Windows NT 4.0

Tips, Trucs en Achtergronden

Gino Damen
2 december 1999
Versie: 3.2

Inhoudsopgave

Inleiding

Dit document bevat een verzameling van tips en trucs voor het dagelijks gebruik van Windows NT 4.0. Voor het samenstellen van dit document is gebruik gemaakt van informatie opgedaan uit eigen ervaringen, maar ook informatie verzameld uit de verschillende online diensten, computerbladen en Microsoft TechNet. Doe er je voordeel mee, maar let er op dat sommige van de tips en trucs een desastreus effect op NT kunnen hebben bij verkeerd of ondoordacht gebruik.

De meest recente versie is altijd beschikbaar onder Downloads bij:

http://ourworld.compuserve.com/homepages/gino_damen

Of op de volgende Compuserve forums:

Windows Forum GO / Ga naar NLWINDOWS

Nieuw is verder dat aan het oogje (👁) te zien is welke items nieuw of aangepast zijn!

Revisies

Versie	Omschrijving
1.0	Initiële release van het document voor intern gebruik
2.0	Release voor het document voor extern gebruik
2.2	Ander Word sjabloon gebruikt i.v.m. problemen in oudere Word versies en korte bestandsnaam.
2.3	NTVDM informatie toegevoegd
2.4	Service Pack 4 en algemeen onderhoud
2.5	Enkele nieuwe register wijzingen toegevoegd en deze ook als losse REG-bestanden opgenomen.
2.6	De losse registry bestanden zijn als een “knip en plak” bijlage opgenomen
3.0	Samenvoegen van het "Tips en Trucs" document en het "Achtergronden" Document tot één document. Verder toevoegingen en aanpassingen die voortvloeien uit SP5 en nieuw indictaor (👁) toegevoegd
3.1	UDMA instellingen activeren en het instellen van de pagefile c.q. bepalen hoeveelheid fysiek geheugen
3.2	Aanpassing Fix-apck informatie en nieuwe "look" optie bij de Registry aanpassingen

Disclaimer

NO WARRANTY. THE DOCUMENT IS PROVIDED "AS-IS," WITHOUT WARRANTY OF ANY KIND, AND ANY USE OF THIS DOCUMENT IS AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE AUTHOR DISCLAIMS ALL WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED WITH REGARD TO THE DOCUMENT.

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE DOCUMENT, EVEN IF THE AUTHOR HAS BEEN ADVISED OF THE POSSIBLITY OF SUCH DAMAGES. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY.

Copyright (c) 1999 Gino Damen. All rights reserved.

Sectie 1: Tips en Trucs

Tips en trucs voor normaal gebruik

Onmisbare utilities

NT bevat al een aanzienlijke hoeveelheid utilities, maar er zijn een aantal utilities die het leven voor de NT gebruiker zeker vergemakkelijken:

TweakUI 1.1 NT	Hiermee kunnen allerlei opties voor het gedrag van Explorer worden ingesteld.;
Dos Prompt Here 1.0	Maakt het mogelijk om in elke directory een command prompt te openen die ook in die directory staat;
Diskeeper Lite	Het defragmentatie programma voor onder NT, toekomstig onderdeel van Windows 2000

TweakUI en Dos Prompt Here zitten in de Powertoys van MS, Diskeeper Lite is gratis te downloaden bij Executive Software (WWW.EXECSOFT.COM).

Meer zicht op bestanden

Standaard worden alle extensies van geregistreerde bestanden verborgen. Ook bestanden met de extensie *.dll, *.sys, *.vxd, *.386 en *.pnd en bestanden met het hidden en/of system attribuut worden standaard verborgen door de Explorer. Voor veel gebruikers is dit geen probleem, maar voor mensen die meer inzicht en grip op hun systeem willen hebben is dit zeer lastig. V.b. Is een lege directory wel echt leeg? Misschien staan er wel DLL's in?

Doe het volgende om alle bestanden zichtbaar te maken: Start Explorer en kies View -> Options... -> View tab. Klik "Show all Files" aan en zet het vinkje uit voor "Hide file extensions for known file types". Zelf zet ik ook nog de opties "Display the full path in the title bar", handig op een netwerk, en "Display compressed files en folders with alternate color" aan. De kleur voor gecomprimeerde bestanden is met TweakUI te wijzigen.

Plug en Play onder NT

Het is wel degelijk zo dat onder NT Plug en Play voor ISA apparaten mogelijk is. Om hiervan gebruik te kunnen maken moet de z.g.n. "enabler driver" geïnstalleerd worden. Deze zorgt dan voor de herkenning en configuratie van deze apparaten. Het betreffende stuurprogramma (PNPISA.SYS) is in de \Drvlib folder op de Windows NT CD te vinden.

- Ga naar de \DRVLIB\PNPISA\X86 (voor Intel-dozen).
- Rechts klik op PNPISA.INF, en kies "Install".
- Wanneer er om gevraagd wordt, herstart de computer.

Dit stuurprogramma bevat niet de complete Windows 95 Plug and Play support. Het is bijvoorbeeld niet mogelijk om dynamisch resources toe te kennen aan PnP ISA apparaten. Het is wel mogelijk om, via een user interface, handmatig de systeem resources in te stellen op zo'n manier dat er geen conflicten ontstaan met ander

apparaten in het systeem. Hiermee wordt de installatie van PnP geluidskaarten en modems weer een fluitje van een cent. Zie ook sectie 2 van dit document

Het Volume control (speaker) in de systemtray

Indien er een audiokaart of chip aanwezig is en de stuurprogramma's zijn correct geïnstalleerd, dan hoort er een speaker icoontje in de systemtray te verschijnen (naast de tijd). Indien dit niet het geval is, is het speaker icoontje op volgende manier te activeren: Kies Control Panel -> Multimedia. Klik op de Sound tab en zet een vinkje in het vakje voor de "Show volume control on the taskbar" instelling. Met een dubbelklik is nu de Master volume op te roepen, terwijl rechts klikken toegang geeft tot de ander volume opties.

Het batterij metertje in de systemtray

Bij laptops is het handig om, in de systemtray, naast het klokje een mini batterij icoontje te hebben. Op deze manier is eenvoudig het energie niveau van de batterij en de tijd te gaan te bepalen. Het icoontje is op de volgende manier te activeren: Control Panel -> Power Management. Zet een vinkje in de "Enable battery meter on taskbar" instelling. NT ondersteund standaard geen APM. Er moet dus van de leverancier een speciale driver verkregen worden voordat dit mogelijk is.

Open een bestand met je favoriete editor

Maak een shortcut aan naar je favoriete editor. Sleep of kopieer deze naar de SendTo folder, dit is een subfolder van de Windows folder. Deze shortcut verschijnt hierdoor in het "Send To" menu. Rechts klik nu op een bestand en stuur deze naar je editor!

Bewaren van een bestand zonder default extensie

Zet quotes om de naam van het bestand, indien de extensie moet afwijken van de standaard extensie die het programma gebruikt. B.v. In Notepad wordt het volgende bestand bewaard (Info.letter). Het bestand wordt echter onder de naam Info.letter.txt bewaard. Maar indien er quotes omstaan ("Info.letter") wordt het bestand echt onder deze naam bewaard. Het doel van die automatische extensie is dat het document nog steeds herkenbaar blijft als een Notepad bestand. (.txt).

De Recycle Bin versus de Recycler folder

Opmerking:
Dit geldt alleen indien er NTFS als bestandssysteem gebruikt wordt!!

Op NTFS-partities is standaard een folder genaamd Recycler aanwezig. In deze folder staat minimaal één, maar meestal meerdere Recycle Bins. Deze Recycle Bins hebben als naam een lang nummer, bijvoorbeeld S-1-5-21-100929458-935556567-212551020-1377. Dit nummer is het zogenaamde SID (Security IDentifier) van de eigenaar, is een NT-user, van de bewuste Recycle Bin.

De combinatie NT / NTFS maakt dus voor elke gebruiker zijn eigen Recycle Bin aan! De gebruiker merkt dit niet omdat op de desktop altijd zijn / haar eigen Recycle Bin staat. Omdat FAT niet de mogelijkheid bied om per gebruiker bij te houden wie wat heeft verwijderd, wordt daar gewerkt met een algemene Recycle Bin.

Probeer dan ook niet deze Recycler directory te verwijderen omdat NT zelf bij de eerste keer iets weggooien, deze directory met daarin een Recycle Bin voor de huidige gebruiker zal aanmaken.

Instant Task Manager

Er zijn twee manieren om snel de Task Manager tevoorschijn te halen:
- Rechtsklik op de Taakbalk en kies voor Task Manager
- Of gebruik de toetsencombinatie CTRL+SHIFT+ESC

Tips en trucs voor de ervaren gebruiker

Installeren op EIDE harde schijven groter dan 8 GB

Het standaard stuurprogramma voor EIDE schijven (ATAPI.SYS) kan niet meer ruimte adresseren dan 8GB, ook al is de schijf groter. Vanaf Service Pack 4 is dit probleem verholpen. SP4 installeert een nieuwe versie van deze driver en vanaf dat moment is het mogelijk om ook de resterende ruimte te gebruiken.

Om bij een nieuw systeem direct de maximale ruimte te kunnen benutten moet de betreffende driver naar de NT installatie diskettes gekopieerd worden en moet de installatie dus vanaf diskette worden uitgevoerd. Bedenk wel dat de maximale partitie grote initieel nooit groter dan 4 GB kan zijn. Dit omdat de installatie altijd op FAT basis wordt uitgevoerd en NT een maximale cluster grootte van 64 KByte ondersteund. De driver is los te downloaden van ftp://ftp.microsoft.com/bussys/winnt/winnt-unsup-ed/fixes/nt40/atapi/atapi.exe.

Het snelst is het dus om de ondersteuning toe te laten voegen door de installatie van het Service Pack en daarna de partitie grootte aan te passen met een programma als Partition Magic.

Converteren van FAT naar NTFS

Om een drive van het FAT-type te converteren naar NTFS, start een Command Prompt en type het volgende commando in:

```
CONVERT <drive> /FS:NTFS
```

Indien de drive de boot drive is, zal het converteren pas plaats vinden bij het opnieuw starten van het systeem. In alle andere gevallen wordt de drive meteen geconverteerd. Om dit te kunnen uitvoeren moet men wel Administrator privileges hebben.

Mogelijke problemen met Disk Administrator en Zip Drives

Het kan gebeuren dat het starten van Disk Administrator crashed waardoor Dr. Watson verschijnt. Dit treedt op indien er een SCSI-ZIP drive in / aan het systeem zit, de voortgangsbalk genaamd "Disk Administrator is Initializing" zichtbaar is en de ZIP drive is het enige of eerste apparaat op de SCSI controller met het laagste basis I/O adres.

Dit zorgt er voor dat de controller het eerst door Disk Administrator ondervraagd wordt. Het probleem treedt alleen op indien er geen disk in de drive zit. Indien er wel een disk in de drive zit dan zal de disk correct geïdentificeerd worden.

Er zijn een aantal oplossingen mogelijk:
- Zorg dat er altijd een disk in de ZIP-drive zit voordat Disk Administrator gestart wordt.

- Sluit de ZIP-drive aan op de SCSI controller waaraan ook de HD's van het systeem zelf zitten en verwijder de ZIP-controller. Je moet dan natuurlijk wel SCSI-HD's hebben...
- Stel, indien mogelijk, het I/O addres van de ZIP controller in op een hoger adres (hexadecimaal) dan het adres van de controller met de HD's.

Instellen van de drive letter van een CD-Rom en/of een ZIP

Het kan zeer onhandig zijn dat de CD-Rom speler de eerste drive letter na de locale vaste schijven krijgt. Dit is vooral problematisch als er gebruik wordt gemaakt van verwisselbare media als ZIP-drives. Het is mogelijk om de CD-Rom, net zoals onder Windows 95, op een bepaalde drive letter vast te zetten.

Start Disk Administrator (onder Programs -> Administrative Tools menu.) Klik op de CD-Rom partitie. Kies Tools->Assign drive letter. Nu is het mogelijk om zelf te bepalen wat de drive letter moet zijn. Het handigst is het om voor Z: te kiezen, deze staat namelijk nooit in de weg.

Vanaf Service Pack 5 is het nu ook mogelijk geworden om de drive letter van een ZIP drive via de Disk Administrator in te stellen! Dit voorkomt dus een hoop problemen bij systemen waar de ZIP nog wel eens aan de wandel gaat.

Het vollopen van de Log-files

Standaard gaat Windows NT niet netjes om bij een volle log file, sterker nog er kunnen zelfs rare dingen gebeuren! Het beste is het om de System, Application, en Security Logs op "Overwrite events as needed" te zetten, hierdoor kan een log nooit vol raken. Start Event Viewer (onder Programs -> Administrative Tools), selecteer Log->Log Settings optie uit het Event Viewer menu en vink de optie "Overwrite events as needed" voor de drie verschillende log types aan (dit moet dus drie keer gedaan worden).

Valide TCP/IP adressen voor eigen netwerken

De TCP/IP specificatie (RFC1597) heeft speciaal een aantal TCP/IP adressen gereserveerd voor gebruik op privé netwerken. Bij het gebruik van deze adressen gebeurd er in principe niks desastreus indien het netwerk per ongeluk met het Internet verbonden wordt. De volgende adres gebieden mogen gebruikt worden.

10.0.0.0	-	10.255.255.255	(Klasse A netwerk)
172.16.0.0	-	172.31.255.255	(Klasse B netwerk)
192.168.0.0	-	192.168.255.255	(Klasse C netwerk)

De gereserveerde netwerk adressen zijn van het type klasse A, B en C, hierdoor is er geen beperking in het ontwerp en grote van het eigen netwerk. Omdat er geen directe connectie met het Internet is -en mag zijn- doet het er niet toe dat dezelfde adressen misschien ook gebruikt worden door andere privé netwerken. Het enige wat van belang is, is dat binnen het eigen netwerk de adressen uniek zijn (met het correcte gebruik van DHCP-servers is dit geen probleem.)

NT draaien op een "small memory foot print"

NT kan draaien op machines met maar 12 tot 16 Mb intern geheugen. De verbetering van de performance, die bereikt wordt met het stoppen van niet essentiële processen, services en netwerk protocollen, is aanzienlijk. Het vrijkomende geheugen kan Windows NT dan gebruiken voor het laden van de benodigde programma's en het cachen van

bestanden. Om services te stoppen opent men het Services applet in het Control Panel en selecteert de te stoppen service en klikt daarna op de Stop knop.

Let op: Stop alleen services en processen, waarvan je weet wat ze doen. Sommige services zijn van essentieel belang voor het correct functioneren van Windows NT en mogen dus niet gestopt worden. Hieronder staan niet essentiële services en processen die afgesloten kunnen worden en de geheugen winst die er mee geboekt wordt.

Service / Process		Naam	Doel	Geheugen
S	Messenger	thread in services.exe	Stuurt en ontvangt pop-up boodschappen	49 Kb
S	Telephony Server	Tapisrv.exe	Handelt het bellen en RAS-connecties af	200 Kb
S	Schedule	Atsvc.exe	Start programma's in de achtergrond op vooraf bepaalde tijden	1,2 Mb
S	ClipBook Server	Clipsrv.exe	Deelt Clipboard bestanden over een netwerk	1,3 Mb
S	Spooler	Spoolss.exe	Handelt het printen af. Stoppen van deze service maakt printen op deze computer onmogelijk.	1,7 Mb
S	Network DDE en Network DDE DCOM	Nddeagnt.exe en Netdde.exe	Maakt DDE over het netwerk mogelijk, wordt o.a. door Hearts en Chat gebruikt.	1,6 Mb
P	De Explorer	explorer.exe	De standaard shell van NT verzorgt het bureau blad en het startmenu.	1-3 Mb
S	Netwerk services en protocollen	Control Panel→Network	Uitschakelen overbodige protocollen en services	0-2 Mb

Activeren Ultra DMA ondersteuning

De kans is groot dat je niet het uiterste uit je nieuwe harde schijven haalt. Windows NT4 activeert namelijk standaard **niet** de Ultra-DMA ondersteuning!. Met het volgende stappenplan is het mogelijk om snel en eenvoudig het maximale uit je schijven te halen. Ter indicatie een Maxtor DiamondMax 10GB in een Celeron 300A systeem haalde na de wijziging ongeveer rond de 13MB/sec "average sustained transactions" bij een processor belasting van 5%. Voor de wijziging was dit ongeveer 6MB/sec. Dit loont toch echt wel de moeite lijkt me!

Stap 1: Zonder de juiste hardware hoef je natuurlijk niks te beginnen. Controleer dus of zowel het moederbord als de harde schijven UDMA ondersteunen. Indien het moederbord een Intel LX, EX, ZX of BX chipset bevat, dan is het moederbord geen probleem.

Step 2: Installeer Service Pack 4 of hoger en herstart het systeem. Maar als het goed is heb je deze reeds geïnstalleerd, niet waar? En je hebt ookal de Rescue Disk ververst? Zo niet, doe dat dan!

Stap 3: Download het programmaatje CLIBench. http://www.geocities.com/SiliconValley/Vista/9159/clibench.zip. Dit is een eenvoudige benchmark, maar het stelt je instaat om te controleren of de installatie van het SP de UDMA instellingen geactiveerd heeft. Draai een "Disk Throughput" test voor elke schijf die UDMA ondersteund.

Stap 4: Download DMACheck en start het. Activeer DMA voor alle IDE kanalen waaraan DMA compatibele schijven hangen en herstart vervolgens het systeem.

Stap 5: Draai nu opnieuw de "Disk Throughput". Indien er een aanzienlijke verandering is (zie stap 7 voor de cijfers), dan is de operatie geslaagd. Is dit echter niet het geval én DMA was nog niet actief (Stap 4), dan moeten we nu de registry induiken. Het blijkt namelijk ookal geeft DMACheck aan dat UDMA actief is,

deze niet noodzakelijk gebruikt wordt door NT. Met de volgende aanpassingen is dit echter te forceren.

Stap 6: Ga naar de volgende hive(s):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\atapi\Parameters\Device 0
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\atapi\Parameters\Device 1

Welke, dat is afhankelijk waar je UDMA wilt activeren. Zoek daar de key genaamd **DmaDetectionLevel**. Deze kent drie mogelijke waarden:

0x0 = Disable
0x1 = Autodetect
0x2 = Always Enabled

Nu is het zo dat he kiezen van activeren in DMACheck niet de waarde 0x2 in de registry plaatst, maar 0x1!. Het punt is dat NT dan toch kan besluiten, ookal ondersteund alle aanwezige hardware het, om UDMA uit te zetten. Met 0x2 forceer je dus UDMA ondersteuning. Herstart het systeem na de wijzigingen. Kan je het systeem nu niet meer starten, blijkbaar zijn je spullen toch niet UDMA..., dan kan je altijd nog kiezen voor de optie "Last Known Good" tijdens de systeem start en wordt de oude situatie weer in ere hersteld

Stap 7: Draai nu opnieuw de "Disk Throughput" test en controleer of er een verschil is. Ter indicatie een Maxtor DiamondMax 10GB in een Celeron 300A systeem haalde na de wijziging ongeveer rond de 13MB/sec "average sustained transactions" bij een processor belasting van 5%. Voor de wijziging was dit ongeveer 6MB/sec.

Het zal duidelijk zijn dat een verdubbeling van de schijfdoorvoer toch wel een verdomd leuke winst is. Zeker omdat je tenslotte al betaald hebt voor de hardware en het je hoogstens een tijdsinvestering van een stief kwartiertje kost.

Benodigde downloads. Deze staan ook op het Windows Forum (GO NLWINDOWS) in de library Windows NT:
CLIBench = http://www.geocities.com/SiliconValley/Vista/9159/clibench.zip.
DMACheck = http://support.microsoft.com/download/support/mslfiles/Dmachcki.exe.

Instellen van de Pagefile en bepalen werkgeheugen

Een heel belangrijk onderdeel en tevens het minst begrepen onderdeel van Windows NT zijn de Virtueel geheugen instelling en dus de pagefile. Een niet correct ingestelde pagefile kan als een enorme handrem werken op de performance van een systeem. Initieel gaat het meestal wel goed met de standaard instelling van de pagefile. Het gaat pas mis, als een systeem wat langer gebruikt wordt of als er extra geheugen wordt toegevoegd. Omdat de Windows NT page file niet dynamisch is (dit i.t.t. die van Windows 9x) moeten we dus zelf deze correct instellen. Hiervoor zijn er een aantal vuistregels beschikbaar.

De Microsoft vuistregel voor de grote van de page file is: Intern geheugen + 12 Mb. De reden hierachter is tamelijk eenvoudig te verklaren. Microsoft heeft NT zo ontworpen dat deze bij een zware systeem crash de gehele geheugen inhoud naar de pagefile kan schrijven. Daarom moet deze dus minimaal zo groot zijn als het interne geheugen met

wat extra ruimte voor wat boekhouding. Bevat de machine dus 128 Mb (wat standaard zou moeten zijn in elke NT machine) dan is de page file dus 140Mb.

Vandaag de dag is dit een regel die niet meer echt werkt. Het is tenslotte niet mogelijk dat één regel zowel opgaat voor een machine met 32 Mb en een machine met 512 Mb aan boord. Daarom volgen nu algemene drie regels en een methode om zelf de optimale grootte te kiezen.

Geheugen	Regel	Voorbeeld
<96	RAM * 1,75	64 intern -> 112Mb pagefile
128-256	RAM * 1,5	128 intern -> 192 Mb pagefile
> 256	RAM + 12	256 intern -> 268 pagefile

Voor machines met meer dan 256 Mb geldt dat als het kunnen dumpen van het geheugen voor analyse doeleinden je **niet** interesseert je ook van de regel RAM * 0.75 kunt uitgaan. Maar bedenk dat het niet erg is als pagefile te groot is.

Het instellen van de grote van de page file gebeurd via Control Panel -> System Properties -> tabblad Performance. Ga daar naar de sectie "Page File Size for selected Drive". Initieel zullen we alleen de instellingen van pagefile aanpassen voor de schijf waar de Winnt directory staat. De optimalisatie van de locatie komt hierna aanbod. Er zijn twee waarden in te geven: "Initial Size" en "Maximum Size". Laat je niet in de luren leggen door deze twee opties, de waarden **moeten** gelijk zijn! Als de initiële grote namelijk te klein is zal de pagefile alleen maar fragmenteren en kostbare processor tijd opeten. NT gaat standaard namelijk van de opgegeven initiële grote uit bij het aanmaken van de pagefile en zal deze zo nodig vergroten. De kunst is dan ook om te voorkomen dat er dus expansie nodig is én dat de maximale grote voldoet! Bepaal de grote van de pagefile vast aan de hand van de drie hierboven gegeven regels, waarbij dus Initial en Maximum even groot moeten zijn, en vul deze in. Herstart vervolgens het syteem, iets wat NT toch wel zal eisen.

De volgende stap is het achterhalen hoe groot de pagefile nu eigenlijk moet zijn, of beter: Hoeveel virtueel geheugen is nu echt nodig? Hiervoor moet de computer stevig, maar wel volgens het normale patroon gebruikt worden. Doe geen dingen die je normaal ook niet doet. Dus geen bestanden van 500 Mb gaan laden e.d. Het doel is tenslotte om de geheugen behoefte bij normaal gebruik te achterhalen.

Nadat je dit dus gedurende een dag gedaan hebt wordt het tijd om de Task Manager op te roepen. Dit kan via rechtsklikken Taakbalk en vervolgens Task Manager of via de toetsencombinatie SHIFT+CTRL+ESC. Ga nu naar het tabblad "Performance". De sectie die voor ons van belang is, is "Commit Charge (K)" sectie. Hier kan je het eenvoudigst achterhalen hoeveel geheugen je hebt en hoeveel Virtueel Geheugen je zou moeten hebben.

Er zijn drie waarden beschikbaar in deze sectie. Deze drie waarden vertellen je het volgende:

Total: De hoeveelheid geheugen, zowel echt als virtueel, dat momenteel in gebruik is. Dit cijfer doet er eigenlijk niet toe.

Limit: De maximale hoeveelheid geheugen, zowel echt als virtueel, die je kunt gebruiken.

Peak: Dit is nu de waarde waar het allemaal om draait. Dit is dus de maximale hoeveelheid geheugen, weer zowel echt als virtueel, die tijdens deze sessie in gebruik was.

Indien de peak waarde hoger is dan die van het limit, dan heb je een serieus probleem. Je hebt dan meer virtueel geheugen nodig en vermoedelijk ook meer fysiek geheugen.

Hoe bepaal je nu echter waarvan je meer nodig hebt? In de perfect NT wereld zou het zo moeten zijn dat de peak waarde nooit hoger ligt dan wat er fysiek aan geheugen in de machine zit. De hoeveelheid benodigde fysieke geheugen is dus aan de hand van de peak waarde en de aanwezig hoeveelheid fysiek geheugen te achterhalen. Zodra de peak waarde namelijk meer dan 50% is van de hoeveelheid fysiek geheugen wordt het tijd om geheugen bij te plaatsen. Stel dat je dus 64Mb aan geheugen hebt, dan mag de peak waarde dus niet boven de 96Mb uitkomen. Is dit wel het geval, dan moet er dus geheugen bij. Neem als voorbeeld mijn huidige machine. De peak waarde staat nu op 88,654K. Dat is dus niet boven die 50% indien er 64 Mb aan geheugen in zou zitten, maar desondanks zit er dus toch 128 Mb in deze machine. Het werkt gewoon fijner.

Kortom, zorg dat die peak waarde binnen de 50% blijft en je zit gebakken. Zit je echter al binnen die 50%-grens dan is de keuze voor meer geheugen dus helemaal aan je zelf. Het hebben van meer geheugen dan de peak waarde is iets waar ik persoonlijk naar zou streven. Maar doe je dat niet dan blijft toch de impact op de performance redelijk binnen de grenzen zolang je maar niet te dicht bij die 50% grens komt met de peak waarde.

Na het bepalen van de hoeveelheid fysiek geheugen is het nu tijd om eens te kijken naar de hoeveelheid virtueel geheugen. Gebaseerd op de aangegeven vuistregels moet deze al goed staan. Waar je dus in ieder geval voor moet zorgen is dat de peak waarde **nooit** hoger komt dan de Limit waarde. Als je over de limit waarde gaat, gaat NT namelijk toch de grootte van de pagefile aanpassen en dat veroorzaakt dus pagefile fragmentatie en dat vertraagd het systeem alleen maar. Zolang je de hierboven beschreven regels hanteert is de kans wel vreselijk klein, eigenlijk bijna onmogelijk, dat je over de limit waarde gaat.

De locatie van de pagefile kan ook nog wat uitmaken. Standaard zal NT de pagefile op de schijf waar ook de %winnt% naar wijst. Dit is standaard eigenlijk de C-schijf. Dat is alleen optimaal indien je de beschikking hebt over één fysieke harde schijf. Zodra je dus twee of meer schijven hebt loont het de moeite om de pagefile er over te gaan verdelen. Begin echter absoluut niet aan het splitsen van de pagefile over verschillende partities op één schijf. Die schijf kan tenslotte maar één ding te gelijk en NT is daarentegen wel in staat om meerdere lees/schrijf opdrachten tegelijkertijd uit te hebben staan. Hierdoor is NT ook zo goed instaat voordeel te halen uit het feit dat de pagefile gesplitst is over meerdere schijven. Bij IDE schijven is het trouwens het beste om in het geval van splitsen de schijven op de verschillende kanalen te hebben zitten.

Optimaliseer I/O verkeer

Deze aanpassing was van oorsprong alleen bedoeld voor de zware server, maar gezien de ontwikkelingen op de markt is de PC van vandaag gelijkwaardig aan de server van gisteren. Daarom kan het best wel de moeite lonen op de IOPageLockLimit registry waarde te optimaliseren. Standaard staat deze op 0 wat door NT gelijk wordt gesteld aan 512KB. Machines die een heftig schijf gebruik kennen én die een aanzienlijke hoeveelheid geheugen bevatten (meer dan 128 MB), waarvan structureel niet alles gebruikt wordt zijn de aangewezen kandidaat voor deze aanpassing. Alle andere machines, zeker als deze minder dan 128 MB bevatten, komen dus **niet** in aanmerking voor deze tweak!!

Een goede start waarde voor de IOPageLockLimit is 64 tot 128 keer het totale interne geheugen in MB maar dan in KB uitgedrukt (uitleg volgt <s>). Voor een machine met 128MB levert dat dus een waarde op tussen 8192KB en 16384KB

Dit is helaas een generieke regel en je zult dus zelf aan de slag moeten om te bepalen wat de optimale instelling voor jou systeem is. Verwacht daarnaast niet extreme wijzigingen in de performance, maar alle beetjes helpen en als het maar genoeg beetjes zijn dan valt het wel op.

LET OP: Een wijziging in deze key **kan** als effect hebben dat het systeem **niet** meer start. Een up-to-date Recovery Disk is dus absoluut geen luxe bij deze tweak.

Start de registry editor en breng de aangeven wijzigingen aan.

Hive:	HKEY_LOCAL_MACHINE\System
Key:	CurrentControlSet\Control\Session Manager\Memory Management
Naam:	IOPageLockLimit
Type:	REG_DWORD
Waarde:	0 (standaard)

Wijzig de waarde van *Hex* naar *Decimal* en vul de berekende waarde in. Sluit vervolgens de registry editor en herstart de computer om de wijziging door te voeren.

Registry hacks

Indien een bepaalde key zoals deze in een tip wordt aangegeven niet aanwezig is dan moet deze dus aangemaakt worden. Let er dan wel op of het nuttig is om de tip door te voeren. Sommige tips hebben namelijk betrekking op een specifieke situatie qua hardware of software.

In bijlage IV kunnen een aantal wijzigingen teruggevonden worden die na knippen en plakken direct doorgevoerd kunnen worden in de Registry.

Registry Editor

Er gaan veel spook verhalen rond over het wel of niet gebruiken van een bepaalde Registry editor met Windows NT, hieronder staat een overzicht van de Editors en hun gebruik.

	Windows NT	Windows 95
Regedit.exe (NT)	✓	✓
Regedt32.exe (NT)	✓	✗
Regedit.exe (W95)	✗	✓

Kortom, gebruik **nooit** de Windows 95 Registry Editor voor een **Windows NT Registry**. De editors die meegeleverd worden met NT zijn dus wel veilig.

Het belangrijkste verschil tussen Regedit (NT) en Regedt32 is dat er met Regedt32 de rechten op trees, hives, en keys kunnen worden gewijzigd en dat delen van een tree of hive bewaard en ingeladen kunnen worden terwijl met Regedit in alle elementen (keys, values en data) gezocht kan worden naar een bepaalde waarde of string.

Instant paden in een Dos venster

Het kan tamelijk lastig zijn om in een dos venster lange bestands- en folder namen correct in te typen. Gelukkig kan NT zelf meestal de namen in en aanvullen. Typisch genoeg staat deze optie standaard uit.

Hive: HKEY_CURRENT_USER\Software
Key: Microsoft\Command Processor
Naam: CompletionChar
Type: REG_DWORD
Waarde: 9
Naam: EnableExtensions
Type: REG_DWORD
Waarde: 1

In een dos venster hoeft nu, voor een commando, slechts de eerste twee karakters van het bestand of folder te worden ingetikt. Met een druk op TAB vult NT zelf het eerste bestand of foldernaam in die voldoet. Indien deze niet correct is, druk dan net zolang op TAB totdat de juiste folder c.q. bestandsnaam verschijnt.

Console vensters onder NT (DosBox)

Onder Windows NT is het mogelijk om de algemene eigenschappen voor NTVDM (NT Virtual Dos Machine) in te stellen. Deze eigenschappen worden dan door alle NT Console programma's gebruikt. Deze eigenschappen gelden ook voor die DOS-

programma's die niet een eigen PIF-bestand hebben. Ga met de Explorer naar de Windows NT directory en rechtsklik op het bestand _default.pif en kies voor Properties.

Het is even van belang om te weten dat deze en alle ander PIF-bestanden gebruik maken van de Config.nt en de Autoexec.nt in de <winnt>\system32 directory. Zo is o.a. in de Config.nt de optie EMM= terug te vinden. Met deze optie is het geheugengebruik voor EMS te fine tunen. Indien er zo veel mogelijk geheugen beschikbaar moet zijn kan deze optie het beste op RAM gezet worden (EMM=RAM).

Tijdens het starten gebruikt Windows NT ook de autoexec.bat indien deze aanwezig is. Hieruit worden meestal een additioneel pad en een aantal omgevingsvariabelen gehaald, de rest wordt genegeerd. Met de volgende instelling is te voorkomen dat NT überhaupt gebruik maakt van autoexec.bat.

Hive: HKEY_CURRENT_USER\Software
Key: Microsoft\WindowsNT\CurrentVersion\WinLogon\
Naam: ParsAutoexec
Type: REG_SZ
Waarde: 0

Automatisch inloggen activeren

Het is mogelijk om het inlog venster te omzeilen. Dit kan door de in te vullen naam en paswoord in de Registry vast te leggen. Vul hier je domain naam (indien van toepassing), account naam en password in. Indien de aangegeven optie niet aanwezig is dan moet deze dus worden aangemaakt.

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: Microsoft\WindowsNT\CurrentVersion\WinLogon
Naam: DefaultDomainName
Type: REG_SZ
Waarde: {het domain of workgroup}
Naam: DefaultUserName
Type: REG_SZ
Waarde: {de gebruikernaam}
Naam: DefaultPasword
Type: REG_SZ
Waarde: {het wachtwoord}
Naam: AutoAdminLogon
Type: REG_SZ
Waarde: 1

Is de DefaultPassword string niet is ingevuld dan zal Windows NT automatisch de waarde van de AutoAdminLogon key van 1 (true) in 0 (false) veranderen en hiermee de AutoAdminLogon feature weer uitschakelen.

Automatisch Inloggen deactiveren

Indien automatisch inloggen actief is, is deze te deactiveren door tijdens het starten van Windows NT de **SHIFT**-toets ingedrukt te houden, totdat de Welcome Dialog box verschijnt. Indien je reeds ingelogd bent, druk dan CTRL+ALT+DEL en kies de Log off knop, klik op de OK knop en druk daarna onmiddellijk de SHIFT toets in totdat de Welcome dialog box verschijnt. Volg de stappen zoals hiervoor beschreven om Automatisch inloggen weer te activeren.

Locatie van automatisch startende software

Windows NT heeft naast de groepen Startup, zowel Common als persoonlijk, ook nog een Registry key waar software geregistreerd staat die wel automatische gestart moet

worden maar die niet in een startup groep mag staan. Dit geldt bijvoorbeeld voor TweakUI en de Systemtray.Onder H**KEY_LOCAL_MACHINE\Software \Microsoft\Windows\CurrentVersion\Run** zijn deze programma's terug te vinden.

Terugvinden van de CD-Key

Zonder CD-Key geen nieuwe installatie. Maar soms is het wel een lastig om deze terug te vinden. Gelukkig staat deze ook in de registry verstopt en wel onder: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion** in het item **ProductId**. De CD-key loopt van het 6de tot en met het 15de getal.

Instellen van de standaard NT-shell

Het is mogelijk om zelf te bepalen welke shell Windows NT standaard gebruikt. Open de Registry en ga naar de subkey **HKEY_LOCAL_MACHINE/Software /Microsoft/WindowsNT/CurrentVersion/Shell**

Standaard gebruikt NT als shell Explorer.exe, maar op machines met weinig geheugen is het mogelijke om als shell te kiezen voor CMD.EXE. Het is altijd mogelijk om programma's te starten via de TaskManager. Deze is via de CTRL+ALT+DEL combinatie te bereiken.

Muismarges instellen

Computer-beginnelingen hebben nogal eens moeilijkheden om bij het dubbelklikken de muis op de juiste plaats te houden. Windows laat een bepaalde afwijking van +/- 4 pixels toe om dat te ondervangen. Je kan die tolerantie wat ruimer zetten via de volgende registry instellingen:

Hive: HKEY_CURRENT_USER
Key: ControlPanel\Mouse
Waarde: DoubleClickHeight
Type: REG_SZ
Waarde: DoubleClickWidth
Type: REG_SZ
Waarden: 4 tot 32

Wijzigen van Internet Auto-Search

Standaard zoekt IE op Yahoo bij het ingeven van GO met keywords. Ga naar **HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchUrl** en wijzig de zoek-string in die voor één van de onderstaande zoeksites.

Zoek site	Auto-search string
AltaVista	www.altavista.digital.com/cgibin/query?pg=q&q=%s
Excite	www.excite.com/search.gw?search=%s
Infoseek	guidep.infoseek.com/Titles?qt=%s
Lycos	www.lycos.com/cgibin/pursuit?query=%s
MSIE-default	home.microsoft.com/access/autosearch.asp?p=%s
Yahoo (MSIE)	msie.yahoo.com/autosearch?p=%s
Yahoo (normaal)	search.yahoo.com/bin/search?p=%s

Bepalen van het browsertype

Het is mogelijk om een werkstation wel of niet een Preferred Browser te maken.

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\Services\Browser\Parameters

Naam: MaintainServerList
Type: REG_SZ
Waarde: Auto/Yes/No

Activeren van HPFS ondersteuning

Standaard is er geen ondersteuning voor HPFS meer aanwezig in NT 4.0. Om nu toch NT 3.x en OS/2 HPFS schijven te kunnen benaderen moet er gebruik gemaakt worden van het HPFS stuurprogramma van NT 3.51, deze is op deze site onder Downloads en Tools beschikbaar.

Voer de volgende stappen uit om het HPFS stuurprogramma te activeren:

- Kopieer het bestand **PINBALL.SYS** naar de **winnt\system32\drivers** subdirectory.
- Open in de Registry Editor de volgende key:
  HKEY_LOCAL_MACHIN\SYSTEM\CurrentControlSet\Services
- Maak via Edit -> New -> Key de key "Pinball" aan.
  ✓ Voeg aan de Pinball key (via Edit -> New, of rechtsklikken in het rechterpaneel) de volgende drie *DWORD Value* keys toe:
  ✗ Value Name : ErrorControl
  Value Data : 1
  Base : Hexadecimal
  ✗ Value Name : Start
  Value Data : 1
  Base : Hexadecimal
  ✗ Value Name : Type
  Value Data : 2
  Base : Hexadecimal
- Voeg aan de Pinball key (via Edit -> New) de volgende *String value* key toe:
  Value Name : Group
  Value Data : Boot file system

Controleer, na het herstarten van het systeem, via Control Panel -> Devices of het Pinball stuurprogramma geladen is. Is dit het geval dan kunnen de aanwezige HPFS schijven benaderd worden. Bedenk wel dat sommige features zoals o.a. de Recycle Bin en Diskeeper Lite niet zullen werken op de HPFS schijven.

Koppelen uitzetten bij een onbekend bestand

Bij het dubbelklikken op een onbekend bestandstype, is het mogelijk om via de Open With dialog box het te gebruiken programma aan te geven. Het probleem is alleen dat standaard de " Always use" checkbox aan gevinkt is. Met de volgende wijziging in de registry is dit eenvoudig te voorkomen en zal het vakje standaard **geen** vinkje meer bevatten.

Hive: HKEY_CLASSES_ROOT\Unknown
Key: Unknown\shell\OpenAs\command
Naam: default

Dubbelklik op de (default) ingang in het Contents venster en voeg vervolgens een **spatie** en een **%2** direct toe achter de %1 en sluit vervolgens weer de registry editor.

Notepad koppelen aan onbekende bestanden

Hiermee wordt het mogelijk om Notepad als de standaard applicatie in te stellen voor bestanden die niet aan enige andere programma gekoppeld zijn. Tevens wordt standaard Notepad aan het rechtsklik menu toegevoegd voor elk bestand. Hierdoor wordt het mogelijk om willekeurig welk bestand te openen in Notepad zonder het Send-To menu

te gebruiken en het wordt mogelijk om op een bestand zonder associatie, zoals config.sys, te dubbelklikken en deze zo te openen in Notepad.

Ga naar de key **HKEY_CLASSES_ROOT\Unkown\Shell**. Open deze key en creëer hier de key "**Notepad**". Open ook weer deze key en maak hier de key "**Command**" aan. Klik nu op deze key en wijzig de optie Default, die rechts aanwezig is. Dubbelklik hierop en vul hier nu het volgende in: **notepad "%1"** (let op de quotes om de %1!). Klik op OK, druk vervolgens op F5 (verversen) en test het uit.

Het volledige pad van de net gemaakte registry key moet er dus als volgt uitzien:
HKEY_CLASSES_ROOT\Unkown\Shell\Notepad\Command

Uitschakelen bewaren DUN wachtwoord

Standaard is het mogelijk om de gebruikersnaam en het wachtwoord te bewaren d.m.v. het selectie vakje in het dial-up networking (DUN) venster. Dit is een potentieel gevaarlijke situatie, want onbevoegden kunnen nu eenvoudig inloggen onder de naam van de gebruiker. Met de volgende wijziging in de registry is deze optie uit te schakelen:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\Services\RasMan\Parameters
Naam: logging
Type: REG_DWORD
Waarde: 1

Na een herstart zal DUN de checkbox "save password" niet meer laten zien in het inbelvenstertje.

Opnemen door de Ras-server instellen

Standaard neemt een RAS server direct de telefoon op. Soms is dit echter te snel en is het beter om minimaal één of twee "rings" te wachte. Dit is helaas alleen via een registry ingreep in te stellen:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\Control\Class

Klik op Class en zoek naar het modem en wel naar het item ATS0=0. Verander de 0 in het aantal gewenste "rings" en herstart de server.

Wachtwoord termijn instellen

Zo'n veertien dagen voordat het wachtwoord verloopt begint NT al te waarschuwen. Op zich goed bedoelt, maar toch wel erg overdreven. Vijf dagen van te voren is meestal vroeg genoeg. Deze termijn is via de volgende key eenvoudig in te stellen.

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: Microsoft\WindowsNT\CurrentVersion\Winlogon
Waarde: PasswordExpiryWarning
Type: REG_DWORD
Waarde: {aantal dagen}

Snel herstarten

Het is mogelijk om de herstart tijd van NT aanzienlijk te verkorten door een item aan de WinLogon key toe te voegen. Een bij komend voordeel van deze methode is dat het ook nog een relatief correcte manier is om Windows af te sluiten. Daarnaast is het de beste dan wel enige manier om zonder veel brokken te herstarten wanneer de machine vast zit in cpu-loops, of wanneer zelfs het startmenu en/of crtl-alt-del niet meer werken.

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: Microsoft\WindowsNT\CurrentVersion\Winlogon
Waarde: EnableQuickReboot
Type: REG_SZ
Waarde: 1

Herstart vervolgens het systeem. Hierna is het mogelijk om een snelle herstart uit te voeren met de toetsencombinatie: Shift+Ctrl+Alt+Delete. Deze actie genereert een Event ID 6008 “unexpected schutdown record” in de systeem eventlog.

Hangende programma's

Soms komt het wel eens voor dat één of andere applicatie niet reageert en dat je deze moet stoppen met de "End Task". Vooral bij het uitloggen of als je een snelle herstart wilt is dit een leuke ergenis. Met de volgende wijziging in de Registry is dit op te lossen:

Hive: HKEY_USER\.Default
Key: Control Panel\Desktop
Waarde: AutoEndTask
Type: REG_SZ
Waarde: 1

Hive: HKEY_CURRENT_USER
Key: Control Panel\Desktop
Waarde: AutoEndTask
Type: REG_SZ
Waarde: 1

Elke taak wordt nu gedwongen om te stoppen na een eventuele crash. Een stap verder gaat het instellen van de wachttijd met de waarde **WaitToKillAppTimeOut** (REG_SZ) (zelfde locatie) waarin de standaard-instelling 20000 milliseconden is. Als de gebruiker niet zelf reageert binnen deze tijd wordt de gecrashte applicatie automatisch gestopt.

Het beperken van een NT Explorer Crash

Een manier om te voorkomen dat een crash van de Explorer je in de kou laat staan is het mogelijk om elk Explorer venster een apart proces te laten zijn. Dit is vooral handig indien de desktop update van IE4 gebruikt wordt. Omdat deze optie te activeren, moet in de Registry Editor de volgende key gewijzigd worden:

Hive: HKEY_LOCAL_MACHINE\Software
Key: Microsoft\Windows\CurrentVersion\Explorer
Naam: DesktopProcess
Type: REG_DWORD
Waarde: 1

Sluit cervolgens de Registry Editor, log uit en weer opnieuw aan. Vanaf nu is het mogelijk om toch toegang te hebben tot de taakbalk en de desktop, ook als een Explorer venster hangt. Het zal duidelijk zijn dit deze oplossing meer geheugen en processor capaciteit kost.

Separate Memory Space feature

Indien ter crash bescherming van 16-bits applicaties de Separate Memory Space functie bijna altijd gebruikt wordt dan is deze standaard te activeren. Wijzig de volgende registry entry.

Hive: HKEY_LOCAL_MACHINE\System

Key: CurrentControlSet\Control\WOW
Naam: DefaultSeparateVDM
Type: REG_SZ
Waarde: yes

Indien er nu 16-bits applicaties draaien dan zullen deze automatische in eigen VDM draaien ook al is het vakje onder properties niet aangevinkt!

Deactiveren van Dr.Watson

Dat Dr. Watson elke keer verschijnt als een programma crashed is wel leuk, maar eigenlijk alleen maar nutig voor de ontwikkelaar en niet bepaald nuttig voor een normale gebruiker.Verwijder de volgende key uit de registry om van Dr.Watson af te zijn:
HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows NT\ CurrentVersion\ Aedebug

Het herstellen van de activiteiten van Dr.Watson gaat via het volgende commando, uit te voeren van af de commandoregel: DRWTSN -i

Machine automatisch uitschakelen na shutdown

Deze optie staat al een hele tijd te boek, maar werkte in de praktijk nooit. Maar met ingang van Service Pack 4 en hoger is het wel mogelijk! Zorg dus wel dat eerst SP4 geïnstalleerd is. Zoek in het service pack het bestand **hal.dll.softex** op. Kopieer deze naar een tijdelijk locatie en hernoem deze vervolgens in **hal.dll**. Kopieer deze vervolgens naar de WINNT\SYSTEM32 directory, waar de originele hal.dll staat. (hernoem deze in b.v. hall.dll.org!) Maak vervolgens de volgende wijziging in de registry:

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: Microsoft\WindowsNT\CurrentVersion\Winlogon
Waarde: PowerDownAfterShutdown
Type: REG_SZ
Waarde: 1

Herstart vervolgens het systeem en zorg er voor dat APM wel actief is in het BIOS maar dat verder alle andere APM-timers gedeactiveerd zijn (harde schijf, beeldscherm e.t.c.).

Om het uitschakelen ook altijd goed te laten lukken kunnen het beste de volgende twee waarden ook gewijzigd c.q. ingevuld worden:

Hive: HKEY_CURRENT_USER\Software
Key: Microsoft\WindowsNT\CurrentVersion\Shutdown
Waarde: ShutDown Setting (Let op de spatie!)
Type: REG_DWORD
Waarde: 3
Waarde: Logoff Setting (Let op de spatie!)
Type: REG_DWORD
Waarde: 0

De volgende waardes zijn geldig in beide gevallen:
0 = Logoff
1 = Systeem afsluiten
2 = Systeem afsluiten en opnieuw starten
3 = Systeem afsluiten en computer afzetten (SP4/5 én ATX voeding)

Sectie 2: Achtergronden

Het starten van Windows NT

Het starten van Windows NT is een zeer complex proces, inzicht in dit geheel kan verhelderend werken op sommige gedragingen en aspecten van NT. Het starten van een Windows NT systeem is in vier stappen op te delen:

Fase	Omschrijving
De initiële fase	Voert de zelftest uit. Initialiseert de computer en localiseert de boot sectie op de primaire partitie. Hierna wordt de Ntldr (de Boot Loader) gestart;
De Boot loader fase	Verzamelt informatie over de aanwezige hardware en drivers voordat de kernel geladen wordt;
De Kernel fase	Laad en initialiseert de kernel en device drivers en laadt de verschillende services;
De Logon fase	Het boot proces wordt pas als afgerond beschouwd indien een gebruiker succesvol inlogt. Hierdoor wordt de Clone control set gecopieerd naar de LastKnownGood control set.

De initiële fase

De initiële fase omvat het hardware diagnostisch stuk.

De Power On Self Test (POST)

Dit is de eerste algemene test en NT onafhankelijk. Hierbij wordt de hoeveelheid intern geheugen bepaald en er wordt gekeken of alle benodigde hardware aanwezig is en functioneert. Na de algemen systeem POST krijgt elke adapter met een eigen BIOS de kans zijn eigen POST uit te voeren.

Initiële startup

De eerste sector op de aanwezige harde schijf is kritiek voor het opstart proces, dit omdat deze sector het Master Boot Record (MBR) en de partitie tabel bevat. Na de POST probeert het systeem BIOS een start schijf te localiseren. Meestal zal eerst naar een diskette gezocht worden en indien deze niet aanwezig is wordt er gezocht op de aanwezige actieve harde schijf (of schijven).

Master Boot Record

Indien de harde schijf de startschijf is als zal het BIOS de MBR uitlezen en deze in het geheugen laden. Hierna wordt de MBR-code geactiveerd. Deze code zal hierna opzoek gaan naar de Partitie tabel om zo de systeem partitie te kunnen localiseren. Indien de systeem partitie gevonden wordt, wordt de code die in sector 0 van deze partitie staat in het geheugen geladen en geactiveerd. Deze code kan een diagnostisch programma zijn, een virus… maar meestal is het de start code voor een OS. Indien er geen systeem partitie aanwezig is, dan zal het MBR een foutmelding geven in de trend van: “Invalid partition table”, “Error loading operating system” of “Missing operating system”.

Partitie Boot Sector

Wat de partitie boot sector precies doet is afhankelijk van het OS en het bestandssysteem. Op Intel machines is de NT partitie boot sector verantwoordelijk voor

het vinden van de boot loader (Ntldr) in de root van de schijf en het laden en starten van Ntldr.

Op Intel machines moet de systeem partitie zich op de eerste fysieke harde schijf bevinden. De boot partitie, deze partitie bevat Windows NT, kan de systeem partitie zijn, een andere partitie op dezelfde schijf of een partitie op een andere schijf.

De Boot loader fase

Gedurende de boot loader fase worden er door NT verschillende programma's gebruikt om informatie te verzamelen over de in de computer aanwezige hardware en de aanwezige drivers. Dit gebeurt voordat de kernel geladen wordt. In de volgende tabel worden deze programma's beschreven.

Bestand	Omschrijvng
Ntldr	Het OS systeem loader. Deze moet in de root van de schijf staan
Bootsec.dos	Een verborgen bestand die door Ntldr geladen wordt indien een ander OS, zoals MS-Dos geselecteerd wordt. Bootsec.dos bevat de pré-NT bootsector.
Boot.ini	Bevat de opbouw van het Boot Loader OS Selection menu
Ntdetect.com	Geeft informatie over de aanwezige hardware door aan Ntldr
Ntoskrnl.eze	De kernel
Ntbootdd.sys	De device driver nodig om SCSI apparaten aan te spreken, indien de adapter geen BIOS bevat of gebruikt.
SYSTEM	De **HKEY_LOCAL_MACHINE\SYSTEM** registry tak

De voor het systeem benodigde drivers, zoals SCSI en video drivers, worden ook gedurende deze fase geladen.

Het selecteren van het Operating Systeem

Ntldr bestuurt het OS selectie proces en de hardware detectie totdat de NT-kernel geïnitialiseerd is. Als de Ntldr gestart wordt verschijnt de volgende medeling op het scherm

```
OS Loader V4.0
```

Ntldr voert de volgende activiteiten uit:

- Schakelen van de processor in de 32-bits flat memory mode. Intel machines lopen namelijk standaard in real mode.
- Starten van de benodigde minifile systeem. Dit is nodig om een FAT of NTFS partitie aan te kunnen spreken. Deze code is in NTLDR ingebouwd. Hierdoor is het ook relatief lastig om FAT32 aan dit lijstje toe te voegen. Één bug en foetsie NT…
- Het lezen en weergeven van het Boot.ini. Het z.g.n. *boot loader screen*, het startmenu dus.
- De gebruiker laten kiezen uit de aanwezige OS-en. Indien voor NT wordt gekozen, dan wordt Ntdetect.com gestart om informatie over de aanwezige hardware te verzamelen.
- De keuze presenteren met welke configuratie, default of Last Known Good configuratie, de computer gestart moet worden. Dit is alleen het geval indien er op de spatiebalk gedrukt is of als er meerdere hardware profielen aanwezig zijn.
- Als laatste laadt en start Ntldr Ntoskrnl.exe en wordt de hardware informatie, die door Ntdetect.com verzameld is, doorgegeven.

Het detecteren van de aanwezige hardware (Ntdetect.com)

Ntdetect.com is het hardware identificatie programma voor Intel machines. Dit programma verzamelt een lijst met informatie over de aanwezige hardware en geeft deze informatie door aan Ntldr. De activering van Ntdetect.com is te herkennen aan de volgende melding op het scherm, na het selecteren van NT als gewenst OS in het boot loader menu.

```
NTDETECT V4.0 Checking Hardware . . .
```

Ntdetect.com is in staat om de volgende componenten te identificeren:

- Computer ID
- Bus/Adapter type (ISA,EISA,MCA,PCI)
- Video
- Toetsenbord
- Communicatie poorten (COM1..8)
- Parallelle poorten (LPT1..3)
- Diskdrives
- Muis

Ntdetect.com is dus niet instaat om aanwezige multimedia kaarten te detecteren. Indien deze ISA én PnP zijn, kan de speciale PnP-Enabler later in het startproces deze taak op zich nemen.

Het kiezen van een configuratie (optioneel)

Nadat de hardware informatie verzameld is en doorgegeven aan Ntldr, verschijnt de volgende mededeling:

```
OS Loader V4.01
Press SPACEBAR now to invole Hardware Profile/Last Known Good menu.
```

De boot loader wacht een paar seconden zodat er de kans is om op de spatiebalk te drukken. Indien dit niet gebeurt en er is maar één hardware profiel dan wordt NT met de default control set geladen. Meerdere hardware profielen kunnen vooral bij laptops handig zijn (wel / geen dockingstation).

Het Last Known Good Menu is nodig indien er problemen waren bij het starten van Windows NT. De informatie die dan gebruikt wordt is de informatie die bewaard is bij het laatste succesvol inloggen van een gebruiker.

Het laden van de Kernel

Na het selecteren van de gewenste hardware configuratie, of default indien er geen actie ondernomen is, wordt door de boot loader de Windows NT kernel (Ntoskernl.exe) en de Hardware Abstractie Laag (Hall.dll) geladen. Het aparte is dat deze code nog niet geactiveerd wordt. Eerst wordt de registry key **HKEY_LOCAL_MACHINE\SYSTEM** uit de directory %systemroot%
System32\Config het bestand System geladen.

Op dit punt in het boot proces wordt de control set aangemaakt waarmee de computer geïnitialiseerd gaat worden. De waarde in de subkey
HKEY_LOCAL_MACHINE\SYSTEM\Select bepaalt welke control set er gebruikt moet worden. Standaard gebruikt de Loader de control set die door de **Default** value wordt aangeduid, behalve indien er voor de Last Known Good configuratie gekozen is. In dit

geval wordt de waarde die bij LastKnownGood staat gebruikt om te bepalen welke **ControlSet00x** er gebruikt moet worden. De waarde van **Current** in de **Select** subkey wordt gewijzigd in het nummer van deze control set.
Hierna wordt van alle services die in de registry subkey **HKEY_LOCAL_MACHINE\SYSTEM\CurrentContolSet\Services** staan gekeken welke als **Start** waarde 0x0, wat wel laden maar niet initialiseren betekend, hebben. Dit zijn meestal low-level hardware drivers voor b.v. de harde schijf. De **Group** waarde van de driver bepaalt in welke volgorde de drivers geladen moeten worden. Dit staat in de registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder** aangegeven.

De Kernel fase

Op het moment dat de boot loader (Ntldr) de controle doorgeeft aan Ntoskrnl.exe start de kernel fase. Windows NT initialiseert zich in drie fases:

- Kernel initialisatie;
- Laden en initialiseren van de device drivers;
- Laden en initialiseren van de services;

Het geheel wordt hierna door de Logon fase gecomplementeerd.

Kernel initialisatie

De kernel wordt geïnitialiseerd als het scherm blauw wordt en een vergelijkbare tekst als hieronder verschijnt:

```
Microsoft (R) Windows NT (TM) Version 4.0 (Build 1381: Service Pack 5)
2 System Processors (256 MB Memory)
```

Deze melding geeft aan dat Ntoskrnl.exe succesvol geïnitialiseerd is en dat de controle door Ntldr is over gedragen. De kernel creëert de **HKEY_LOCAL_MACHINE\HARDWARE** key met de informatie die door de boot loader verzameld is. Deze key bevat dus hardware informatie die bij elke systeem start opnieuw bepaald wordt.

Hierna maakt de kernel een Clone control set aan door een copie te maken van de control set die als Current gemerkt is. De Clone set wordt nooit gewijzigd, omdat het de bedoeling is dat deze identiek blijft aan de informatie die gebruikt is om de computer te initialiseren. Wijzigingen tijdens het startup proces worden hierin dus niet doorgevoerd (wel in de Current!!).

Laden en initialiseren van de device drivers

De kernel initialiseert de drivers die tijdens het laden van de kernel wel geladen zijn, maar nog niet geïnitialiseerd. Indien er een fout optreedt wordt er actie ondernomen gebaseerd op de waarde onder **HKEY_LOCAL_MACHINE\SYSTEM\CurrentContolSet\Services*DriverNaam*\ErrorControl**.

Ntoskrnl scant de registry **tak HKEY_LOCAL_MACHINE\SYSTEM\CurrentContolSet\Services** voor device drivers die onder ***Driver*\Start** als waarde 0x1 hebben staan. Net zoals bij het laden van de kernel bepaalt ook hier de **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder** de laad volgorde. Deze drivers worden wel meteen geïnitialiseerd.

Laden en initialiseren van de services

De Session Manager (Smss.exe) start de z.g.n. hogere orde subsystemen en services voor Windows NT. Informatie voor de Session Manager is in de **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager** sub key terug te vinden. De Session Manager voert de volgende taken uit.

BootExecute data item

Het BootExecute data item bevat één of meerdere commando's die de Sesion Manager moet uitvoeren, voordat de services geladen kunnen worden. Standaard wordt altijd Autochk.exe uitgevoerd, dit is de NT-versie van Chkdsk.

```
BootExecute : REG_MULTI_SZ : autocheck autochk*
```

De Session Manager kan meer dan één programma uitvoeren. In het onderstaande voorbeeld wordt ook de Convert utility gestart om partitie x van FAT naar NTFS te converteren bij de volgende systeemstart:

```
BootExecute : REG_MULTI_SZ: autocheck autochk* autoconv \DosDevices\x:
/FS:ntfs
```

Nadat de Session Manager deze commando's heeft uitgevoerd wordt door de kernel (Ntoskrnl.exe) de ander registry keys geladen die in %systemroot%\System32\Config staan.

Memory Management key

Vervolgens wordt de "paging" informatie (swapfile informatie), nodig voor de Virtual Memory Manager, opgehaald. Deze informatie is in de volgende data-items aangegeven:

```
PagedPoolSize        : REG_DWORD 0
NonPagedPoolSize     : REG_DWORD 0
PagingFiles          : REG_MULTI_SZ : c:\pagefile.sys 0
```

DOS Devices key

Vervolgens worden de "symbolic links" aangemaakt. Deze links verwijzen bepaalde commando types naar het juiste component in het file systeem. De volgende default informatie is aanwezig:

```
PRN : REG_SZ : \DosDevices\LPT1
AUX : REG_SZ : \DosDevices\COM1
NUL : REG_SZ : \Device\Null
UNC : REG_SZ : \Device\Mup
PIPE : REG_SZ : \Device\NamedPipe
MAILSLOT : REG_SZ : \Device\MailSlot
```

Subsystems key

Vanwege de aard en gelaagde opbouw van de verschillende subsystemen moet eerst het Windows subsysteem (Win32) worden gestart. Dit subsysteem controleert alle I/O en toegang tot het video subsysteem, de procesnaam van dit subsysteem is Csrss.exe.. Het Windows subsysteem start het Winlogon proces, welke op zijn beurt weer ander subsystemen activeert.

De configuratie informatie voor de benodigde subsystemen is aangegeven met de **Requered** value in de **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems** subkey van de registry.

Nadat er geen problemen ontdekt zijn bij de controle van alle aanwezige harde schijven (zie BootExecute data item) worden de pagefiles geactiveerd zoals gedefinieert onder de subkey **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager\Memory Management**.

De volgende stap is het laden van de SOFTWARE tak van de registry in het geheugen door de Session Manager. Vervolgens worden de benodigde subsystemen geladen zoals aangegeven in de **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager\SubSystems\Required**. Standaard is alleen het Win32 subsysteem nodig.

Als laatste stap worden alle drivers geladen door de Session Manager die als Start waarde 0x2 in de registry hebben staan (deze zijn dus afhankelijk van de aanwezigheid van een subsysteem).

De Logon fase

Het Windows NT boot proces wordt pas als afgerond beschouwd op het moment dat een gebruiker succesvol ingelogd is. Ook deze actie is in drie stukken onder te verdelen

Begin van Logon

Zoals hiervoor reeds beschreven start het Windows subsysteem automatisch Winlogon.exe. Winlogon start op zijn beurt de Local Security Administration (Lsass.exe). Het resultaat hiervan is dat het **Begin Logon** dialoog venster wordt weergegeven. Op dit moment, ook al is Windows NT nog steeds bezig met het initialiseren van andere subsystemen, meestal netwerk drivers, kan de gebruiker reeds inloggen.

Service Controller

Vervolgens wordt de Services Controller (Screg.exe) gestart. Dit proces gaat nog een keer door de registry heen en controleert of alle services die automatisch moesten starten (Start waarde = 0x2) wel gestart zijn. Is dit niet het geval dan worden ze alsnog gestart in de volgorde van afhankelijk zoals aangegeven in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriverName**.

Clone Control Set

Nadat een gebruiker succesvol is ingelogd wordt de Clone control set gecopieerd naar de LastKnownGood control set. Dit is handig indien er een probleem ontstaan is door een wijziging in der registry, hetzij door software of hardware. Het is dan ook van belang om te wachten met het inloggen, indien er een nieuw stuk software of een nieuwe driver geïnstalleerd is en het systeem herstart wordt, tot dat het systeem helemaal tot rust is gekomen en er geen melding op het scherm is verschenen in de trend van "At least one driver failed at startup".

Opbouw en doel van het BOOT.INI bestand

De BOOT.INI wordt door de Boot Loader (Ntldr) gebruikt om te bepalen welke OS opties er worden weergegeven bij het starten van het systeem. BOOT.INI is een read-only bestand en hoeft standaard niet met de hand worden aangepast. Dit kan voor de belangrijkste opties namelijk via Control Panel -> System. Hieronder staat een voorbeeld van een BOOT.INI:

```
[boot loader]
timeout=30
default=scsi(0)disk(0)rdisk(0)partition(1)\winnt

[operating systems]
scsi(0)disk(0)rdisk(0)partition(1)\winnt = "Windows NT"
/NODEBUG
C:\ = "Microsoft Windows"
```

Hieronder volgt een regel-voor-regel verklaring van de bovenstaade BOOT.INI:

[boot loader]
timeout=30

Timeout bepaald de tijd die NT wacht voor door te gaan met het default OS.

default=scsi(0)disk(0)rdisk(0)partition(1)\winnt

Default bepaald het standaard OS dat na de timeout geladen wordt.

[operating systems]
scsi(0)disk(0)rdisk(0)partition(1)\winnt = "Windows NT"
/NODEBUG
C:\ = "Microsoft Windows"

Scsi(0):	De primaire controller, meestal ook de enige in het systeem, die verantwoordelijk is voor het device. Indien er twee controllers in het systeem zitten en de disk zit aan de tweede controller dan zou er scsi(1) staan.
Disk(0):	De fysieke eerste schijf
Rdisk(0):	De rdisk() parameter bepaalt welke SCSI logische unit (LUN) er gebruikt wordt. Dit kan een losse schijf zijn, maar bij de meeste systeemen is er maar één LUN per SCSI ID.
Partition(1):	Is de partitie waar het OS staat. Zijn er meerdere partities dan wordt er oplopend genummerd (C=1, D=2, E=3 enz)
\winnt:	Is de directory waar het te starten OS staat.

Switches:

/NODEBUG	Er is geen debug informatie nodig. Dit is namelijk alleen van belang bij ontwikkelen van software of bij troubleshooting.
/DEBUG	Er wordt dubug informatie bij gehouden. Dit vertraagd NT alleen wel in enige mate.
/SOS	Laat de stuurprogramma namen zijn die door het OS tijdens het starten geladen worden. Standaard zijn namelijk alleen die stippeltjes zichtbaar (progressie indicator).
/NOSERIALMICE	Voorkomt detectie van seriele muizen op alle com-poorten.
/NOSERIALMICE:COMx	Voorkomt detectie een seriele muis op Com x,
/NOSERIALMICE:COMx,y,z	Voorkomt detectie van seriele muizen op COM x, y en z.

C:\ = "Microsoft Windows"

Dit is het vorige OS en zal in dit geval Windows 3.1, 95 of 98 zijn.

Actieve processen onder Windows NT

Als Task Manager (rechtsklikken op de taakbalk -> Task Manager) gestart wordt is op de tab Processes te zien welke processen actief zijn op een Windows NT machine. De hier genoemde processen zijn de meest voorkomende en belangrijkste processen. Het is heel goed mogelijk dat er op het eigen systeem meer en andere processen actief zijn. (Klik op PID (ProcessID) om de processen op een oplopend PID te sorteren als dit nog niet het geval is.)

Proces	Omschrijving
System idle Process	Is een soort negatief belastingsindicator.
System	Is een bestand met configuratie instellingen en bevindt zich in %winnt_root%System32\Config en is een afspiegeling van de registry hive HKEY_LOCAL_MACHINE\System. Dit bestand wordt tijdens het starten van NT door de NT-bootcode in het geheugen gezet.
Smss.exe	Session Manager System Service. Deze controleert en activeert de verschillende subsystemen. Standaard wordt alleen het WIN32-subsysteem gestart. (zie ook hkey_local_machine\System\ CurrentControlSet\Control\Session Manager
Csrss.exe	Dit is WIN32 subsysteem. Deze initieert op zijn beurt weer o.a. het winlogon proces.
Winlogon.exe	Dit is het logon proces. Winlogon start op zijn beurt weer het Local Security Administration subsysteem.
Lsass.exe	Local Security Administration System Service. Deze verzorgt het inlogproces van de gebruiker. NT is op het moment van activering van dit proces, door winlogon, nog steeds bezig meet het laden en activeren van andere services, meestal de netwerk services.
Screg.exe	Deze controleert of Winlogon wel alle autoload services gestart heeft, is dit niet geval dan wordt het nog een keer geprobeert. Dit proces sluit zich zelf ook weer af.
Het systeem is nu in principe actief. De volgende processen zijn meer user georiënteerd.	
Spoolss.exe	Spooler Service (voor printen e.d.)
Locator.exe	Netwerk Locator Service
Rpcss.exe	Remote protocol Connection (wordt bij RPC gebruikt)
Nddagent.exe	Net DDE services (o.a. Hartenjagen)
Explorer.exe	Het bureaublad
Inetinfo.exe	Peer Web Services(NT Workstation) (iisserve.exe op NT Server)
Systray.exe	Systeemtray, onderdeel van taakbalk
Rasman.exe	De Remote Access Service, wordt gebruikt bij externe connecties naar andere netwerken, zoals het internet.
tapisrv.exe	De Telephone API Service, gaat hand in hand met Rasman
Ntvdm.exe & wowexec.exe	Deze twee zijn het resultaat van het draaien van een Windows 3.1 of een Dos-taak. Het is de NT Virtual Device Manager (creëert een virtuele computer en de Windows On Windows Executive (creëert de Win16 omgeving)
De volgende processen zijn vaak echte voorbeelden van geheugen vervuiling	
Loadwc.exe	Onderdeel van IE. Zorgt voor de melding dat de huidige browser niet meer de standaard browser is.
Fastfind.exe	Het indexeer programma van Microsoft Office. Zorgt ervoor dat het systeem bij tijd en wijlen extreem traag kan worden
Osa.exe	Het snelstart onderdeel van MS-Office. Deze laat alvast een aantal DLL's in het geheugen zodat de Office toepassingen een "flitsende start"hebben

Verwijderen van Windows NT

Windows NT kan verwijderd worden, zonder de harde schijf opnieuw te formatteren. Het is wel van belang dat de partitie maximaal 2 GB mag zijn en de partitie FAT geformatteerd is. Voer hiervoor de volgende stappen uit

- Maak een MS-DOS start diskette (format a: /s)

- Zet de volgende bestanden op de diskette:
  Sys.com
  Attrib.com
  Deltree.exe
  Scandisk.exe
  Defrag.exe

- Maak een batch file en noem deze Killnt.bat en zet er het volgende in:

```
@Echo Off
A:
SYS C:
DELTREE /Y C:\WINNT
DELTREE /Y C:\PROGRA~1
A:\ATTRIB -S -H -R C:\BOOT.INI
DEL C:\BOOT.INI
A:\ATTRIB -S -H -R C:\NTDETECT.COM
DEL C:\NTDETECT.COM
A:\ATTRIB -S -H -R C:\NTLDR.
DEL NTLDR.
A:\ATTRIB -S -H -R C:\BOOTSECT.DOS
DEL C:\BOOTSECT.DOS
DEL C:\FATBOOT.BIN
DEL C:\PAGEFILE.SYS
REM
REM Het is belangrijk om hierna de HD te controleren en
REM te defragmenteren!!!
REM
A:\SCANDISK C: /CUSTOM
A:\DEFRAG C: /F
```

Start de computer met de gemaakte diskette op en start killnt.bat. Na het uitvoeren van deze procedure is Windows NT complete verwijderd van het systeem zonder te hoeven formatteren.

Aanmaken van een Windows NT start diskette

Indien Windows NT geïnstalleerd is op een Intel-systeem en de boot record van de actieve partitie of de bestanden nodig voor het starten van Windows NT zijn corrupt, dan is het niet mogelijk om NT of enig ander OS op die PC te starten.

Dit is te voorkomen door een NT start diskette aan te maken. Omdat NT niet zoals Dos op één diskette past bevat een NT start diskette die bestanden die nodig zijn om het OS, door de eerste start fase te helpen. Voor de rest van het start proces worden de bestanden van de NT installatie op de HD gebruikt. Zo'n diskette wordt op de volgende manier gemaakt:

- ✓ Formateer een diskette onder NT, via de Explorer.
- ✓ Kopieer uit de root directory van de boot partitie van de HD de volgende bestanden:
  - ✗ Boot.ini;
  - ✗ Ntldr;
  - ✗ Bootsect.dos;
  - ✗ Ntdetect.com.

Dit zijn systeem bestanden en dus standaard niet zichtbaar in Explorer. Om deze wel zichtbaar te maken kies in Explorer View -> Options -> View-tab en klik "View all file-types" aan en "Hide extensions for know filetypes" uit.

- ✓ Indien NT op een SCSI drive geinstalleerd is kopieer dan ook Ntbootdd.sys naar de boot diskette

Indien een diskette onder Explorer geformateerd is, dan wijst de boot record standaard naar het Ntldr bestand. Indien Ntldr gestart wordt, dan worden de beschikbare OS'en geladen uit de Boot.ini. Indien er voor WinNt gekozen wordt dan start Ntldr Ntdetect.com en geeft daarna de controle door aan Osloader.exe. Indien de gebruiker voor een ander OS kiest dan start Ntldr de alternatieve bootsector (Bootsect.dos).

Plug and Play ISA Apparaten

Voordat Plug and Play ISA (PnP ISA) apparaten onder Windows NT gebruikt kunnen worden moet er een z.g.n. "enabler driver" geïnstalleerd worden. Deze zorgt dan voor de herkenning en configuratie van deze apparaten. Het betreffende stuurprogramma, PNPISA.SYS, is in de \Drvlib folder op de Windows NT CD te vinden.

Deze enabler bevat niet de complete Windows 95 Plug and Play support. Het is b.v. niet mogelijk om dynamisch resources toe te kennen aan PnP ISA apparaten. Het is wel mogelijk om via een user interface (UI) handmatig de systeem recources in te stellen op zo'n manier dat er geen conflicten ontstaan met ander apparaten in het systeem.

Installeren van PNPISA.SYS

1. Stop de Windows NT compact disk in de CD-ROM drive.
2. Ga naar de \DRVLIB\PNPISA\X86, voor Intel machines
3. Rechts klik op PNPISA.INF en kies Install.
4. Herstart na de installatie de computer, wordt om gevraagd.

Uitschakelen van PNPISA.SYS

1. Open Control Panel -> Devices.
2. Selecteer "PnP ISA Enabler Driver" en kies "Startup".
3. Klik op "Disabled" en daarna op OK.

Het installeren van PnP ISA apparaten

Als het systeem start met de enabler stuurprogramma (PNPISA.SYS) geïnstalleerd, dan zal de enabler die PnP ISA apparaten in de computer activeren (to enable) waarvoor resources (IRQ, DMA enz.) zijn ingesteld. Voor elk nieuw apparaat dat ontdekt wordt kunnen stuurprogramma's worden geïnstalleerd, zodra er met het administrator privilege wordt ingelogd. Bij het inloggen zal Windows NT een "New Hardware Found dialog box" presenteren voor elk nieuw apparaat die het vindt.

Opmerking: Sommige PnP ISA kaarten bevatten meerdere functies. In deze gevallen zal er voor elke functie op zo'n kaart een dialog box worden geopend.

Indien NT niet een stuurprogramma heeft die speciaal voor een apparaat is, dan wordt er een dialog box gepresenteerd die de volgende opties bevat:

Windows NT default driver:
Indien NT een stuurprogramma heeft dat compatibel is met het apparaat, dan is dit de default keuze. Indien je niet zelf een stuurprogramma hebt of de stuurprogramma niet helemaal vertrouwd, kies dan voor deze optie.

Driver from disk provided by hardware manufacturer:
Indien je een diskette hebt met een stuurprogramma voor het apparaat, kies dan deze optie. De diskette moet dan wel een stuurprogramma voor NT bevatten. Alleen Windows 95 zal niet werken.

Select from a list of alternate drivers:
Indien je geen stuurprogramma's hebt en NT heeft niet zelf een default stuurprogramma kunnen bepalen, dan kan met deze optie een keuze worden gemaakt uit alternatieve stuurprogramma's die NT ondersteund.

Do not install a driver (Windows NT will not prompt you again):
Kies deze optie alleen maar indien er geen stuurprogramma voor het apparaat is. Dit zorgt ervoor dat NT telkens het "New Hardware Found" dialog box presenteert bij het starten of inloggen op het systeem.

LET OP: Indien deze optie gekozen wordt is niet meer mogelijk het apparaat naderhand toch nog te installeren, behalve met de volgende procedure:

1. Shut down NT.
2. Verwijder de kaart uit de computer.
3. Start de computer. NT detecteert dat the kaart verwijdert is uit de machine en verwijdert de entry voor de kaart uit de Registry.
4. Shut down NT.
5. Stop de kaart er weer in.
6. Start de computer. Bij het inloggen wordt de "New Hardware Found" dialog box weergegeven voor het apparaat.

PnP ISA SCSI kaarten

Een Plug en Play SCSI adapter die tijdens geïnstalleerd is tijdens de Windows NT installatie zal opnieuw gedetecteerd worden nadat de Plug and Play ISA enabler geactiveerd is op het systeem. Als de "New Hardware Found" dialog box wordt weergegeven, wordt er gevraagd of het bestaande stuurprogramma behouden moet worden of dat een nieuw stuurprogramma moet worden geïnstalleerd. Kies voor "Yes" om het huidige stuurprogramma te behouden.

Alle Plug en Play ISA SCSI adapters moeten in de "Legacy mode" gezet worden. B.v. De Adaptec AHA152x ISA Plug en Play adapters kunnen op de volgende manier in Legacy mode gezet worden:

- Kies een resource instelling die nog niet gebruikt wordt d.m.v. de DIP switches op de adapter. Kies niet "inactive".
- Druk op Ctrl-A om de SCSI Setup Utility te starten nadat het logo verschijnt.
- Zet de PnP mode uit.

Maken van een DUN connectie

Met behulp van DUN/RAS is het relatief eenvoudig om een connectie te leggen met Compuserve (en iedere andere ISP). Om de stappen hieronder beschreven te kunnen voeren, moet wel de Windows NT Workstation CD-ROM beschikbaar zijn, of een alternatieve lokatie waar de bestanden staan.

Er wordt vanuit gegaan dat er geen netwerk componenten aanwezig zijn. Is dit toch het geval noteer de instellingen goed en lees het volgende stuk eerst goed door.

Het installeren van een modem.

Ga hiervoor naar Control Panel->Modem. Omdat we alleen maar een RAS-connectie gaan maken wordt het modem een soort netwerk adapter. Indien het modem type bekend is dan kan deze beter direct zelf gekozen worden. Is dit niet het geval, laat dan Windows NT eerst zelf naar het modem zoeken. Het is daarna altijd nog mogelijk om het merk c.q. type te veranderen als dit niet mocht kloppen.

Klik na de installatie van het modom op de knop Dailing Properties. Kies vervolgens als land voor Nederland en vul het correcte kengetal in.

Opmerking: In principe kan het modem ook pas bij installatie van de Ras Service geïnstalleerd worden.

Het installeren van de netwerk componenten.

Ga naar het netwerk control panel. Dit kan via Control Panel -> Networks of door rechts te klikken op Network Neighborhood. Ga verder met 1610 indien er nog geen netwerk componenten geïnstalleerd zijn en dus de Network Setup Wizard gestart wordt. Indien er wel reeds netwerkcomponten aanwezig zijn, ga dan verder met 1611.

Network Setup Wizard

Selecteer eerst de optie "Remote Access to the Network" en deselecteer vervolgens de optie "Wired to the Network". Er wordt dus vanuit gegaan dat er geen normale netwerkverbinding aanwezig is. Kies vervolgens géén netwerk adapter en klik dus niet op Start Search!

Zorg bij Network Protocols dat alleen TCP/IP Protocol aangevinkt is. Onder Network Services staat als het goed is ook de service "Remote Access Service". Is dit niet het geval, voeg deze dan alsnog toe.

Verander niet de volgorde van de services en ga door. Kies bij de vraag voor een Workgroup of een Domain, voor Workgroup. De naam is vrij (is namelijk niet van belang).

Geen Network Setup wizard

In dit geval zijn er dus reeds netwerk componenten aanwezig. Selecteer éérst de Protocols Tab en controleer of daar het TCP/IP protocol geïnstalleerd is. Voeg deze zo nodig toe via de Add... knop.

Selecteer vervolgens de Services Tab en controleer of daar de "Remote Access Service" geïnstalleerd is. Voeg ook deze zo nodig toe via de Add... knop.

Vragen tijdens de installatie van de componenten

TCP/IP Setup:
Op de vraag of DHCP gebruikt moet worden is het antwoord "Yes".

Remote Access Setup:
Kies hier het net geïnstalleerd modem of als er nog geen modem aanwezig is, dan wordt aangeboden er een te installeren.

Let op: Indien NT-Server gebruikt wordt **moet eerst** voor de Port Usage van "Receive calls only" in minimaal "Dail out only" of "Dailout and Receive calls" veranderd worden.

Klik hiervoor op de "Remote Access Service" en vervolgens op de Properties-knop. Selecteer vervolgens het gebruikte modem en klik hierna op de knop Configure...

Klik vervolgens op de knop Network en selecteer als protocol alleen TCP/IP bij de Dail-out Protocols.

Na de installatie / configuratie van RAS / TCP-IP

De installatie zal worden afgerond. Klik vervolgens op de Close knop. Er worden een aantal instellingen aangepast en vervolgens komt er een melding dat het systeem opnieuw gestart moet worden voordat de nieuwe instellingen gebruikt zullen worden.

Indien er nieuwe bestanden gekopieerd en geïnstalleerd zijn **en** de machine is voorzien van een Service Pack, dan mag er nog **niet** herstart worden. **Eerst** moet het gebruikte Service Pack opnieuw geïnstaleerd worden! Omdat er originele componenten van de CD of het netwerk gekopieerd zijn, is het risico aanwezig dat na een herstart het netwerk gedeelte niet meer werkt!

Is er **niks** van de originele CD of het netwerk gekopieert dan kan het systeem **wel** direct opnieuw gestart worden. Dit is dus het geval als alles al aanwezig was en er alleen instellingen veranderd zijn!

Aanmaken en activeren van een Dail-Up Connectie.

Kies Start->Programs->Accesories->Dial Up Netwerking (afgekort DUN). Als het de eerste entry in het telefoonboek is, wordt autmagisch de Wizard, die help bied bij het aanmaken van de nieuwe entry, gestart.

De volgende vragen worden door de Wizard gesteld:

- De naam voor deze nieuwe entry;
- Kruis "I am calling the Internet" en "The non-Windows NT server..." aan;
- Vul het inbelpuntnummer, xxx-7110510 of xxxx-711510 in.
  Het is mogelijk om d.m.v. de knop alternates meerdere inbelpuntnummers in te vullen. Deze worden dan roterend afgewerkt indien er sprake is van "in gesprek";
- Kies "Point-To-Point Protocol(PPP)" ;

- Kies voor "Automate with this script" en kies als script WINNT\SYSTEM32\RAS\CIS.SCP uit het lijstje;
  Klik vervolgens op de "Edit script..." knop.
  Zoek de regel op die hieronder vet gemarkeerd is:
  transmit "/go:pppconnect^M"
  Verander deze regel in:
  transmit "/noint/go:pppconnect^M"
  Bewaar het script en sluit Notepad;
- Accepteer voor het IP-adres, de DNS-server en de WINS-server de standaard instellingen. Deze mogen namelijk niet ingevuld worden. Deze worden door CIS automatisch, via het DHCP-protocol, toegekend;
- Klik finish en er is een nieuwe entry in het PhoneBook aangemaakt.

Indien een applicatie een netwerkverbinding probeert te maken dan zal NT automatisch proberen aan DUN-verbinding te maken. Mocht dit onverhoopt niet lukken, sleep dan de betreffende DUN connectie op het werkblad en start zelf een connectie.

Het beveiligen van Windows NT

Bij alle opties wordt er van uit gegaan dat er minimaal Service Pack 3 geïnstalleerd is.

Opmerking: Er is ook een speciale Security Configuration Manager beschikbaar die er een beetje als TweakUI uitziet en een aantal van de hier weergegeven opties ook kan activeren. Deze is op de homepage en het Forum beschikbaar.

Windows NT en het Internet

Checklist voor systemen met een directe Internet verbinding

Hieronder volgen een aantal zaken waarnaar gekeken moet worden om de grootste gaten in Windows NT voor aanvallen vanuit het Internet te dichten. Sommige opties komen nogal radicaal over maar zijn dat voor stand-alone machines vaak niet.

1. Indien mogelijk gebruik een nieuwe installatie en installeer alleen die opties die absoluut nodig zijn. Een optie is om een dualboot omgeving in te richten voor deze doeleinden.
2. Gebruik standaard altijd het NTFS bestandssysteem. Een bestaande FAT partitie kan met *convert.exe* geconverteerd worden naar NTFS.
3. Installeer de laatste Service Pack voor Windows NT. Met hot-fixes moet iets voorzichtiger om gesprongen worden, omdat deze niet zo grondig getest zijn als een SP. Installeer een hot-fix dan ook alleen als er sprake is van het betreffende probleem!
4. Beveilig de user accounts die op de machine zijn aangemaakt:
   a) Hernoem het Administrator account. Let er op dat het wachtwoord ingewikkeld genoeg is en altijd uit een veelvoud van 7 (zeven) tekens bestaat. Een wachtwoord van 8 tekens is namelijk minder veilig dan een van 7 tekens! Het hernoemen maakt het voor een hacker moeilijker om adminstrative rechten te krijgen.
   b) Creëer een nep Administrator account waar geen rechten aan vast zitten. Dus dit account mag in geen groep zitten. Zorg ook hier voor een niet te

gemakkelijk wachtwoord omdat anders voor de hacker snel duidelijk is dat het een nep-account is.

c) Beperk het aantal accounts die in de lokale Administrators groep zijn opgenomen. Hoe meer accounts hier in zitten, hoe meer potentiële gaten er aanwezig zijn.

d) Disable het Guest account. Het Guest account is standaard gedisabled op Windows NT Server. Bij Workstation echter is het Guest account standaard wel enabled! Geef het guest account als extra beveiliging ook nog een goed wachtwoord mee. Let er op dat de optie "User cannot change password" aan gevinkt is.

e) Wijzig de lokale account policy zo dat er minimaal wachtwoorden van 7 tekens gebruikt moeten worden (User Manager -> Policies -> Account)

f) Activeer account lockout voor alle lokale accounts. Let er op dat het Administrator account en afgeleiden hiervan nooit een lockout kunnen krijgen!

5. Beveilig de Security Account Database (SAM) Het SAM bestand bevat de gecodeerde kopieën van de gebruikers wachtwoorden. Indien het niet is afgeschermd zouden hackers deze kunnen benaderen en het mogelijk kraken. De enige manier om de SAM te beschermen is door gebruik te maken van de NTFS bestandspermissies. Dit is één van de redenen dat NTFS als bestandssysteem gebruikt moet worden in plaats van FAT/FAT32.
   a) De standaard kopie van de SAM is te beveiligen door bij de directory *Winnt\System32\config* de *Everyone* groep uit de lijst te verwijderen van gebruikers/groepen die toegang hebben tot deze directory. Voeg vervolgens de groepen toe die wel toegang moeten hebben tot deze directory en de bestanden die er in staan (meestal Users en Administrators).
   b) De backup van de SAM staat in de *Winnt\Repair* directory. Deze bestaat alleen indien er een Emergency Repair Disk is aangemaakt. Verwijder ook hier de *Everyone* groep uit het lijstje met gebruikers/groepen. De enige groep/gebruiker die toegang hoeft te hebben tot de directory en de bestanden is het *System* account en de *Administrators* groep.

6. Beveilig de Registry. Er zijn drie dingen nodig om dit voor elkaar te krijgen.
   a) Beperk de *Netwerk toegang* tot de Registry met de **Winreg** key (zie 1710).
   b) Beperk de *Anonieme toegang* tot de Registry door de **RestrictAnonymous** waarde onder de **LSA** key aan te maken (zie 1711).
   c) Wijzig de standaard bestandsassociatie voor de extensie .REG van *Merge* in *Edit*. Hiermee wordt voorkomen dat een malafide website ongemerkt nieuwe keys kan toevoegen. (Explorer -> View -> Options... -> Tabblad File Types)

7. Beperk de toegang tot de machine vanaf het netwerk c.q. het internet. Dit kan eenvoudig via de User Manager -> Policies -> User Rights. Beperk vervolgens de optie "Access this computer from the network" tot het absolute minimum noodzakelijk. Wat meestal betekend dat alleen *Administrators* dit recht hebben.

8. Indien de *messenger* en *alerter* services niet nodig zijn, wat in stand-alone situaties eigenlijk altijd het geval is, zet ze dan permanent uit. Dit gaat via het Control Panel -> Services item. Selecteer de betreffende service en klik op de Startup... knop en kies voor de optie *Disabled*. Bij de volgende systeem start worden ze niet meer geladen.

9. Indien DCOM niet gebruikt wordt, wat in stand-alone situaties eigenlijk altijd het geval is, zet het dan uit d.m.v. *dcomcnfg.exe*. Omdat DCOM het toestaat om COM objecten uit te voeren die op remote computers staan, kan eenhacker via deze route een aanval openen op het systeem!

10. Indien IIS (Server) of PWS (Workstation) actief is, zorg er dan voor dat het laatste Service Pack geïnstalleerd is.
11. Start de FTP **niet** indien deze niet gebruikt word. Is FTP wel nodig sta dan geen schrijfrechten toe. Indien schrijfrechten wel nodig zijn sta dan **NOOIT** schrijven én lezen toe voor dezelfde directory. Splits dit! Activeer ook **NOOIT** de schrijfrechten voor de FTPRoot directory (zie ook zzz).
12. Configureer de computer **NIET** voor autologon. Standaard is die niet actief en dat moet zo blijven. Het gebruikte wchtwoord wordt namelijk leesbaar op een vaste en bekende plaats in het register bewaard. Gebeurd dit wel dan hebben de andere inspanningen geen enkele zin!
13. Instaleer **NIET** de Simple TCP/IP services. Indien je niet weet dat of waarom je ze nodig hebt, dan heb je ze ook niet nodig! Het klinkt bot, maar het is nu eenmaal zo!
14. Disable de WINS client op de netwerk c.q. dailup adapter (Control Panel -> Network -> tabblad Bindings).

Beperken toegang voor Anonymous Logon Users

Beperken lookup voor accounts, groepen en shares

De volgende wijziging in de Registry staat alleen nog maar Authenticated Users toe om een lijst met accountnamen, groepen en/of een lijst met beschikbare shares op te vragen. Alle verbindingen die Anonymous zijn kunnen deze informatie niet meer via de standaard GUI tools als browsebare informatie opvragen.

1. Start de Registry Editor (het liefst Regedt32.exe!).
2. Ga naar de volgende key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
3. Kies vervolgens Edit -> Add Value en gebruik de volgende gegevens:
   Value Name : RestrictAnonymous
   Data Type : REG_DWORD
   Value : 1
4. Sluit de Registry Editor. De computer moet herstart worden om de wijziging te activeren.

Beperken Anonymous Remote Registry Access

Anonymous Users worden door de volgende wijziging ook de toegang tot de registry gewijgerd en kunnen zo doende dus ook geen registry data meer lezen en schrijven!

Start de Registry Editor. Dit moet Regedt32.exe zijn i.v.m. het wijzigen van de ACL's.

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: CurrentControlSet\SecurePipeServers
Key Name: winreg
Class: n.v.t.

Selecteer vervolgens de key *winreg* en kies Security -> Permisions. Verwijder vervolgens voor extra veiligheid de groep *Everyone* en vervang deze door de groep *Authenticated Users* met als Access *read*. Sluit vervolgens de Registry Editor. De computer moet herstart worden om de wijziging te activeren.

De ACL op deze key bepaalt dus welke groep/gebruiker wel of geen remote toegang tot de registry kan krijgen. In tegen stelling tot Workstation mogen bij alleen de Administrators remote de registry te benaderen. Met de *winreg\AllowedPaths* subkey

wordt bepaalt welke specifieke gedeelten van de registry door geauthenticeerde gebruikers, die niet expliciet opgenomen zijn in de ACL van de *winreg* key, benaderd mogen worden. Dit is o.a. voor printer gebruik, replicatie en andere systeemzaken,

De Authenticated Users groep

Een nieuwe standaard groep is geintroduceerd vanaf Service Pack 3 namelijk "Authenticated Users" De Authenticated Users groep is gelijkwaardig aan de "Everyone" met één belangrijk verschil. Anonymous logon users (en NULL session connections) zijn nooit lid van de Authenticated Users group!

Authenticated netwerk connecties van een willekeurig account uit het domain van de server of een trusted domain worden standaard geidentificeerd als een Authenticated User. De Authenticated Users groep is beschikbaar om rechten aan toe te kennen via elke ACL editor. Het Service Pack modificeert niet de bestaande ACL's opdat de Everyone groep vervangen wordt door de Authenticated Users groep.

Toegang via NetBios van het Internet

Voor Windows NT systemen die direct aan het Internet hangen en die NetBios actief hebben zijn er twee configuratie opties mogelijk:

- Gebruik een firewall en laat deze vervolgens voor de TCP en UDP protocollen alle in en uitgaande verkeer op de poorten 135, 137 en 138 blokkeren. Dit zorgt ervoor dat er geen NetBios communicatie met het Internet kan optreden.
- Wijzig de protocol bindingen tussen de TCP/IP, NetBIOS, Server en Workstation services via het Network Control Panel.

  Verwijder de bindings tussen NetBios en TCP/IP door op het Bindings tabblad de NetBios bindings met de TCP/IP stack uit te zetten. Hierdoor zijn de standaard file sharing services (die de Server en Workstation services gebruiken) niet meer via TCP/IP te benaderen en dus ook niet meer via het Internet. Indien er wel gedeelde bestanden c.q. shares bestaan, dan moet er gebruik gemaakt worden van een LAN-specifieke, niet routable protocol, zoals NetBEUI.

Naast NetBios is ook IIS/PWS een service maar goed naar gekeken moet worden, vanwege de vele problemen die hier ook kunnen ontstaan.

Uitschakelen bewaren DUN wachtwoord

Standaard is het mogelijk om de gebruikersnaam en het wachtwoord te bewaren d.m.v. het selectie vakje in het dial-up networking (DUN) venster. Dit is een potentieel gevaarlijke situatie, want onbevoegden kunnen nu eenvoudig inloggen onder de naam van de gebruiker. Met de volgende wijziging in de registry is deze optie uit te schakelen:

Hive: HKEY_LOCAL_MACHINE\SYSTEM\
Key: CurrentControlSet\Services\RasMan\Parameters
Naam: logging
Type: REG_DWORD
Waarde: 1

Na een herstart zal de checkbox niet meer laten zien in het DUN inbelvenstertje.

Beveiligen van de IIS/PWS FTP service

Één van de standaard Internet services die geïnstalleerd wordt als onderdeel van IIS/PWS is het File Transfer Protocol (FTP). Een veel voorkomend gebruik van FTP is

om via een anonymous logon toegang te verlenen tot algemene bestanden. Bij het configureren van de FTP server wordt aan de server een speciaal user account voor het anoniem inloggen en een standaard home directory aangemaakt. Het default anonymous user account voor FTP is GUEST. Dit moet dus worden gewijzigd en tevens moet er een wachtwoord aan worden toegekend. Daarnaast kan dit account het beste geen deel uitmaken van enige groep met privileges. D.w.z. het account zit alleen maar in de groep *Everyone*. Daarnaast mag dit account geen "Logon on Locally" rechten hebben D.w.z. met dit account kan dan niet interactief, achter de machine zelf, ingelogd worden. Hiermee worden "insider attacks" via dit account voorkomen.

Bij de instelling van de home directory parameter moet met het volgende rekening worden gehouden. De FTP server exporteert de volledige schijf partitie. D.w.z. als beheerder kan je niet aangeven welke directories via FTP te benaderen zijn, maar alleen maar welke partities! Het resultaat is dan ook dat een gebruiker die via FTP een verbinding maakt instaat is om directories te bereiken die "boven" de home directory liggen! Hierom is het aan te raden om voor FTP gebruik een speciale partitie aan te maken en deze aan het account en server toe te kennen.

Potentieel probleem met twee NIC's

Indien de machine twee netwerkkaarten bevat (router, bridge of firewall) dan is er een potentiële bug aanwezig in de instelling die door TCP/IP gebruikt wordt om de buffer grote te bepalen voor het doorgeven van de routed packets.

De standaard instelling voor deze buffer is 0xFFFFFFFF bytes (4 Gb!). Kortom in potentie kan al het geheugen gealloceerd worden. Gelukkig is het mogelijk om deze waarden in te stellen omdat ze in de TCP/IP registry key staan. De aangegeven waarden zijn afgeleid uit door Microsoft verstrekte gegevens.

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Naam: MaxForwardBufferMemory
Type: REG_DWORD
Waarde: 74240
Naam: MaxNumForwardPackets
Type: REG_DWORD
Waarde: 50

Beveiligingen van schijven

Standaard heeft elk programma onder NT toegang tot her CD-Rom en diskette station. Soms is dit alleen niet een gewenste situatie, zeker in een omgeving waar veel met vertrouwelijke stukken wordt gewerkt die op diskette bewaard worden. Vaak is het dan de bedoeling dat alleen die persoon die ingelogd is toegang heeft tot het CD-Rom / diskette station, zodat de betreffende gegevens echt veilig zijn.

In deze mode zijn de diskette stations en/of CD-Rom spelers toegewezen als onderdeel van het logon proces. Ze worden automatisch weer vrijgegeven als de persoon dus uitlogd. Hierom is het dus wel van belang dat diskettes c.q CD's verwijderd worden voordat de betreffende persoon uitlogt!

Opmerking: Ook voor een tape drive geldt dat alle gebruikers hiertoe gewoon toegang hebben. Een consequentie is dan ook dat elke gebruiker elke tape in de drive kan lezen en schrijven. Normaal gesproken is dit geen probleem, want er is maar één gebruiker tegelijkertijd interactief ingelogd. Echter onder bepaalde omstandigheden is het mogelijk

dat een programma door een gebruiker gestart door blijft lopen nadat de betreffende gebruiker is uitgelogd. Als vervolgens een andere gebruiker inlogt en deze stopt een tape in de tape drive, dan kan dit programma stiekem informatie van de tape lezen. Indien dit een mogelijk probleem kan zijn, is de beste optie om het systeem eerst even voor gerbuik te herstarten.

Diskette station toekennen tijdens Logon

Gebruik de Registry Editor om de volgende registry key aan te maken:

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\WindowsNT\CurrentVersion\Winlogon
Naam: AllocateFloppies
Type: REG_SZ
Waarde: 1

Indien de waarde niet aanwezig is of een andere waarde dan 1 heeft, dan zijn diskette stations door alle processen op het systeem te benaderen. De wijziging wordt pas actief bij de eerst volgende keer dat er wordt ingelogd.

CD-ROM's toekennen tijdens Logon

Gebruik de Registry Editor om de volgende registry key aan te maken:

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\WindowsNT\CurrentVersion\Winlogon
Naam: AllocateCDRoms
Type: REG_SZ
Waarde: 1

Indien de waarde niet aanwezig is of een andere waarde dan 1 heeft, dan zijn CD-Rom spelers door alle processen op het systeem te benaderen. De wijziging wordt pas actief bij de eerst volgende keer dat er wordt ingelogd.

Veilig bestanden delen

De standaard manier waarop Windows NT bestanden deelt is via de SMB gebaseerde server component en de redirector services. Ookal kunnen alleen administrators shares aanmaken, de standaard beveiliging die op een share staat is dat de Everyone groep full control toegang heeft. Deze permissies gelden standaard voor alle bestanden onder zo'n share, indien er FAT als bestandssysteem gebruikt wordt. Dit is dus ook het probleem van FAT. Shares aangemaakt op NTFS schijven dragen hun rechten over op de onderliggende directories en bestanden. Daarnaast is het ook mogelijk en zeker aan te raden om de juiste beveiligingsinstellingen via NTFS te regelen en niet via de shares. Bedenk dat de share informatie een onderdeel van de registry vormt, dit i.t.t. NTFS beveiligingsinstellingen. Is de registry dus niet goed beveiligd dan zit ook daar dus weer een potentioneel lek.

Met de introductie van Service Pack 3 zijn er een aantal uitbreidingen toegevoegd aan het SMB gebaseerde file sharing protocol. Dit zijn:

- Wederzijdse authenticicatie om "man in het midden" aanvallen te voorkomen
- Ondersteuning voor message authenticicatie om aanvallen via messages te voorkomen.

Deze uitbreidingen zijn d.m.v. message signing in de SMB pakketjes opgenomen en worden door zowel de server als de cliënt gecontroleerd. Standaard staan deze opties uit omdat het hierdoor onmogelijk wordt om het bepaalde systemen nog een verbinding te

leggen. Maak de volgende wijzigingen in de registy om deze opties te activeren. Wijzig de volgende registry key om zeker te zijn dat een SMB server alleen nog reageert op een cliënt met message signing:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\LanManServer\Parameters
Naam: RequireSecuritySignature
Type: REG_DWORD
Waarde: 1

Deze wijziging zorgt er dus voor dat de Server service alleen nog communiceert met die clienten die message sigining ondersteunen. Alle andere clienten kunnen dus geen verbinding meer leggen. Hieronder vallen ook Windows 3.1/9x clienten!

Omgekeerd kan ook de client kant zo ingesteld worden dat deze alleen nog maar communiceert met servers die message signing ondersteunen.

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\Rdr\Parameters
Naam: RequireSecuritySignature
Type: REG_DWORD
Waarde: 1

Bedenk wel dat het hierdoor niet meer mogelijk is om een verbinding te maken met een server die message signing niet ondersteund.

Vanaf Service Pack 3 is er ook een andere verbetering aan het SMB file sharing protocol aangebracht. Deze is standaard actief waardoor het niet mogelijk om een verbinding te maken met SMB servers (zoals Samba, VAX of LAN Manager voor UNIX) met een niet gecodeerd (leesbare tekst) wachtwoord. Is zo'n verbinding toch gewenst dan kan deze beveiliging met de volgende aanpassing weer uitgezet worden.

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\Rdr\Parameters
Naam: EnablePlainTextPassword
Type: REG_DWORD
Waarde: 1

Daarnaast is het ook mogelijk om de administratieve shares, de z.g.n.$ shares, te verwijderen. Dit kan eenvoudig op de volgende manier via het "net share" commando gedaan worden:

```
C:\> net share admin$ /d
```

Wissen van de Page File tijdens een shutdown

Het virtuele geheugen van Windows NT gebuikt een page file om geheugen pagina's uit het geheugen tijdelijk op te slaan zodat er ruimte beschikbaar komt voor andere processen. Zolang Windows NT draait is dit bestand exclusief geopend en door geen ander programma te benaderen, wat dus een goede beveiliging garandeert. Mocht het systeem echter multi-boot geconfigureerd zijn dan is, na een herstart in het andere OS, de pagefile niet meer gelocked en is het dus ook mogelijk in de inhoud er van te raadplegen. Vaak zijn het gegevens waar niks uit te halen is, maar ook gevoelige informatie kan in de page file staan. Om nu te zorgen dat deze gevoelige informatie en alle andere informatie die mogelijk in de page file kan staan gewist wordt tijdens een

normale shutdown moet de volgende key in de registry aangebracht worden:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\SessionManager\Memory Management
Naam: ClearPageFileAtShutdown
Type: REG_DWORD
Waarde: 1

Let op: Deze beveiliging functioneert alleen indien er een normale shutdown wordt uitgevoerd. Een harde reset van het systeem (aan/uit knop) heeft dus als effect dat de page file niet gewist word! Indien de page file ook tussen verschillende gebruikers door gewist moet worden, dan zal moeten worden gekozen voor de optie " Shutdown and restart" c.q. "Restart the computer?" en niet voor de optie "Close all programs and logon as a different user" c.q. "Log Off".

Het reanimeren van een defecte Windows NT installatie

De manier om de installatie weer draaiende te krijgen is het draaien van een Emergency Repair met een Emergency Repair Disk die ná de installatie van SP3 is aangemaakt. Het SP3 bevat een aangepaste versie van het Setup.log bestand die het mogelijk maakt om een Windows NT Server of Workstation installatie na een software fout te herstellen.

Standaard wordt er tijdens de installatie van Windows NT aangeboden om een Emergency Repair Disk (ERD) aan te maken. Maar deze initiële ERD bevat alleen die instellingen die tijdens de installatie gemaakt zijn. Het hebben van een van een up-to-date ERD is net zo belangrijk als het regelmatig maken van een back-up. Elke keer als er veranderingen in en aan het systeem plaatsvinden, zoals het installeren van nieuwe software of hardware, of het veranderen van kritieke instelling aan hard en software moet er eigenlijk de ERD moeten worden geupdated met de Rdisk utility die bij Windows NT geleverd wordt (en néé deze staat niet in het startmenu en zal dus zelf moeten worden toegevoegd.)

Indien er iets gebeurt met de harde schijf van het werkstation zodat de opstart bestanden of de NT Registry corrupt worden, dan kan de ERD gebruikt worden om het systeem weer te activeren. Hierdoor wordt het namelijk mogelijk om het systeem weer helemaal operationeel te krijgen door de laatste systeem back-up terug te zetten.

Het reanimatie proces

Volg de onderstaande stappen om de Windows NT boot sector informatie opnieuw aan te maken en de dual-fuctionaliteit te herstellen (indien aanwezig) gebruikmakend van de Emergency Repair Disk:

1. Start het systeem gebruikmakend van de Windows NT Setup Disk 1 en 2

Indien er sprake is van een systeem met Service Pack 3, lees dan eerst "Het Reanimatie proces en Service Pack 3"!!!

2. Druk in het eerste scherm op de R voor Repair.
3. Er worden nu vier selecties gepresenteerd en alle vier zijn standaard geselecteerd. Verplaats de selectie balk met de pijltjes toetsen over opties om deze te selecteren en gebruik de spatiebalk om opties aan of uit te zetten, zodat het gelijk is aan de

onderstaande instellingen.

```
[ ]  Inspect registry files
[ ]  Inspect startup environment
[ ]  Verify Windows NT system files
[X]  Inspect Boot Sector
```

4. Selecteer dus alleen de optie “Inspect Boot Sector”. Verplaats de selectiebalk naar de regel “To Continue” en druk op de ENTER toets.
5. Laat Windows NT zelf alle opslagmediums detecteren en specificeer, indien nodig, met S additionele drivers indien deze nodig zijn.
6. Stop de Emergency Repair Disk van de betreffende PC in de disk-drive wanneer er om gevraagd wordt. Wat ook kan is op ESC drukken om NT te laten zoeken naar reparatie informatie op de harde schijf, dit is af te raden.
7. Repair zal CHKDSK draaien, de boot sector controleren en deze zonodig opnieuw aanmaken, indien nodig.
8. Als alles is afgerond wordt er gevraagd de machine te herstarten.
9. Als de machine herstart zal het Windows NT Boot Loader scherm verschijnen en is het weer mogelijk om te kunnen kiezen uit de aanwezige bootopties.

Het reanimatie proces en Service Pack 3 of hoger

Er is een probleem bij het gebruik van de originele installatie CD-Rom van Windows NT 4.0 voor het herstellen van een Windows NT 4.0 computer waarop een Service Pack 3 geïnstalleerd is. Dit komt doordat er door SP3/4 veranderingen in de Registry Security Hive, de Samsrv.dll, Samlib.dll, en Winlogon.exe zijn aangebracht.

Het resultaat is dat de pre-SP3 versies van deze bestanden niet meer bij de Windows NT system security informatie kunnen. Worden er toch pre-SP3 versies van deze bestanden gebruikt dan resulteert dit in een stop scherm met de stop code 0xC00000DF. (D.w.z.: Het opgegeven domain bestaat niet) en is het systeem niet meer te benaderen (inloggen is onmogelijk!!)

De oplossing is om de geupdate versie van SETUPDD.SYS (deze zit bij SP2 en hoger) te kopiëren naar de Windows NT Setup Disk 2. Hierdoor wordt de vorige versie van Setupdd.sys vervangen door de nieuwe versie.

Indien er een volledige reparatie van Windows NT wordt uitgevoerd zal het systeem in een GEEN SERVICE PACK installatie worden hersteld. Indien er wel een Service Pack nodig is dan moet deze opnieuw worden uitgevoerd als de Emergency Repair is afgerond en het systeem opnieuw gestart is.

Een volledige reparatie moet alleen maar worden uitgevoerd indien het systeem helemaal niet meer wil starten. I.v.m. de gemodificeerde Security hives blijven de bestanden, Samlib.dll, samsrv.dll en winlogon.exe wel achter.

De reanimatie, fase 2

Indien de computer niet wil starten en de standaard reparatie optie, zoals hierboven beschreven, heeft ook niet geholpen. Of als er geen Emergency Repair diskette of een er is geen CD-ROM drive aanwezig is, dan is de enige oplossing een upgrade van Windows over Windows NT 4.0 met Service Pack 3 of hoger uit te voeren. Dit moet op de volgende manier gebeuren:

✓ Kopieer de i386 folder van de originele Windows NT 4.0 CD-ROM op de harde schijf van het systeem, indien deze FAT is. Bij NTFS zal er gebruik gemaakt moeten worden van een netwerk share om daar de folder in te kunnen kopiëren. Hernoem in deze folder de volgende bestanden en kopieer deze naar de locatie van de Service Pack 3 bestanden:

Samsrv.dl_	Samsrv.org	SP3+
Samlib.dl_	Samlib.org	SP3+
Winlogon.ex_	Winlogon.org	SP3+
Lassrv.dl_	Lassrv.org	SP4
Services.ex_	Services.org	SP4
Msv1_0.dll	Msv1_0.org	SP4

✓ Kies de correcte procedure gebaseerd op het bestandssysteem:

✗ Er is sprake van FAT en de i386 folder staat op de lokale harde schijf:
- Start de computer in MS-DOS mode (boot diskette)
- Start WINNT /B in de i386 folder.
- Kies de "Upgrade option" tijdens de setup.

✗ Indien de installatie folder op het net staat en er is sprake van FAT, dan moet of Windows geïnstalleerd worden met netwerk geactiveerd, of maak een installatie boot diskette aan via de Windows NT Server CD-ROM. Maak hierna een verbinding met de aangepast i386 folder, en start WINNT /B.

✗ Indien er sprake is van NTFS, dan moet er een parallelle installatie worden uitgevoerd in een nieuwe folder, waarna er vanuit deze parallelle installatie WINNT32 /B vanuit de aangepast i386 folder gestart moet worden.

De reanimatie, code Rood

Indien niks help, dan zit er niks anders op dan opzoek te gaan naar de back-up, die je natuurlijk hebt, van je data en de installatie diskettes en CD's van de programmatuur.

Verwijder NT zoals beschreven in "Verwijderen van Windows NT" op pagina 25 en voer een nieuwe installatie uit. Let er op minimaal de initiele ERD wordt aangemaakt.

Als alles geïnstalleerd is, d.w.z zonder een Service Pack en zonder IE 4, en het werkt ook allemaal, doe dan het volgende:

1. Start Rdisk (Run→ Rdisk);
2. Klik op "Update Repair Info" en kies voor Yes;
3. Als er gevraagd wordt of de ERD moet worden geupdated kies dan Yes en gebruik een NIEUWE diskette.

Installeer hierna SP3 en voer de bovenstaande stappen opnieuw uit.
Installeer hierna, indien gewenst IE4 en voer de bovenstaande stappen weer opnieuw uit.

Het resultaat is dus vier (4) ERD-diskettes. Een initiële, eentje met alle software, maar pre-service pack, eentje met SP3 en eentje met IE4. Indien er bij een probleem een ERD nodig is gebruik je altijd de laatste. Die "oudere" zijn om bij problemen, van lastige (lees IE4) software of te kunnen komen.

De reanimatie en Service Pack 4 en 5

Hetzelfde wat voor Service Pack 3 geldt, geldt ook voor Service Pack 4. Opnieuw zijn de bestanden Samsrv.dll, Samlib.dll, Winlogon.exe en de Registry Security Hive,

aangepast. Daarom moet ook nu weer enige voorwerk verricht worden voordat er een herstel proces kan worden uitgevoerd, dit om het leven eenvoudig te houden.

Kopieer de SP4 c.q. SP5 versie van SETUPDD.SYS naar de Windows NT Setup Disk 2. Hierdoor wordt de vorige versie van Setupdd.sys vervangen door de nieuwste versie.

Indien er een volledige reparatie van Windows NT wordt uitgevoerd zal het systeem in een GEEN SERVICE PACK installatie worden hersteld. Indien er wel een Service Pack nodig is dan moet deze opnieuw worden uitgevoerd als de Emergency Repair is afgerond en het systeem opnieuw gestart is.

Een volledige reparatie moet alleen maar worden uitgevoerd indien het systeem helemaal niet meer wil starten. I.v.m. de gemodificeerde Security hives blijven de bestanden, Samlib.dll, samsrv.dll en winlogon.exe wel achter.

De-installeren van Service Pack 4 of 5

Begin hier domweg **niet** aan. Het aantal problemen dat dit veroorzaakt is groter dan de problemen die SP4 of 5 zou kunnen veroorzaken. De beste oplossing is om de backup terug te zetten en de gemaakt wijzigingen sinds het gebruik van SP4 opnieuw door te voeren.

Wandelende schijfletters

Indien de computer voorzien is van verwisselbare media zoals een ZIP-drive of van PC-Card sloten die Type III kaarten accepteren, zoals PC-Card harde schijven, dan kan het volgende probleem optreden:

Bij het aanwezig zijn van een ZIP-diskette en/of een PC-Card harddisk zal de interne harde schijf niet langer als de C-schijf worden aangeduid. In plaats daarvan zal de ZIP-drive of de PC-Card drive deze schijfletter krijgen. Het resultaat is dan ook dat de meeste applicaties niet goed meer werken of helemaal niet meer werken.

Met ingang van Service Pack 5 is het namelijk ook mogelijk om voor verwisselbare media zoals een ZIP-drive een willekeurige vrije schijfletter te kiezen! Dit is dus een reden te meer om direct voor SP5 te kiezen, zeker bij een nieuwe installatie. Voer ook met SP5 de handelingen onder **Hoe te voorkomen** uit, dit voorkomt dat er problemen ontstaan.

Hoe te voorkomen

Let op!
Voor alle volgende handelingen is een account nodig die in de Adminstrators groep van de machine zit

De oplossing zit hem in het expliciet toekennen een schijfletter aan alle aanwezige volumes op het systeem. Om de problemen voor te zijn moet dit direct nadat de installatie afgerond is gedaan worden. Open hiervoor Disk Administrator (staat in Administrative Tools van het start menu) en laat deze de schijven markeren, dit kan geen kwaad.

Ga vervolgens alle aanwezig volumes af en kies via een rechtsklik voor de optie “Assign drive letter...” en klik vervolgens op OK om de huidige keuze vast te leggen indien deze correct is. Geef dan tevens de eventueel CD-Rom de hoogst mogelijke schijfletter, het

liefst Z! Voor verwisselbare media is het helaas onmogelijk om een schijfletter op te geven (wat ook de veroorzaker van de vele probelemen is!).

Bewaar als laatste stap via Disk Administrator de Schijf configuratie op een diskette. Hiermee is het namelijk mogelijk om deze terug te halen indien er desondanks toch iets mee misgaat. (Partition -> Configuration... -> Save)

Hoe op te lossen

Voor mensen die SP5 geïnstalleerd hebben is de oplossing heel simpel. Zij kiezen gewoon een nieuwe schijf letter voor de ZIP-drive en na een systeem start is alles in principe weer oké.

Let op!
De volgende handelingen moeten alleen gebeuren indien de machine voor zien is van Service Pack 4 of lager!

Als het reeds te laat is en er is geen goede Schijf configuratie op diskette beschikbaar, dan kan de volgorde nog op de volgende manier hersteld worden:

1) Zet de computer aan, start Windows NT in Safe mode (op deze manier zijn de minste services actief), en log on als een administrator. Configureer de CD-ROM drive, gebruikmakende van Disk Administrator, op een hoge schijf letter zoals Z.

2) Om zoveel mogelijk volumes vrij te maken en dus hierdoor eenvoudig van schijf letter te kunnen veranderen moeten alle onnodige toepassingen worden afgesloten en alle onnodige services worden gestopt en tijdelijk helemaal uitgeschakeld te worden, dit gaat via Control Panel -> Services.

   De volumes die de Windows NT directory en de page file bevatten zijn niet vrij te maken. Probeer daarom in ieder geval de page file op dezelfde volume als de Windows NT directory te hebben staan, zodat maar één volume gelocked blijft. Indien de computer genoeg geheugen bevat, minimaal 48 Mb!, dan kan de page file zelfs tijdelijke helemaal verwijderd worden

3) Herstart de computer, dit vanwege alle wijzigingen in de services en mogelijk ook de page file door te voeren en dus zoveel mogelijk volumes vrij te hebben. Zorg er ook nu weer voor dat Windows NT in de safe mode start.

4) Start de Disk Administrator wijzig alle schijf letters in een zo hoge letter, b.v. F naar Y, E naar X enz. Voor elke volume die gewijzigd moet worden en die toch nog gelocked is moet een herstart worden uitgevoerd om de wijziging effectief te maken. Dit kan dus een paar keer nodig zijn (denk om de safe mode!)

5) Sluit Windows NT af en zet de computer uit en verwijder de PC-Card hard disk of de koppel de interne ZIP-drive los.Wat ook kan in het geval van een ZIP-drive is het draaien van SP3. Door een bug wordt de ZIP-drive bij de volgende systeem start als een super diskette en niet als een verwisselbare drive gezien.

6) Als het goed is, zijn nu de lage schijfletters (C,D enz) vrij. Geef eerst alle andere volumes de juiste schijfletter en geef als allerlaatste de systeem partitie zij schijfletter, welke meestal C is. Dit zal tot een aantal meldingen over mogelijk problemen leiden. Zorg er desondanks voor dat de toekenning plaats vindt en wacht

geduldig af. Dit duurt namelijk even.

7) Kies vervolgens in Disk Manager voor Partitions -> Commit changes now… en laat de machine opnieuw starten. Denk erom dat het nog steeds in de veilige mode moet, vanwege de pagefile die nu fout staat of niet aanwezig is! Als blijkt dat alle schijfletters weer naar juiste volumes wijzen, kan dus de ook de page file correct ingesteld worden.

   a) Indien de ZIP-drive via SP3 tot een B-schijf is gedegradeerd, laat de machine dan niet direct opnieuw starten na het wijzigen van de page file, maar gebruik eerst even de Post-SP3 fix voor de ZIP-drive om deze weer goed te krijgen. Het systeem zal namelijk na deze fix zeker opnieuw op moeten starten.

   b) Indien de ZIP-drive fysiek is losgemaakt, sluit dan Windows NT af en zet de computer uit. Sluit vervolgens de ZIP-drive weer aan of plaats de PC-Card harde schijf (NT ondersteunt geen Plug and Play voor PC-Card apparaten).

8) Start Windows NT, dit hoeft niet meer in safe mode, en log on als een administrator. De PC-Card drive c.q. ZIP-drive zou nu de eerste vrije schijfletter toegewezen moeten krijgen. Bewaar de huidige Disk Manager configuratie op een diskette en voer RDISK uit om de ERD-diskette te vernieuwen.

Bijlage I: Utilities

Defragmentatie

Onder Windows NT 4.0 is standaard geen programma beschikbaar waarmee eenvoudig een harde schijf is te defragmenteren. Volgens Microsoft was dit ook niet nodig, omdat een harde schijf onder NTFS niet of nauwelijks fragmenteerde. De werkelijkheid is dat NT-machines onbruikbaar worden c.q. onwerkbaar bij een te hoge mate van fragmentatie. De volgende programma's kunnen goed de harde schijf defragmenteren.

Diskeeper 5.0

Diskeeper van ExecSoft (www.execsoft.com) is een van de meeste gebruikte defragmenteerders voor Windows NT. Er zijn twee uitvoeringen beschikbaar:

- Diskeeper Lite;
- Diskeeper 5.0.

Diskeeper Lite is gratis te downloaden van ExecSoft's website en van het Forum. Deze uitvoering van Diskeeper is alleen geschikt voor thuisgebruik onder NT Workstation of NT Server.

Diskeeper, daarentegen, kan als een service draaien. Hierdoor is het mogelijk om de machine, alleen indien de belasting het toelaat, continue te defragmenteren. In tegenstelling tot de Lite versie kan Diskeeper wel gescheduled worden. Tevens is het mogelijk om andere NT-machines op afstand te defragmenteren.

Microsoft heeft bekend gemaakt dat in Windows 2000 Diskeeper Lite standaard als defragmentatie utility wordt meegeleverd.

Norton Utilities voor Windows NT 2.0

Dit is de andere gereedschapskist onder NT. Naast Speedisk heeft Norton tevens de mogelijk om bestanden op NTFS-partities te kunnen terug halen (de Unerase optie). Bedenk wel dat vooral het gebruik van System Doctor en Unerase een onaanvaardbare hoge belasting van het systeem tot gevolg heeft.

Let op!
De gedeeltelijke uninstall optie van Norton werkt niet! Het is dus onmogelijk om een reeds geïnstalleerde applicatie te verwijderen. De enige oplossing is om alle utilities te verwijderen en daarna de gewenste onderdelen te installeren.

Mijenix Fix-It 99

Deze gereedschapskist werkt onder zowel Windows NT als Windows 9x. Alle belangrijke opties zijn ook hierin aanwezig, waaronder een goede defragger, maar ook o.a. een afgeslankte versie van TweakUI, een Registry scanner en reparatie optie, een Rescue optie, een mogelijkheid om een Windows NT bootprompt te hebben en een virusscanner.

TweakUI 1.1 / 98

Eén van de belangrijkste utilities voor Windows NT is TweakUI. Hiermee is het mogelijk om de meeste wijzigingen in het uiterlijk en gedragingen van NT te veranderen, zonder dat er zelf in de Registry gegraven hoeft te worden. Dit voorkomt, dat door fouten, het systeem instabiel of totaal onbruikbaar wordt.

In principe zijn er drie versies van TweakUI beschikbaar, namelijk de 1.1 versie, de Windows 98 en een speciale NT versie. De Windows 98 en NT versies werken alleen maar indien er minimaal IE4 geïnstalleerd is. Aangezien dit toch een vereiste is om NT4 millennium bestendig te maken zal dat geen problemen geven en kan ook het beste, na de installatie van IE4 of hoger, voor de NT-versie gekozen worden.

Hieronder worden een aantal handige dingen van TweakUI er uit gelicht. In de help van TweakUI kan ook veel over de verschillende functie teruggevonden worden. De help kan op de Mouse-tabblad worden opgeroepen door op **Tips** te klikken of via het Snelhelp knopje in de vensterbalk. Let er alleen op dat soms de foute toelichting bij een optie wordt weergegeven! Houdt er rekening mee dat voor de meeste opties je Administrator rechten moet hebben.

Opmerking: Er is ook een speciale Security Configuration Manager beschikbaar die er een beetje als TweakUI uitziet. Deze is op de homepage en het Forum beschikbaar.

Tabblad General

Op dit tabblad onder anderen de **Effecten** van Windows 98 naar eigen wens ingesteld worden. Doordat zo'n beetje alles geanimeerd is, is dit een stevige aanslag op de rekenkracht van de machine. Zelf zet ik alles uit, op de volgende drie items na:

Beep on errors	Dit lijkt me wel duidelijk
Menu underlines	Laat het streepje onder sneltoets combinaties zien
Mouse hottracking effect	Laat de tooltips verschijnen!

Vooral de laatste optie moet niet uitgeschakeld worden. Veel programma's geven handige informatie via de ToolTips. Dit is vaak ook wel nodig gezien de vaak wat cryptisch aandoende icoontjes in de werkbalken!

Van het item **Special Folders**, mag eigenlijk alleen maar de locatie van de **My Documents** folder aangepast worden. De andere locaties kunnen het beste met rust worden gelaten omdat er nog veel programma's zijn die er domweg vanuit gaan dat de betreffende folders zich op de standaard locatie bevinden.

Tabblad Explorer

In de **Startup** sectie kan de "Tip van de dag" weer geactiveerd worden, indien deze is uitgezet. Uitzetten kan zowel in het "Tips van de dag" venster als in TweakUI.

In de **Settings** sectie kan het beste de optie “Prefix 'Shortcut to' on new shortcuts” optie worden uitgezet. Hierdoor wordt er door Windows 98 niet meer standaard de tekst “Snelkoppeling naar / Shortcut to” voor een nieuwe snelkoppeling neergezet.

Tabblad Desktop

Door middel van de kruis-vakjes is te bepalen welke iconen wel of niet op de desktop zichtbaar zijn. Dit is vooral handig voor al die programma’s die zichzelf zo belangrijk vinden dat ze op de desktop thuis horen.

Dit is een systeem wijde optie. Iedereen zal dus een icoon zien of niet meer zien! De enige uitzondering is de Network Neighborhood, deze is wel per gebruiker. Het verwijderen van de desktop icon verwijdert alleen maar het icon. De software die er bij hoort blijft gewoon geïnstalleerd. Indien the Network Neighborhood wordt verwijdert dan moet eerst worden uit- en ingelogd om de verandering door te voeren.

Consequenties van het verbergen van de Network Neighborhood
Omdat de ondersteuning voor de Universal Naming Convention (UNC) notatie door de Network Neighborhood wordt gedaan zorgt het verbergen ervan ervoor dat Explorer niet meer bij resources kan komen die een UNC gebruiken. Alleen door het mappen (koppelen) van een drive letter zijn netwerk resources vanuit Explorer te benaderen.

Opmerking
De Command prompt en andere programma’s worden hierdoor niet beïnvloed. Dit omdat zij geen gebruik maken van de Network Neighborhood om de UNC-namen te bepalen.

Tabblad IE4

Deze is alleen aanwezig indien de Active Desktop geïnstalleerd is. De Active Desktop is via deze optie ook weer uit te zetten, maar dan zal het tabblad niet verdwijnen! Hier kunnen de gedraging van IE4/5 worden aangepast. Omdat ikzelf niet zo’n voorstander ben van de Active Desktop (is nogal geheugen en processor intensief) en ook geen gebruik maak van de Documenten en Favorieten items op het Start-menu, vink ik nogal wat items uit. De enige drie items die ik **aangevinkt** heb staan zijn:

Allow Logoff	Dit omdat er soms moet worden uit- en ingelogd om instellingen te kunnen activeren.
Detect Accidential Double-clicks	Omdat IE4 aanstaat en ik de “enkel klik” geactiveerd heb, is dit een onmisbare optie (hoe enkel klik te activeren is, wordt verderop uitgelegd)
IE4 Enabled	Dit **uitvinken** heeft als effect dat W98 er ongeveer als W95 gaat uitziet en zich ook zo gaat gedragen.

Tabblad Paranoia

Hier is in te stellen welke historie lijsten standaard gewist moeten worden. In principe kan alles aangevinkt worden, behalve het item “Clear Last User Logon”. Indien deze wel aangevinkt is wordt standaard “vergeten” wie als laatste ingelogd was. Dit is vooral lastig indien altijd dezelfde persoon met de computer werkt en/of als de computer niet in een netwerk staat.

Tevens kan hier het wel of niet uitvoeren van de “Autoplay” optie voor zowel audio als data-cd’s worden gecontroleerd.

Bijlage II: Bug fixes en Service Releases

Een van de belangrijke aspecten van Windows NT zijn de Service Packs. Door middel van de SP's zorgt Microsoft voor de volgende zaken:

- Bug-fixes;
- Up-to-date houden van het OS door introductie van nieuwe features;

Service Packs zijn niet incrementeel. Het is dus niet nodig om eerst SP1 en SP2 toe te passen voordat SP3 gebruikt kan worden. Elk SP bevat alle wijzigingen van de voorgaande SP's. Het voordeel is eenvoudige installatie van het SP. Nadeel is dat ze steeds groter worden, naarmate het SP-nummer stijgt.

Wat vooral opvalt bij NT 4 is de snelheid waarmee de eerste twee SP's na de initiële release van NT werden uitgebracht.

Datum	Produkt
Okt 1996	Release Windows NT 4
Nov 1996	Service Pack 1
Dec 1996!	Service Pack 2
Mei 1997	Service Pack 3
Okt 1997	Internet Explorer 4.0
Sep 1998	Service Pack 4
Mrt 1999	Internet Explorer 5.0
Mei 1999	Service Pack 5
Nov 1999	Service Pack 6
Nov 1999	Internet Explorer 5.01
Dec 1999 / Jan 2000	Internet Explorer 5.5 Beta

Service packs zijn op de volgende locatie terug te vinden:

```
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/
```

Opmerking: Installeer geen Service Pack indien er geen problemen zijn met NT en er geen software gebruikt wordt die een bepaalde SP nodig heeft.

Service Pack 1

Repareert de initiële release bugs in NT 4. Is geïntegreerd in de huidige installatiesets.

Service Pack 2

Repareert een hele bak bugs en voegt een aantal componenten toe aan NT. Helaas introduceerde deze SP veel meer bugs dan dat ze repareerde. Dat gaf zo veel probelemen dat de hele NT-gemeenschap Microsoft bijna ophing. Sommige bugs kunnen een NT-machine totaal onbruikbaar maken.

Service Pack 3

Ondanks dat dit SP een bèta test ondergaan heeft zijn er momenteel reeds een aanzienlijk aantal SP3-hot-fixes uitgebracht. De meeste hebben betrekking op het

dichten van beveiligingsfouten in de netwerk en Internet componenten. Desondanks is SP3 een goed service pack voor de meeste gebruikers.

Internet Explorer 4.0

Internet Explorer 4.0 is niet een echte service pack speciaal voor Windows NT, toch worden er een aantal zaken ingrijpend gewijzigd. Dit geldt vooral bij het kiezen voor de Desktop Update. Let er op dat voordat IE4 geïnstalleerd wordt, er eerst SP3 geïnstalleerd moet zijn. Dit moet ook gebeuren als na het installeren van SP3 nog software geïnstalleerd is!

Service Pack 4

Na bijna anderhalf jaar is dan eindelijk Service Pack 4 verschenen. Dit was zo langzamerhand ook wel nodig omdat er ondertussen zoveel Post-SP3-fixes beschikbaar waren dat het én alleen al een studie op zich was om deze correct te installeren én er Post-SP3-fixes waren die andere Post-SP3-fixes weer repareerde.

SP4 repareert 642 bugs die als zodanig bekend staan in de Knowledge Base en tevens zorgt SP4 voor de nodige aanpassing opdat NT Y2K compliant is.

Internet Explorer 5.0

Internet Explorer 5.0 is niet echt een service pack is, maar toch worden er weer een aantal zaken gewijzigd. IE5 werkt met minimaal SP3, maar kies minimaal voor SP5 omdat hiermee tevens de meeste beveiligingslekken gedicht worden. Let er alleen wel op dat er na het installeren van het SP telkens ook opnieuw IE “gerepareerd” moet worden (i.v.m. registry wijzigigen). Dit kan eenvoudig via Control Panel -> Add/Remove Software.

Service Pack 5

Service Pack 5 bevat een 150-tal verbeteringen en aanvullingen t.o.v. SP4, vooral op Jaar 2000, beveiligings- en crashbestendigheidsvlak. Het is echter niet een "verplicht" Service Pack. Desondanks is het aan te raden om SP5 en niet SP4 te installeren als de keuze daar is. Het voorkomt toch weer het na installeren van een aantal hot fixes.

Service Pack 6a

Service Pack 6 is beschikbaar. De eerste versie bevatte echter een ernstige bug in de TCP/IP implementatie. Let er daarom op dat SP6a gebruikt wordt. Deze is dus de verbeterde versie van SP6.

Internet Explorer 5.01

Ondanks het onoogelijke verschil in de versie nummers lost deze versie veel problemen op die er zijn met de basis versie. Zo worden de nodige beveiligingsgaten gedicht (en blijven er nog de nodige open). IE501 werkt met minimaal SP3, maar kies liever voor SP6 omdat hiermee het systeem echt helemaal up-to-date is. Let er alleen wel op dat er na het installeren van het SP telkens ook opnieuw IE “gerepareerd” moet worden (i.v.m. registry wijzigigen). Dit kan eenvoudig via Control Panel -> Add/Remove Software.

Internet Explorer 5.5 Beta

IE5 (en 5.01) bevatten zoveel gaten dat MS vervroegt met IE5.5 naar buiten gaat komen. Deze update zal zich dan ook primair richten op het stabiliseren van het platform en het verder uitvijlen van de performance van het geheel.

Bijlage III: Registry aanpassingen

Hieronder volgen een aantal kant en klaar registry bestanden. Selecteer daarvoor de informatie tussen Selecteer daarvoor de informatie die tussen "- 8< -" staat. Deze kan dan vervolgens in Notepad geplakt worden en opgeslagen met als extensie .REG

Let er wel op dat NotePad altijd standaard .TXT achter een bestand plakt, ook al wordt zelf een andere extensie opgegeven. De oplossing hiervoor is het plaatsen van quotes om de naam van het bestand.

Elke Verkenner in een eigen proces

Zorgt ervoor dat bij een crash van een verkenner venster niet alle verkenners inclusief de desktop afgesloten worden.

```
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]
"DesktopProcess"=dword:00000001
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
```

Elke Internet Explorer in een eigen proces

Zorgt ervoor dat bij een crash van een Internet Explorer venster venster niet alle IE vensters afgesloten worden.

```
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BrowseNewProcess]
"BrowseNewProcess"="yes"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BrowseNewProcess]
"BrowseNewProcess"="YES"

- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
```

Voorkom het bewaren van het DUN wachtwoord

```
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters]
"Logging"=dword:00000001
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
```

Elk Win31 / Dos programma standaard een eigen VDM

```
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW]
"DefaultSeparateVDM"="yes"
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
```

Activeren van de Prompt Autocomplete functie

```
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Command Processor]
"EnableExtensions"=dword:00000001
"CompletionChar"=dword:00000009

- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
```

Deactiveren van het gebruik van de autoexec.bat

```
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]
"ParseAutoexec"="0"
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
```

Activeren van de snelle herstart optie

Te activeren via SHIFT+CTRL+ALT+DEL

```
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"EnableQuickReboot"="1"
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
```

Soft powerdown

Installeer SP4 of hoger en haal uit het SP het bestand **hal.dll.softex** en kopieer deze naar een tijdelijk locatie en hernoem deze vervolgens in **hal.dll**. Kopieer deze vervolgens naar de WINNT\SYSTEM32 directory, waar de originele hal.dll staat. Zorg dat APM wel actief is in het BIOS maar dat verder alle andere APM-timers gedeactiveerd zijn.

```
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"ShutdownWithoutLogon"="1"

[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Shutdown]
"Shutdown Setting"=dword:00000003
"Logoff Setting"=dword:00000000
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
```

Openen met Notepad indien ongeregistreerd bestand

Deze wijziging doet meer dan één ding. Standaard zal nu altijd de extensie van een bestand weergegeven worden. Verder zal bij elk onbekend bestand de optie "NotePad" beschikbaar zijn in het context menu (rechtsklikken) en indien voor de optie "Openen met..." gekozen wordt, dan zal daar standaard geen vinkje meer staan in het aanwezige selectie vakje.

```
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
REGEDIT4

[HKEY_CLASSES_ROOT\Unknown]
"AlwaysShowExt"=""

[HKEY_CLASSES_ROOT\Unknown\shell]

[HKEY_CLASSES_ROOT\Unknown\shell\Notepad]

[HKEY_CLASSES_ROOT\Unknown\shell\Notepad\Command]
@="notepad \"%1\""

[HKEY_CLASSES_ROOT\Unknown\shell\openas]

[HKEY_CLASSES_ROOT\Unknown\shell\openas\command]
@=hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,73,79,73,74,65,6d,33,32,5c,72,\
  75,6e,64,6c,6c,33,32,2e,65,78,65,20,25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,\
  73,79,73,74,65,6d,33,32,5c,73,68,65,6c,6c,33,32,2e,64,6c,6c,2c,4f,70,65,6e,\
  41,73,5f,52,75,6e,44,4c,4c,20,25,31,20,25,32,00
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
```

Windows 2000 Look

Voegt een extra schema, genaamd Windows 2000, toe aan Display -> Appearances.

```
- - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - - 8< - - - - -
[HKEY_CURRENT_USER\Control Panel\Appearance\Schemes]
"Windows 2000"=hex:02,00,00,00,9a,11,ed,77,01,00,00,00,10,00,00,00,10,00,00,00,\
  12,00,00,00,12,00,00,00,f5,ff,ff,ff,00,00,00,00,00,00,00,00,00,00,00,00,bc,\
  02,00,00,00,00,00,00,00,00,00,00,54,00,61,00,68,00,6f,00,6d,00,61,00,00,00,\
  20,00,53,00,65,00,72,00,69,00,66,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
```

```
  0f,00,00,00,0f,00,00,00,f5,ff,ff,ff,00,00,00,00,00,00,00,00,00,00,00,90,\
  01,00,00,00,00,00,00,00,00,00,00,54,00,61,00,68,00,6f,00,6d,00,61,00,00,00,\
  20,00,53,00,65,00,72,00,69,00,66,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  12,00,00,00,12,00,00,00,f5,ff,ff,ff,00,00,00,00,00,00,00,00,00,00,00,90,\
  01,00,00,00,00,00,00,00,00,00,00,54,00,61,00,68,00,6f,00,6d,00,61,00,00,00,\
  20,00,53,00,65,00,72,00,69,00,66,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  f5,ff,ff,ff,00,00,00,00,00,00,00,00,00,00,00,90,01,00,00,00,00,00,00,00,\
  00,00,00,54,00,61,00,68,00,6f,00,6d,00,61,00,00,00,20,00,53,00,65,00,72,00,\
  69,00,66,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,f5,ff,ff,ff,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,90,01,00,00,00,00,00,00,00,00,00,00,54,00,61,00,68,\
  00,6f,00,6d,00,61,00,00,00,20,00,53,00,65,00,72,00,69,00,66,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,f5,ff,ff,ff,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  90,01,00,00,00,00,00,00,00,00,00,00,54,00,61,00,68,00,6f,00,6d,00,61,00,00,\
  00,20,00,53,00,65,00,72,00,69,00,66,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,d4,d0,c8,00,3a,6e,a5,00,0a,24,6a,00,80,80,80,00,d4,d0,c8,00,ff,ff,ff,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,ff,ff,ff,00,d4,d0,c8,00,d4,d0,c8,00,80,\
  80,80,00,0a,24,6a,00,ff,ff,ff,00,d4,d0,c8,00,80,80,80,00,80,80,80,00,00,00,\
  00,00,c0,c0,c0,00,ff,ff,ff,00,40,40,40,00,d4,d0,c8,00,00,00,00,00,ff,ff,e1,\
  00
- - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - - - 8< - - - - -
```