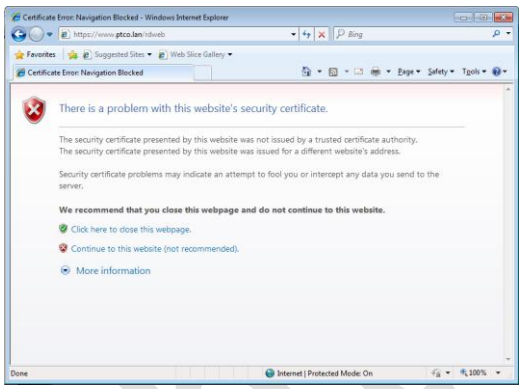
Onze pagina kan er dan bijvoorbeeld zoals hieronder eruit zien.

9.2.1 Gebruik van de RDweb

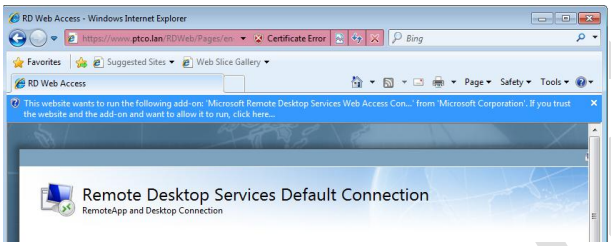
Zoals al bij de benodigdheden geschreven hebben we minstens Internet Explorer 6.0 nodig.
Het webadres is in ons geval www.ptco.lan
Om gebruik te kunnen maken van de RDweb surfen we dus naar https://www.ptco.lan/rdweb



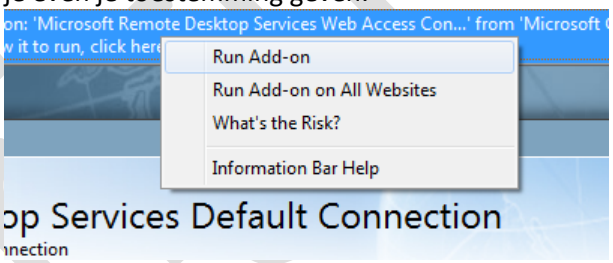
"Browser Not Supported". Onze Chrome werkt hier niet mee.



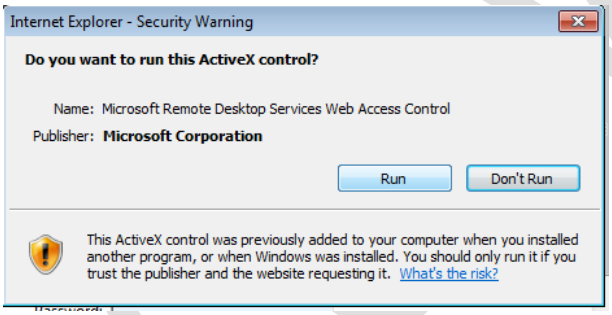
Wegens we geen geldig certificaat hebben moet je even je toestemming geven.



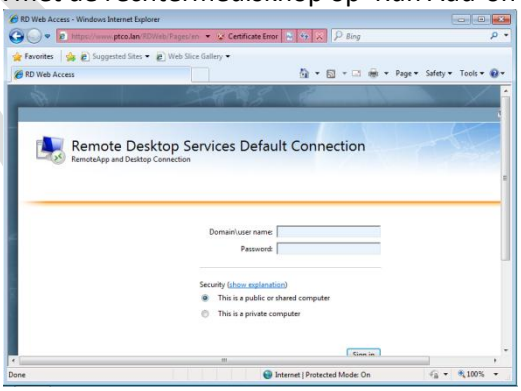
Er is een "Add-on" voor nodig.



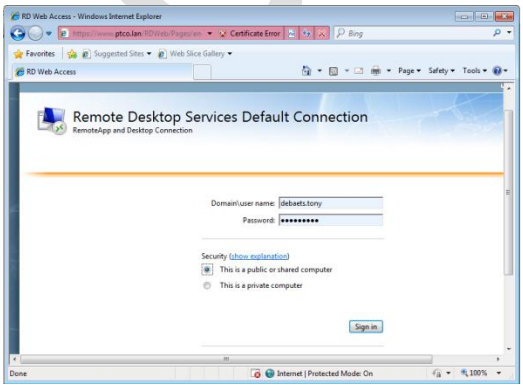
Klik met de rechtermeuisknop op 'Run Add-on'



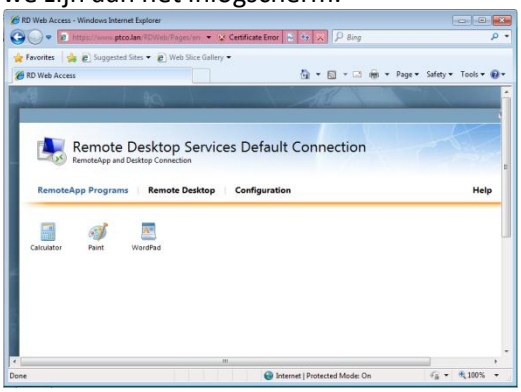
Druk 'Run' om de ActiveX control te vertrouwen.



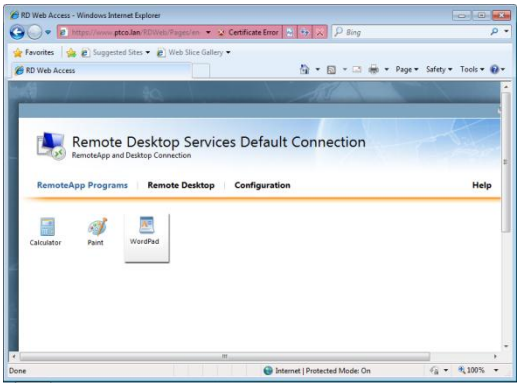
En we zijn aan het inlogscherm.



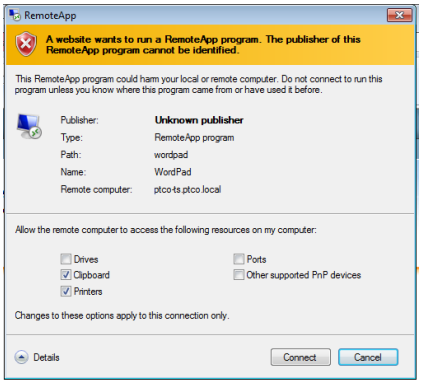
Geef je gebruikersnaam en wachtwoord in en geef aan of je op een gedeelde of private computer werkt.



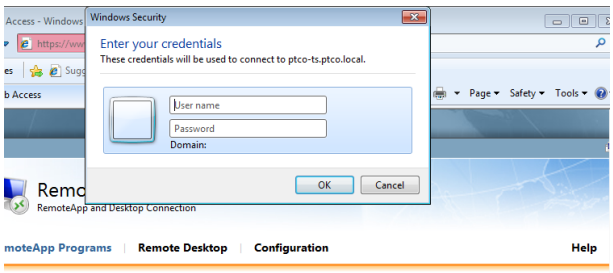
Je bent aangemeld en de programma's die voor u beschikbaar zijn zie je staan.



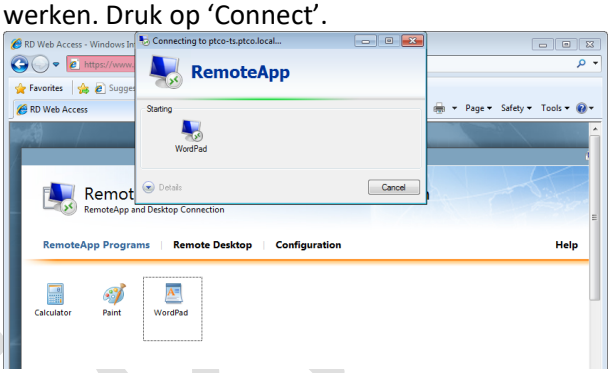
Druk op ‘WordPad’.



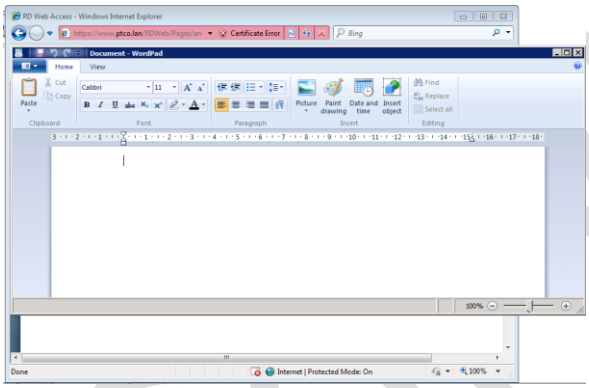
We willen het RemoteApp program laten werken. Druk op ‘Connect’.



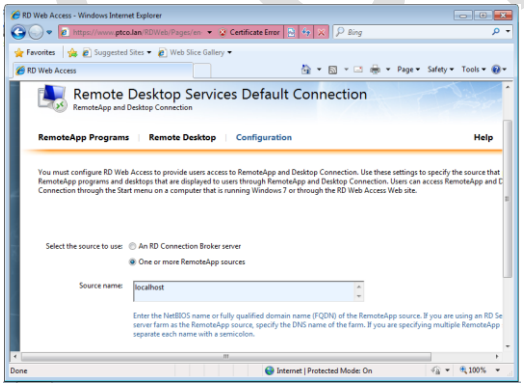
Geef nogmaals je gebruikersnaam en wachtwoord in.



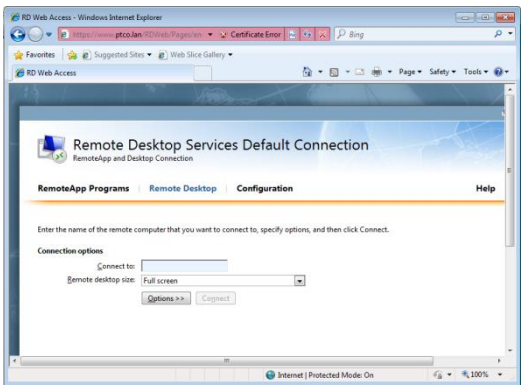
En het programma wordt gestart.



Proficiat het programma is gestart en klaar voor gebruik.



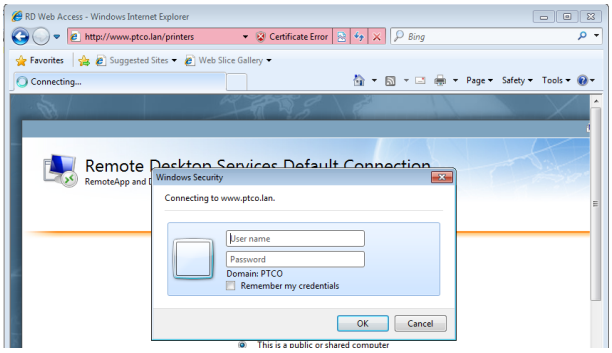
Wegens we Admin-rechten zien we ook de tab ‘Configuratie’. Wegens we maar één RemoteApp source hebben gebruiken we geen Broker maar werken we ‘local’.



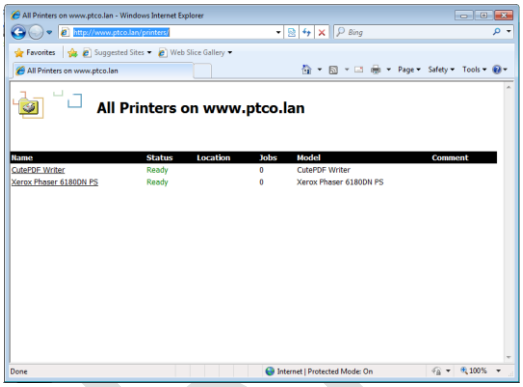
Het is ook mogelijk om de computer over te nemen.

9.2.2 Gebruik van de printers via web

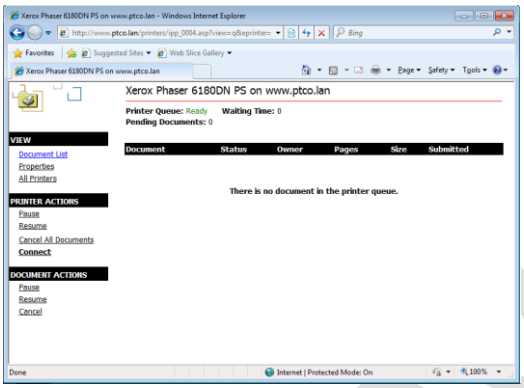
Surf naar http://www.ptco.lan/printers



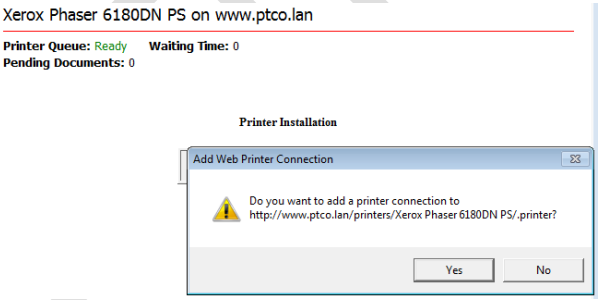
Geef je gebruikersnaam en wachtwoord in.



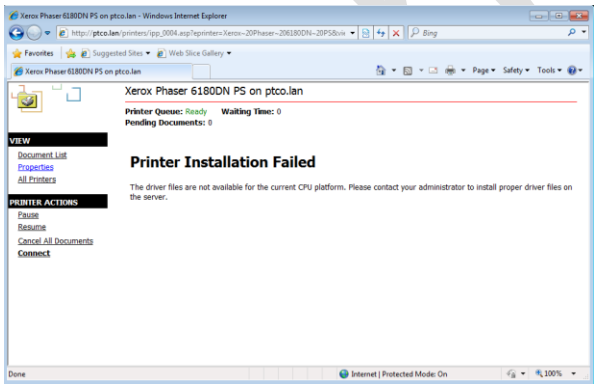
Dit zijn de printers die worden gedeeld.
Klik op de Xerox printer.



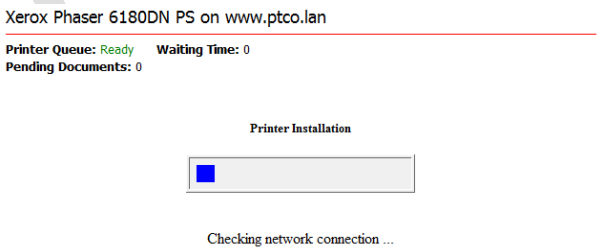
U komt in de Status pagina terecht. Druk links op ‘Connect’.



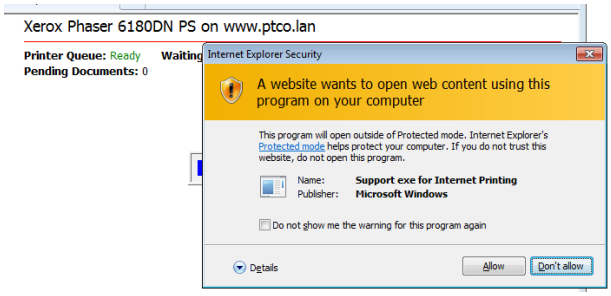
Wil je deze printer toevoegen?



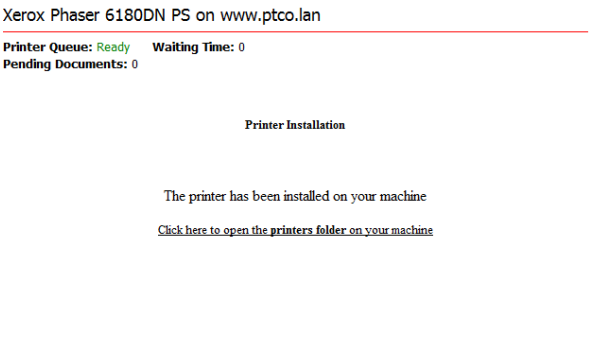
Oeps! Een foutje? We hebben niet de juiste driver voor ons cpu-platform.
(Zie verder 9.3 Driver Error.).



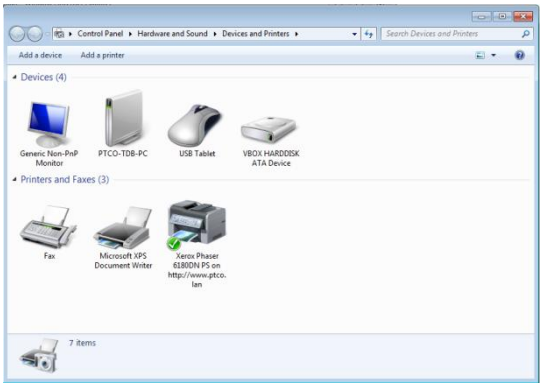
Na controle wordt de printer geïnstalleerd.



Klik 'Allow' voor de toestemming.

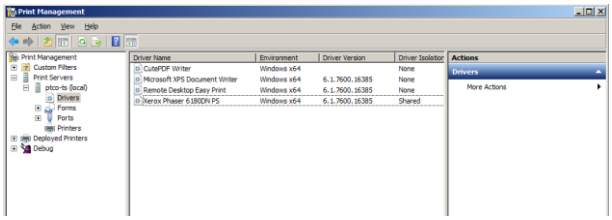


Proficiat de printer is geinstalleerd.
Klik op de link om de printer map te openen.

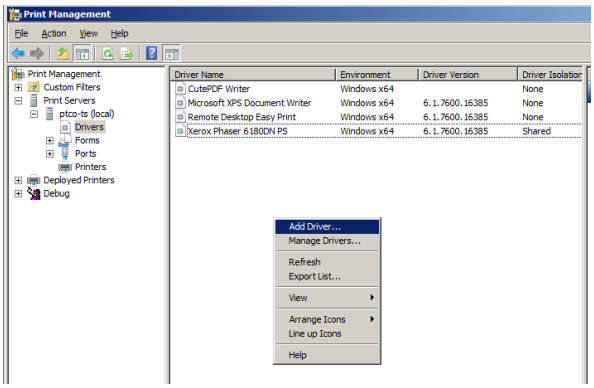


En ja hoor. De printer is toegevoegd aan onze printers en klaar voor gebruik.

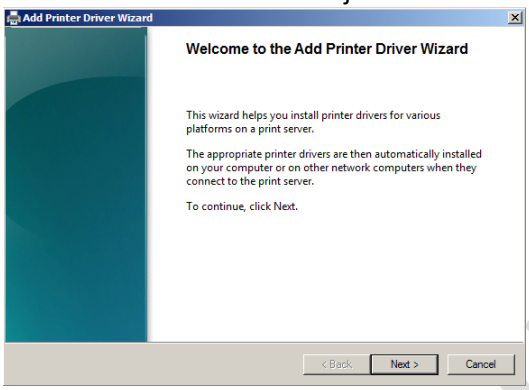
9.3 Driver Error.



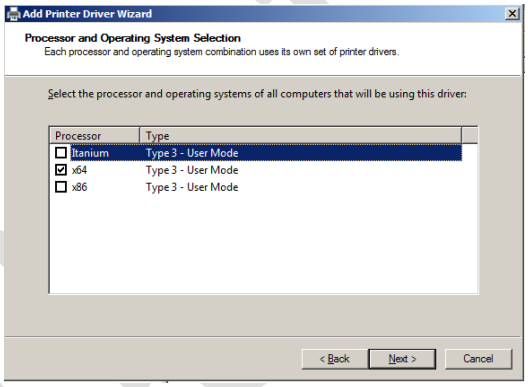
Op de Print server open de ‘Print Management’. Ga onder uw domein naar drivers. We zien dat alle drivers voor de x64 versie zijn.



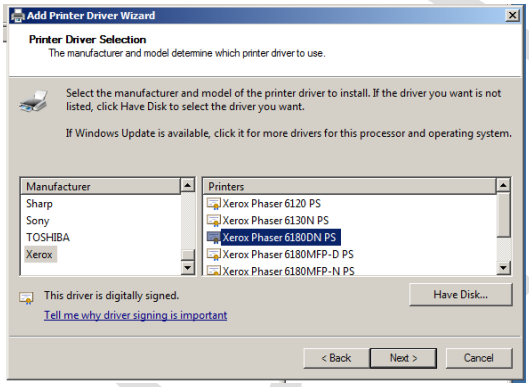
Klik rechtermuisknop en ‘Add Driver’.



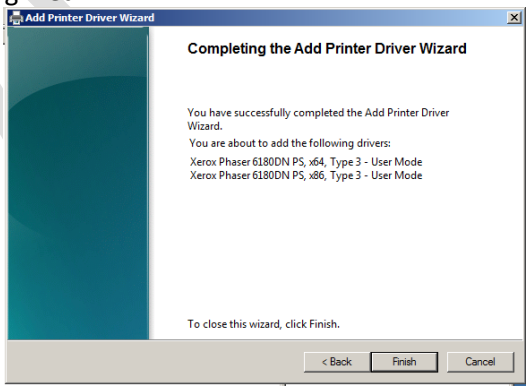
We zitten in een wizard om extra drivers te installeren.



De x64 processor is aangevinkt maar onze x86 nog niet.



Selecteer de juiste printer.



En op de samenvatting zie je dat hij de driver neemt voor de x64 en de x86.

10 Besluit

Het uitwerken van onze C-proef was begonnen bij het ontwerp van een Visio presentatie. Het idee was om een interactie te creëren tussen Linux en Windows servers. Om de C-proef een praktische invulling te geven, interpoleerden we onze opzet naar een fictief bedrijf waarbij we volgende elementen voor ogen hadden; Een bedrijf heeft verschillende medewerkers met allen toegang tot het netwerk. Op een gecontroleerde manier stellen we hen software-applicaties ter beschikking. En in functie van hun rechten verkrijgen ze de toegang tot collectieve gegevens.

Hierbij hebben we twee mogelijkheden. De eenvoudigste oplossing is dat iedere medewerker zijn computer gewoon op het netwerk zet. Alle applicaties werken autonoom op iedere PC en de collectieve gegevens staan op een NAS-drive met een beveiligde toegangscode. We hebben echter voor een tweede oplossing gekozen waarbij we verschillende elementen van onze 3-jaar opleiding gebruiken.

Bij aanvang was duidelijk dat we de rechten van het domein met een domain controller zouden opvangen en een terminal server zouden gebruiken om collectieve applicaties ter beschikking te stellen. Een verrijking tijdens het opzetten van ons eindwerk was om te werken met Nagios, een netwerk supervisie software. Het gaf ons de mogelijkheid om op een overzichtelijke manier een beeld te vormen van het actief zijn van de verschillende netwerkgebruikers. Gedurende de implementatie van het Nagios-software pakket, leefde ons project. We zagen nieuwe mogelijkheden en gingen de uitdaging aan. Ons initieel idee van gegevens die we wensten in te lezen werd bijgestuurd. Nagios heeft ons de mogelijkheid gegeven om beter de informatie uitwisseling tussen monitor server en clients te verstaan. Hoe zet je de juiste poorten open en hoe wordt informatie geëncrypteerd doorgestuurd? Doch hebben we door tijdsgebrek dingen naast ons laten liggen. Het leek ons ook een grote uitdaging om checks via SNMP in te lezen. Zo konden we bijvoorbeeld statussen van switchen, routers, UPS of gewoon berichten van derden die over het netwerk circuleren inlezen.

We hadden aanvankelijk geopteerd om de routing, DHCP-service en firewall functies op een linux server te laten draaien. Ons voorkeur viel voor Smoothwall software. Volgens de informatie die we hadden ingewonnen, was dit de perfecte invulling voor een kleine KMO die we voor ogen hadden. Tijdens de implementatie werden we geconfronteerd met verschillende beperkingen. Smoothwall is een redelijk gesloten systeem waarbij we naast de root geen andere gebruikers konden aanmaken. De nagios nrpe_checks konden we niet implementeren. We waren zodoende genoodzaakt een andere oplossing te zoeken. Na aanvullende ‘google research’ viel onze keuze op Clear OS. Clear OS werkt eveneens in een Linux omgeving, heeft meer mogelijkheden met daarbij een gebruiksvriendelijkere grafische interface. Naast de taken die we eerder bepaalden, biedt Clear OS ons tevens volgende functionaliteiten. DHCP server, DNS server, firewall, web server, FTP server, SSH server, MySQL database server, …

Het gedeelte Domein Controller, Terminal Server en Print Server was redelijk afgelijnd. We hebben een standaard installatie uitgevoerd, aangepast aan de noden van ons project. Bij de uitvoering van de C-proef zijn er dagelijks punten naar boven gekomen waarvan we bij aanvang geen weet van hadden. Ervaring is een opstapeling van vergissingen, het is een eufemisme voor het tijdverlies die we hebben opgelopen om dingen te begrijpen, aan te passen en in het slechtste geval opnieuw moesten her-installeren. Een concept voor een KMO uitwerken is een levend project. We hadden bij aanvang een vaag idee van ons einddoel. Al doende kwamen er elementen naar boven waarvoor we

oplossingen dienden te vinden. En sommige ingeslagen wegen hebben geen keer. De keuze van de IP-range waarin we zullen werken hadden we snel ingevuld. Een subnet 255.255.255.0 Het is een klein piloot project waarbij we de 254 gebruikers niet zullen overschrijden. Stel dat het pilootproject toch in uitvoering komt dan hebben we hier de fundamenten voor een groter geheel reeds bepaald.

Onze opleiding en C-proef heeft ons de mogelijkheid gegeven om aan onze parate kennis een bredere basis te geven. De fundamenten om verder op te bouwen. Maar weet dat netwerkbeheerder zijn een permanent leerproces is. En zoals Jean Gabin het verwoorde: “Je sais, je sais, je sais qu'on ne sait jamais. Mais ça, j'le SAIS... !

11 Lijst gebruikte afkortingen

AD	Active Directory
ADSI Edit	Active Directory Service Interface Editor
CPU	Central Processing Unit
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server/service
FTP	File Transfer Protocol
GPO	Group Policy Object
HD	Hard Disk
IP	Internet Protocol
IPSec	Internet Protocol Security
JOE	Joe's Own Editor
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC address	Media Access Control address
MSQL	Mini Structured Query Language
NAS	Network Attached Storage
NFS	Network File System
NRPE	Nagios Remote Plugin Executor
NTP	Network Time Protocol
OS	Operating System
OU	Organizational Unit
PDC	Primary Domain Controller
POP	Post Office Protocol
PPTP	Point to Point Tunneling Protocol
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RPM	Red Hat Package Manager
SCP	Secure Copy
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Mail Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TAR	Tape Archive
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
Windows NT	Windows New Technology
WINS	Windows Internet Name Service
YAST	Yet Another Setup Tool
YUM	Tellow Dog Update Manager

12 Bibliografie

12.1 TCP/IP

Literatuur

- Tcp/Ip, Rob Scrimger, Academic Service, 2002
- TCP/IP Foundations, Andrew G. Blank, Sybex, 2002
- TCP/IP Tutorial and Technical Overview, IBM Redbooks, 2006

Websites

http://nl.wikipedia.org/wiki/TCP/IP
http://hwi.uni.be/archief/nl/h3.htm
http://www.computerwoorden.nl/tcpip-protocol-suite-woordenboek.htm
http://ims.xebe.be/netwerken/IP-klassen%20&%20Subnetting.pdf

12.2 ClearOS

Websites

http://www.dataforce.nl/web/page.php?2
http://www.dataforce.nl/web/page.php?5
http://www.clearcenter.com/support/documentation/clearos_enterprise_5.2/user_guide/start
http://schoolitexpert.com/network-tools/clearos
http://www.ulverston.myzen.co.uk/mini-itx/pages/samba.htm

12.3 Nagios

Literatuur

- Pro Nagios 2.0, James Turnbull, Apress, 2006
- Learning Nagios 3.0, Wojciech Kocjan, Packt Publishing, 2009
- Nagios System and Network Monitoring, Wolfgang Barth, Open Source Press Munich, 2006
- Nagios NRPE Documentation, Ethan Galstad, 2007
- Building a monitoring infrastructure with Nagios, David Josephsen, Prentice Hall, 2007
- The Nagios Book, Chris Burgess, 2005
- Nagios 3 – Entreprise Network Monitoring, Syngress, 2008

Websites

http://wiki.comdivision.com/pages/viewpage.action?pageId=8028341
http://techgurulive.com/2010/12/16/a-step-by-step-to-isntall-nagios-client
http://www.thegeekstuff.com/2008/06/how-to-monitor-remote-linux-host-using-nagios-30/
http://www.kernelhardware.org/nagios-nrpe-to-monitor-remote-linux-server
http://www.retroviz.com/CMS/a73_Installing_Nagios_on_openSUSE_%28no_linux_knowledge_required%29.aspx
http://nagios.sourceforge.net/docs/3_0/monitoring-windows.html
http://www.opengeneration.org/papers/nagios_en.pdf
http://www.cpels.nl/linux-2/nagios/nagios-installeren
http://www.thegeekstuff.com/2008/05/nagios-30-jumpstart-guide-for-red-hat-overview-installation-and-configuration/
http://oreilly.com/perl/excerpts/system-admin-with-perl/twenty-minute-snmp-tutorial.html
http://nagios.sourceforge.net/download/contrib/documentation/misc/config_diagrams/nagios-config.png
http://www.geckotechnology.com/Win32APIProxy
http://exchange.nagios.org/directory/Plugins/Operating-Systems/Windows/Win32APIProxy/details
http://www.thegeekstuff.com/nagios-core-ebook/

http://pdftop.net/nagios+core+3-pdf/
http://www.softpanorama.org/Admin/Monitoring/nagios.shtml#NRPE_plug-in
http://www.siamkia.com/open-source-help/how-to-fix-check-nrpe-error-could-not-complete-ssl-handshake.html
http://www.devside.net/guides/linux/openssl

12.4 Domein Controller

Literatuur

- Introducing Windows Server 2008 R2, Charlie Russell and Craig Zacker, Microsoft, 2010
- Windows Server 2008, Portable Command Guide, Darril Gibson, Pearson, 2011
- Inleiding Windows Server 2008, Gunther Van Bleyenbergh, Academic Service, 2009

Websites

http://grok.lsu.edu/Article.aspx?articleid=15456
http://www.windowsreference.com/windows-server-2008/step-by-step-guide-for-windows-server-2008-domain-controller-and-dns-server-setup/

12.5 Remote desktop services

Literatuur

- Introducing Windows Server 2008 R2, Charlie Russell and Craig Zacker, Microsoft, 2010
- Windows Server 2008, Portable Command Guide, Darril Gibson, Pearson, 2011
- Inleiding Windows Server 2008, Gunther Van Bleyenbergh, Academic Service, 2009

Websites

http://en.wikipedia.org/wiki/Remote_Desktop_Services
http://www.microsoft.com/en-us/server-cloud/windows-server/remote-desktop-services.aspx
http://windows.microsoft.com/nl-BE/windows-vista/What-is-a-Terminal-Services-Gateway-server
http://technet.microsoft.com/en-us/library/cc753844%28v=ws.10%29.aspx
http://technet.microsoft.com/nl-nl/library/cc755053%28v=ws.10%29.aspx

12.6 Gebruik van de RD Services en Print Services

Websites

http://technet.microsoft.com/nl-nl/library/cc731508%28v=ws.10%29.aspx

13 Dankwoord

De passie en de volharding blijven hebben om drie jaar lang een netwerkbeheerders opleiding te volgen zijn er naast je persoonlijkheid tevens andere factoren die bepalend zijn geweest om die missie tot een goed eind te brengen. Het is zoals bij een gerecht voorbereiding. Alle individuele ingrediënten met elkaar doen combineren maken er een lekker gerecht van. Bij de opleiding netwerkbeheerder hebben onze hulpvaardige leerkrachten 'de ingrediëntenlijst' meegeven om computers, servers, switchen, applicaties met elkaar te doen communiceren. En zoals een kok maar zijn materie zal beheersen door zelf met de pannen te experimenteren, zal een netwerkbeheerder al doende zijn kennis vervolledigen. Onze eerste labo-schaal toepassingen waren de eerste toetsing met de praktijk. Tijdens de opzet van onze C-proef ervaren we de eerste complexiteit om meerdere applicaties en machines met elkaar te doen communiceren. De grote challenge zal zijn om ons later verder te ontplooien en onze kennis te toetsen in het geheel van grote en professionele systemen.

We willen ons dank betuigen aan onze leerkrachten die verschillende onderdelen van de grijze materie hebben onderwezen. Theorie en praktijk hadden hier een grote samenhang. Uiteraard mogen we de pauzes niet vergeten waar algemene kennis werd vergaard. Onderwerpen, anekdotes of weetjes werden aangereikt die je normaal in het dagelijks leven niet opvangt.

Verder is het een genoegen mijn dank uit te spreken aan mijn medeleerling Tony (en ik zal het maar schrijven) en ook vice-versa. Zijn hulpvaardigheid en opgewektheid hebben een gevoelige verlichting betekend toen we deze bladzijden voorbereiden en reviseerden.

Tenslotte wil ik uiteraard mijn medeleerlingen niet vergeten, die eveneens een steun zijn geweest om de lessen met een vrolijk gevoel te blijven volgen. Je ziet elkaar toch in goede en slechte dagen, bij ziekte en op momenten van verminderde belangstelling, maar doordat je een aangename band hebt met elkaar blijft het geheel plezant.

En als laatste een grote dank aan het thuisfront. Drie jaar lang de familie belasten met logistieke problemen omdat de chauffeur van dienst naar Sint-Niklaas was gereden.