Introduktie Windows/NT
Voor UNIX liefhebbers

Erik Meinders
Jos Visser
Open Solution Providers
http://www.osp.nl

6 juni 1997

Inhoudsopgave

Hoofdstuk 1

Inleiding

1.1 Introduktie Windows/NT, voor UNIX liefhebbers

Introduktie Windows/NT

Voor UNIX liefhebbers

Erik Meinders en Jos Visser
Open Solution Providers
http://www.osp.nl

Notities

Welkom bij deze lezing over Windows/NT. Het zal niemand ontgaan zijn dat Windows/NT, alhoewel een relatief nieuw besturingssysteem, bezig is met een ongekende zegetocht. Het is denken wij nog niet eerder voorgekomen dat een nieuw OS zo snel door zo velen is omarmd. Ook in omgevingen die traditioneel van UNIX gebruik maken duiken steeds meer Windows/NT servers op: als file server in een intranet, als applicatie server voor het draaien van Windows applicaties, maar ook als database of transactie server voor client/server applicaties.

UNIX omgevingen zien zich dus voor de taak gesteld om Windows/NT in de infrastructuur te integreren. In deze lezing wordt een inleiding gegeven in Windows/NT, worden de koppelingsmogelijkheden tussen Windows/NT en UNIX (kort) beschreven en worden een aantal kritische noten geplaatst bij Windows/NT.

1.2 Inhoud

Inhoud

- Deel 1: Inleiding Windows/NT
  - Sales pitch
- Deel 2: Integratie Windows/NT en UNIX
  - In bestaande netwerken
- Deel 3: Kanttekeningen en op- en aanmerkingen
  - De kritische noot

Notities

De lezing bestaat uit drie gedeelten. In het eerste gedeelte worden de features en eigenschappen van Windows/NT besproken. In het tweede gedeelte worden de mogelijkheden voor de integratie van Windows/NT en UNIX behandeld. Tot slot worden er een aantal kritische kanttekeningen bij Windows/NT en de inzetbaarheid ervan geplaatst.

In de bijlagen zijn een tweetal interessante artikelen opgenomen over Windows/NT domains en over het verschil in systeembeheer tussen UNIX en Windows/NT.

Hoofdstuk 2

Inleiding Windows/NT

2.1 Inleiding Windows/NT

Inleiding Windows/NT

Notities

In dit hoofdstuk worden de belangrijkste eigenschappen van Windows/NT behandeld. Aan de orde komen de geschiedenis van Windows/NT, de architectuur van het OS en de belangrijkste onderdelen en subsystemen. Er wordt ook een korte vooruitblik naar Windows/NT 5.0 gegeven.

2.2 Geschiedenis van Windows/NT

Geschiedenis van Windows/NT

- Microsoft besturingssystemen
  - MS DOS
  - Windows 3.x
  - OS/2
- New Technology operating system
  - Dave Cutler
  - Pas later beinvloedt door Windows!

Notities

Microsoft is zijn bestaan begonnen als leverancier van een "besturingssysteem" (a mess DOS) voor losstaande personal computers. Het bleek echter dat steeds meer organisaties gebruik gingen maken van netwerken om gegevens uit te wisselen. Met name centrale bestandsopslag en toegang tot gedeelde printers was (is) voor veel organisaties de eerste stap om de "losse" PC's te integreren. Microsoft wilde natuurlijk ook een deuntje meeblazen in de server markt. DOS was vanzelfsprekend niet het ideale platform om te dienen als file en/of printer server in een netwerk. Een nieuw OS was nodig.

In samenwerking met IBM is Microsoft toen begonnen aan de opvolger van DOS: OS/2. OS/2 moest de nadelen van DOS opheffen, het moest een stabiel multi tasking OS worden, dat gebruik kon maken van alle resources van de PC (niet alleen de eerste 640K geheugen), met een leuk grafisch interface. OS/2 moest de basis worden voor een aantal server applicaties voor file en printer serving (LanManager), remote databases (Database Manager) en communicatie (Communications Manager).

Om d'een of d'andere reden voelde Microsoft zich toch niet lekker over OS/2 of over de samenwerking met IBM. Toen Bill Gates hoorde dat Dave Cutler (de architect van DEC's vlaggeschip VMS) weg wilde bij Digital greep hij zijn kans: hij huurde Cutler en het grootste gedeelte van zijn staf in om een nieuw

OS te bouwen, gebaseerd op nieuwe technologie: het New Technology operating system. Cutler liet zich natuurlijk de kans om een geheel nieuw OS te bouwen niet ontgaan.

In eerste instantie hielden Cutler en de zijnen zich hoofdzakelijk bezig met de binnenkant van het nieuwe OS. Voor de NT system services (de NT Executive en de environment subsystems) kozen ze een modulaire opbouw gebaseerd op microkernel technologie. Na niet al te lange tijd moest er een buitenkant voor het nieuws OS komen. Hierbij liet het NT ontwikkelteam (intussen aangevuld met hele volksstammen Microsoft programmeurs) zich "inspireren" door het Windows 3.x user interface.

2.3 Eisen aan Windows/NT

Eisen aan Windows/NT

- Compleet nieuw OS
- Voor desktop en server
- Multi platform
- Netwerk gereed
- Compatibel
- Internationalisatie
- Veilig

Notities

Microsoft (Cutler c.s.) had voor het NT besturingssysteem duidelijk de visie dat het de basis moest gaan vormen voor een hele reeks server produkten waarmee Microsoft ook de markt voor afdelings- en bedrijfsservers kon gaan bestormen. NT moest echter ook een besturingssysteem worden wat op de desktop inzetbaar was. Windows/NT is hierdoor een merkwaardig OS geworden: aan de binnenkant alle mogelijke eigenschappen van een echt besturingssysteem, aan de buitenkant ogenschijnlijk niet te onderscheiden van zijn voorganger Windows 3.x.

2.4 Windows/NT als desktop OS

Windows/NT als desktop OS

- Sequential Multi User :-)
  - Effectief: single user
- Graphical User Interface
  - Eerst gebaseerd op Windows 3.x
  - Tegenwoordig gebaseerd op Windows95
- Ondersteuning voor OpenGL
  - 3D graphics, CAD

Notities

Met Windows/NT hoopte Microsoft ook een voet tussen de deur te krijgen op de markt voor krachtige werkstations. Hierbij moet in eerste instantie worden gedacht aan CAD/CAM en andere applicaties die flink veel reken- en tekenkracht op het bureau van de gebruiker behoeven. Hiertoe is Windows/NT vanaf de eerste versies uitgerust geweest met een grafisch gebruikers interface waardoor de drempel voor gebruikers om met NT te gaan werken behoorlijk werd verlaagd. In plaats van een uiterst krachtige (en complexe) commandoset (zoals in UNIX) kan de gebruiker werken met een DOS/Windows compatible command prompt en grafische werkomgeving.

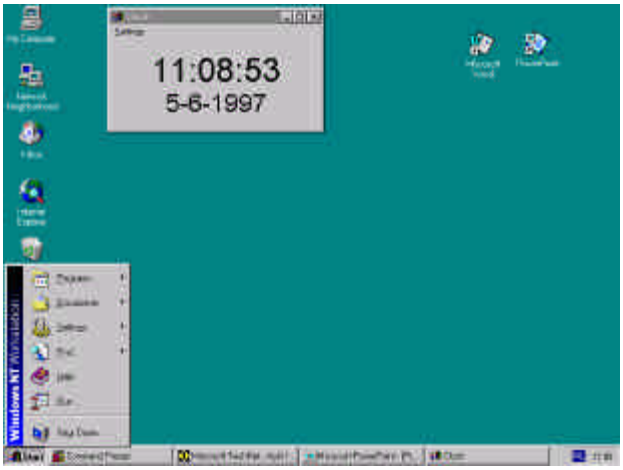
De veiligheidseisen die aan NT werden gesteld maken het verplicht om aan een NT computer aan te loggen. NT is echter nooit verzonnen als multi user besturingssysteem! Het aanlogproces is hoofdzakelijk bedoeld om ervoor te zorgen dat alleen geautoriseerde personen van een NT systeem gebruik kunnen maken. NT is trouwens ook in staat om een groot aantal instellingen (zoals de desktop indeling) per gebruiker op te slaan en te herstellen. Als een gebruiker echter door het netwerk gaat zwerven wordt het echter gaande moeilijker om zijn gebruikersinstellingen achter hem aan te laten reizen.

Microsoft heeft op dit moment twee strategische desktop besturingssystemen: Windows/NT (in de workstation uitvoering) en Windows 95. In onze optie gokte

Microsoft initieel alleen op Windows/NT voor de volgende generatie van de desktop. Toen de invoering en acceptatie van Windows/NT (mede door de hardware eisen) trager verliep dan verwacht heeft Microsoft Windows 95 in elkaar geknutseld op basis van de bestaande DOS en Windows technologie. Windows 95 is een hybride besturingssysteem wat niet gebaseerd is op nieuwe ontwikkelingen. Het is in feite niet meer dan DOS 7.0 en Windows for Workgroups 4.0, voorzien van een nieuwe buitenkant en met een uitgebreidere faciliteit voor het draaien van 32-bits applicaties. Steeds vaker zien we daarom ook dat organisaties Windows/NT toepassen als desktop operating systeem in plaats van Windows 95. De verbeterde stabiliteit, mogelijkheden en veiligheid van Windows/NT maken dat OS voor professionele organisaties een betere keuze is.

2.5 Windows/NT desktop

Windows/NT Desktop



Notities

Op de slide zien we een voorbeeld van de Windows/NT 4.0 desktop. Zoals u ziet is dit niet van Windows 95 te onderscheiden. In (uit) principe draait NT alle 32-bits applicaties die ook onder Windows 95 draaien. Met ingang van NT 4.0 is het user interface ook aangepast aan de nieuwe "look". Tot en met NT 3.51 was het NT user interface compatible met dat van Windows 3.x.

2.6 Windows/NT als server OS

Windows/NT als server OS

- Single user OS, dus server in client/server omgeving
- Multitasking/Multithreading
- SMP
- Stabiel, robuust
- Veilig
- Ingebouwde file en printer server

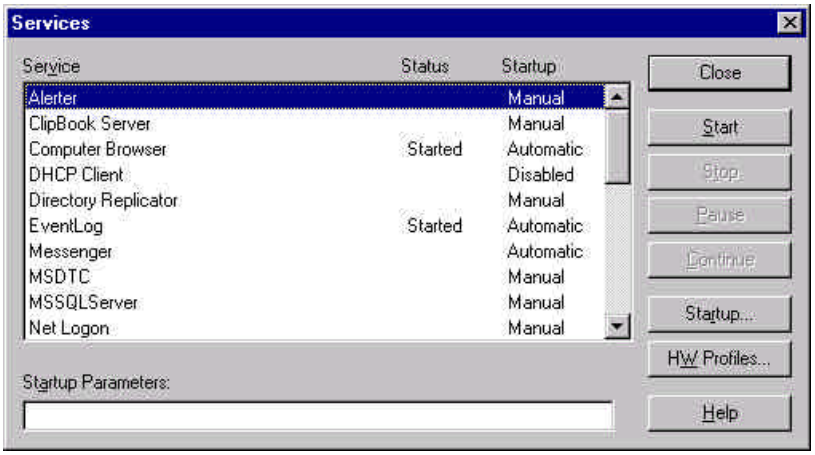
Notities

Een belangrijk doel van Microsoft voor Windows/NT was om als basis te dienen voor de server componenten in client/server omgevingen. Organisaties stellen aan servers vanzelfsprekend zeer hoge eisen, en Microsoft heeft daar vanaf het allereerste begin goed rekening mee gehouden. Het OS herbergt in zich alle eigenschappen die een goed server OS zou moeten hebben: stabiel, robuust en veilig. Ook aan performance is (vanzelfsprekend) de nodige aandacht besteed, onder meer door ondersteuning voor Symmetric Multi Processing: NT ondersteunt de aanwezigheid van meerdere processoren (standaard tot 31) in een computer.

Omdat een groot aantal klanten hun servers hoofdzakelijk gebruikt als file en printer server in een intranet wordt met Windows/NT een dergelijke server applicatie meegeleverd. Deze NT server applicatie is compatible met LanManager (en andere op het SMB protocol gebaseerde servers zoals LanServer) en kan naadloos samenwerken met Windows for Workgroups, Windows 95 en DOS. Hierdoor is de drempel om NT in te zetten als file en printer server behoorlijk laag. Het opzetten van een klein LAN met Windows/NT als file server is behoorlijk eenvoudig: alle benodigde software komt “out of the box” mee en behoeft weinig tot geen nadere implementatieinspanning.

2.7 Windows/NT Services

Windows/NT services



Notities

Om als server te kunnen dienen moet NT natuurlijk achtergrond processen ondersteunen. Nu is NT een multi tasking OS, dus dit zou geen moeite mogen kosten. Een standaard onderdeel van NT is de Service Manager, die verantwoordelijk is voor het starten en stoppen van achtergrond processen. Op de slide ziet u het Services control panel waarmee een overzicht wordt verkregen van welke achtergrond processen draaien. Met een simpele druk op de knop kunnen deze worden gestopt en gestart. Een NT programma moet speciaal als service zijn ontwikkeld om met deze service manager te kunnen samenwerken. In de WIN32 API zitten een groot aantal aanroepen die te maken hebben met de interactie tussen de daemon en de Service Manager.

In veel UNIX'en zitten overeenkomstige features (bijvoorbeeld in AIX/SMIT). Echter, in UNIX hoeft een programma niet speciaal te zijn ontwikkeld om als achtergrond proces te kunnen draaien. Hierdoor wordt er door het OS geen structuur afgedwongen, en is er een grote variatie in hoe UNIX achtergrond processen worden gestart en hoe ze stoppen. In NT is er een hechte integratie tussen het achtergrond proces en de Service Manager. Dit is mogelijk omdat NT precies voorschrijft hoe een service programma zich moet gedragen, en hoe het met het OS moet communiceren (om bijvoorbeeld een stop of pause opdracht te aanvaarden).

2.8 Multi Platform

Multi platform

- OS geschreven in C/C++
- Zeer klein gedeelte in assembler
  - Hardware Abstraction Layer
- Versies van Windows/NT voor:
  - Intel 386+
  - MIPS
  - Digital Alpha
  - PowerPC (wordt afgebouwd)

Notities

Microsoft wilde ook de afhankelijkheid van het Intel platform verminderen. Ten tijde dat met de ontwikkeling van NT werd begonnen kwamen de RISC processoren volop in de belangstelling. Microsoft wilde de mogelijkheid openhouden om NT ook op andere dan de Intel architecturen te draaien (in tegenstelling tot OS/2, wat strict Intel gebonden is). NT is dan ook voor een groot gedeelte op MIPS processoren ontwikkeld.

De ironie wil dat alhoewel Windows/NT vandaag aan de dag op meerdere RISC architecturen verkrijgbaar is, het Intel platform verreweg de belangrijkste van alle NT platformen is. De schaalvoordelen die kunnen worden behaald met het bouwen van computers gebaseerd op Intel processoren zijn dusdanig dat de prijs prestatie verhouding ongekend laag is [1].

Momenteel zijn er praktisch gesproken maar twee platformen van belang: Intel en Digital Alpha. Andere platformen worden afgebouwd (PowerPC) of zijn op sterven na dood (MIPS). De geruchten gaan dat Hewlett-Packard NT geport heeft naar de PA-RISC architectuur, maar dat ze liever wachten op de opvolger van de PA-RISC processor (die ze samen met Intel ontwikkelen).

[1] Inderdaad, hier staat *laag*!

2.9 Netwerkgereed

Netwerkgereed

- Netwerkfaciliteiten aanwezig in hele OS
- Protocollen:
  - TCP/IP
  - Netbeui
  - IPX/SPX
- File en print server
- Netware client en gateway
- Macintosh file server
- Netwerk IPC
  - Named pipes
  - Sockets
  - Mailslots
  - RPC's (DCE-achtig)
  - NETBIOS
- Beheer op afstand
  - Beperkt!
- Domain concept

Notities

Toen Microsoft begon met de ontwikkeling van NT was al duidelijk dat de toekomst van de IT zich in belangrijke mate op, in en rondom het netwerk zou gaan afspelen. De toenmalige Microsoft OS'en (DOS en Windows) zijn rampzalig in combinatie met netwerken. Het New Technology besturingssysteem moest natuurlijk naadloos met netwerken kunnen omgaan. Microsoft heeft dan ook geprobeerd om op alle fronten netwerkfaciliteiten in NT op te nemen. Hieronder valt bijvoorbeeld ondersteuning voor netwerk protocollen en IPC (Inter Process Communication) mechanismes. Ook worden er standaard een aantal applicaties meegeleverd die het mogelijk maken om een NT machine meteen bruikbaar in te zetten in een netwerkomgeving.

NT beheer applicaties zijn doorgaans ook ontwikkeld om over het netwerk te functioneren. Applicaties als de User Manager, de Event Viewer en de Performance Monitor hebben allemaal menu items om contact te zoeken met een remote computer om daar beheerwerkzaamheden op te verrichten. Een nadeel hierbij is dat als de applicatie het niet ondersteunt, het doorgaans ook niet kan. NT kent standaard geen telnet daemon! Deze zijn in het publieke domein wel te vinden, maar hebben weinig nut omdat de meeste NT beheerapplicaties grafisch van aard zijn.

Ondersteuning voor netwerken vinden we ook terug in het domein concept waarmee NT systemen kunnen worden gegroepeerd om gebruik te maken van een

centrale user account database (over het netwerk).

2.10 Compatibel

Compatibel

- Ondersteuning voor:
  - DOS applicaties (alleen "nette" applicaties)
  - Windows 3.x applicaties
  - OS/2 1.3 character mode applicaties
  - POSIX applicaties (hercompilatie nodig)
  - WIN32 applicaties
- FAT en HPFS file systems
- Netware connectiviteit

Notities

Microsoft had natuurlijk ook wel door dat het succes van een OS staat of valt met de beschikbaarheid van applicaties (vergelijk wat er gebeurd is met het NeXTStep besturingssysteem). Om het gebruik van NT een kickstart te kunnen geven is besloten dat NT zeer goed compatibel moest zijn met bestaande operating systemen, zodat er meteen een grote hoeveelheid applicaties was die op NT zou kunnen draaien. Dit zou een installed base voor NT kunnen creeren die het aantrekkelijk zou maken om native (WIN32) NT applicaties te gaan ontwikkelen.

Om deze reden biedt de Intel versie van NT ondersteuning voor het rechtstreeks draaien van DOS, Windows 3.x en OS/2 1.x character mode applicaties (geen Presentation Manager). Omdat DOS, Windows en OS/2 executables Intel X86 machinetaal bevatten kunnen deze programma's in principe rechtstreeks draaien, zonder instructievertaling of iets dergelijks. Het NT ontwikkelteam heeft "simpelweg" stubs geschreven die de DOS, Windows en OS/2 API calls opvangen en omzetten naar bijbehorende NT aanroepen. Om deze reden ondersteunt NT niet de ongedocumenteerde eigenschappen van die besturingssystemen. Alleen "nette" programma's draaien onder NT! DOS programma's die gebruik maken van allerlei "hidden features" kunnen meestal niet onder NT worden uitgevoerd. Ook het rechtstreeks benaderen van allerlei hardware wordt door NT niet toegestaan. Dit is dus een van de "pluspunten" van Windows

95. Omdat dit OS voor een groot gedeelte bestaat uit oude code draaien die ondeugende programma's daar wel!

Een bijzondere compatibiliteit wordt geboden door de ondersteuning voor POSIX applicaties. In principe komt het erop neer dat er in de WIN32 Software Development Kit (SDK) een verzameling header files en libraries zitten die het mogelijk maken om een C/C++ programma wat is geschreven volgens de richtlijnen van POSIX te vertalen. Vervolgens zitten er in het NT runtime gedeelte faciliteiten voor POSIX system calls zoals fork(), open() en link(). Dit zet de deur open naar het porteren van UNIX programma's naar NT. Bedenk echter wel dat allerlei interessante UNIX verschijnselen zoals X-Windows, semaforen en shared memory niet in de POSIX standaard zijn opgenomen. Er is een commercieel produkt, genaamd OpenNT, wat allerlei in UNIX gebruikelijke faciliteiten toevoegt aan Windows/NT. Met OpenNT ziet een Windows/NT systeem er verdacht veel uit als een UNIX systeem!

De flexibiliteit van NT blijkt overigens uit het feit dat zowel Windows als POSIX applicaties worden ondersteund. Deze twee omgevingen verschillen bijvoorbeeld in het feit dat in Windows bestandsnamen case insensitive zijn, en in POSIX case sensitive! De echter Windows/NT system call voor het openen van een bestand heeft een parameter die aangeeft hoe de naam moet worden geinterpreteerd!

Vanaf het eerste begin was duidelijk dat Windows/NT een concurrent voor Novell Netware zou worden. Om omgevingen die Netware gebruiken een makkelijk migratiepad naar NT te bieden heeft Microsoft allerlei features opgenomen die het mogelijk maken om NT machines te gebruiken in Netware netwerken. Er wordt zelfs een conversie utility (NWCONV.EXE) meegeleverd waarmee een hele Netware server (bestanden, user database, groepen, ACL's) kan worden geconverteerd naar een NT server!

2.11 Internationalisatie

Internationalisatie

- Support voor UniCode
  - Bijvoorbeeld in bestandsnamen!
- Message DLL's
  - Geen statische strings in programmatuur
- Internationale versies
- Schakelbare Input Locales

Notities

Om zoveel mogelijk kopieën van Windows/NT te verkopen heeft Microsoft ervoor gezorgd dat het OS in alle mogelijke talen en culturen ter wereld in te passen is. Er zit in NT veel mogelijkheden om applicaties zodanig te ontwikkelen dat het met systeeminstellingen aan te passen is voor verschillende talen. Windows/NT is voor bijna iedere denkbare taal uitgebracht (bijvoorbeeld: Koreaans, Fins, IJslands). Het OS heeft bijvoorbeeld ook ondersteuning voor UniCode, de nieuwe 16-bits karakter codering. Hierdoor kunnen in zaken als bestandsnamen ook niet ASCII karakters worden gebruikt!

2.12 Veilig

Veilig

- Uitgebreide beveiligingsmogelijkheden:
  - User + group identificaties
  - Access Control Lists (files, directories, printers, processen, desktops ...)
  - Uitbreidbare beveiliging
    - Security Support Provider Interface
    - GINA
  - Auditing
- C2 rating (basis OS)
- Administrator mag niet alles!

Notities

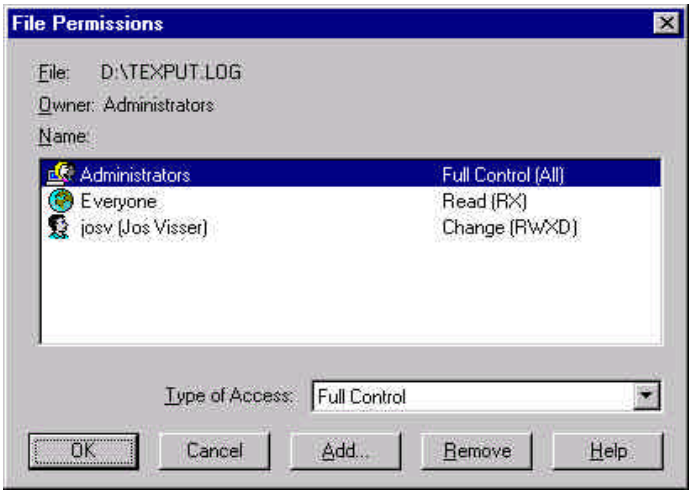
Bij de ontwikkeling van Windows/NT is veel rekening gehouden met beveiliging (naar mijn bescheiden mening niet genoeg, maar voor de meeste toepassingen in ieder geval voldoende). Zo kunnen objecten (bestanden, printers, processen, desktops) worden beschermd met Access Control Lists waarmee precies kan worden vastgelegd wie wat mag. Die ACL's kennen ook "deny" faciliteiten waarmee uitzonderingen kunnen worden geïmplementeerd, zoals: iedereen in de groep 'Users' behalve user 'Bill'.

Verder bestaat de Windows/NT beveiliging uit een aantal componenten die door programmeurs kunnen worden uitgebreid om bijvoorbeeld smart cards of andere bezitselementen te ondersteunen. NT ondersteunt ook auditing waarmee objecten in de gaten kunnen worden gehouden (success en failure). Het basis NT OS is gecertificeerd voor het C2 security niveau (mind you: het netwerkgedeelte van NT is (nog) niet gecertificeerd!).

Een belangrijk verschil met UNIX is dat een NT administrator niet automatisch alle rechten heeft. Administrators zijn net als alle andere gebruikers onderhevig aan NT beveiliging. Een gebruiker kan een administrator bijvoorbeeld uitsluiten van toegang op bestanden! Ook kan een administrator geen resources weggeven aan andere gebruikers (geen equivalent van de chown() system call). Om toch alle bestanden te kunnen backuppen kan een speciale backup user worden gemaakt die het systeemwijde attribuut 'Backup files and directories" heeft.

2.13 Voorbeeld Access Control List

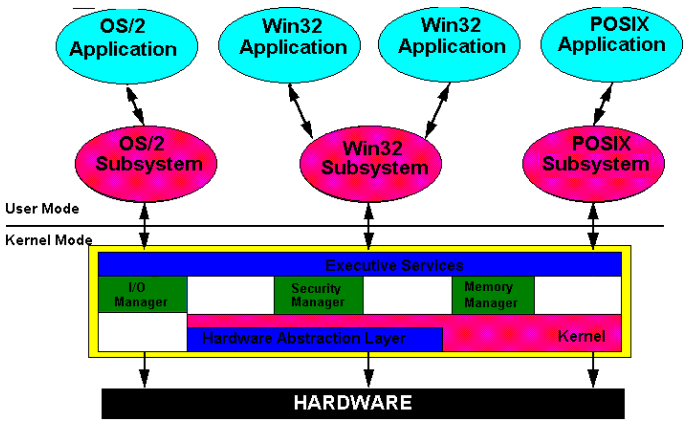
Voorbeeld Access Control List



Notities

Op de slide staat een voorbeeld van een NT access control list. ACL's op bestanden kunnen worden aangebracht met de Explorer (File Manager) of via het commando CACLS.EXE. ACL's op andere objecten moeten worden aangebracht met programma's die speciaal voor dit doel zijn ontwikkeld.

2.14 Windows/NT Architectuur



Notities

Deze slide is eigenlijk te ingewikkeld kort te beschrijven. Voor een uitstekende introduktie in de binnenkant van Windows/NT verwijs ik naar het boek "Inside Windows/NT" van Helen Custer.

De kern van de zaak is dat de opbouw van Windows/NT zeer modulair is. De Executive (wat we in UNIX de kernel zouden noemen) bestaat uit een zeer groot aantal losse modules die bij het booten in het geheugen worden geladen. In de Windows/NT Device Driver Kit (DDK) zitten uitgebreide voorbeelden van hoe drivers en subsystemen voor NT kunnen worden ontwikkeld.

Een belangrijk aspect is dat de user API's van Windows/NT (DOS, Windows, OS/2 en POSIX) als losse subsystemen in user mode draaien!

2.15 Server en Workstation

Server en Workstation

- Twee Windows/NT smaken:
  - Windows/NT Server
    - Basis voor BackOffice lijn
      - SQL Server
      - SNA Server
      - System Management Server
  - Windows/NT Workstation
    - Desktop gebruik
    - Server in hele kleine netwerkjes
- Zelfde OS, andere packaging

Notities

Er bestaan twee varianten van Windows/NT: Workstation en Server. Als je NT gaat kopen heb je de keuze uit twee produkten: Windows/NT Workstation en Windows/NT Server. Dit geeft nogal eens aanleiding tot verwarring. Het betreft namelijk hetzelfde besturingssysteem, alleen in een wat ander jasje. Op de NT Server CD staan bepaalde programma's wel, die op de Workstation CD niet zitten. Kopieer je ze echter met de hand dan werken ze feilloos. Verder zit er in NTW een ingebouwde limiet van maximaal tien clients (voor file/print server toepassingen). Verder is NTS standaard van wat andere defaults voorzien die beter passen bij het gebruik als server in een netwerk.

Sommige applicaties draaien alleen op NT Server, maar dat komt eigenlijk alleen omdat ze bij het installeren controleren of ze wel op een NTS computer worden geïnstalleerd. Technisch gesproken is er eigenlijk geen verschil. Sommige BackOffice applicaties (zoals SQL Server) draaien net zo makkelijk op een NT Workstation. Het prijsverchil tussen NTW en NTS is momenteel ongeveer nlg. 500,=.

2.16 Diverse highlights

Diverse highlights

- New Technology File System (NTFS)
- Remote Access Service (RAS)
- Beheerhulpmiddelen
- Registry
- Mirroring en Striping
- Performance Monitor
- Domains en trusts
- Internet ondersteuning

Notities

Boven en in het basis NTOS zijn er door Microsoft een groot aantal programma's, hulpmiddelen en subsystemen ontwikkeld. Een groot gedeelte van de charme van Windows/NT is dat het standaard wordt uitgeleverd met een groot aantal tamelijk bruikbare subsystemen. Voor bijna al die subsystemen geldt dat het niet de beste denkbare implementaties op dat specifieke gebied zijn, maar voor de meeste klanttoepassingen goed genoeg. Een klant die op een speciaal gebied een betere oplossing wil kan die meestal ergens uit de markt betrekken.

2.17 New Technology File System

New Technology File System

- Journaled file system
- Lange filenames, case insensitive!
- Access Control Lists
- Extended Attributes
- Volume sets
- File size: 16 exabyte (16 miljoen terabyte)
- Compressie

Notities

Een kernonderdeel van Windows/NT wordt gevormd door een nieuwe file systeem implementatie: NTFS. Uit de verhalen rondom de ontwikkeling van NT blijkt dat pas zeer laat is besloten om een eigen file systeem aan NT toe te voegen. Lange tijd is met de gedachte gespeeld om alleen FAT en HPFS te ondersteunen!

De belangrijkste reden voor de meeste organisaties om NTFS te gebruiken is dat alleen het NTFS ACL's ondersteunt! Op bestanden in een FAT of HPFS file systeem kan geen ACL worden gelegd. Een ander opvallend punt van NTFS is dat het een journaling file system betreft wat wijzigingen op de disk op een transactionele manier behandelt, (vergelijk het Veritas eXtended File System) zodat er na een crash een snelle reparatie van het file system mogelijk is. Ook ondersteunt het NTFS compressie per bestand of directory.

Voor een uitstekende uitleg over het NTFS verwijs ik naar het boek "Inside NTFS" van Helen Custer.

2.18 Remote Access Service

Remote Access Service

- Dial-in en Dial-out Networking over kieslijnen:
  - Asynchrone (modems)
  - X.25
  - ISDN
- PPP encapsulation protocol
- Lan proxy
- Callback support

Notities

Standaard wordt met NT een dial-in server en een dial-out client meegeleverd. Deze software gaat door het leven als RAS: de Remote Access Service.

De dial-out client maakt het mogelijk om over een modem, X.25 of ISDN op te bellen naar een PPP server. Na de autenticatie krijgt het uitbelapparaat een netwerkadres op het remote LAN en kan het alle netwerkfuncties via de seriële lijn uitvoeren. De RAS driver in de Executive emuleert als het ware een LAN interface in het remote LAN. Via RAS kan bijvoorbeeld worden uitgebeld naar Internet providers.

Met de RAS dial-in software kan van een NT machine een inbelserver worden gemaakt voor PPP-clients. Een NT Server ondersteunt 255 gelijktijdige inbelsessies (een NTW slechts één). Voor de autenticatie van de inbeller wordt gebruik gemaakt van de NT user administratie. Per gebruiker kunnen inbel- en callback bevoegdheden worden uitgedeeld.

RAS kan overigens vrij slecht overweg met huurlijnen!

2.19 Beheerhulpmiddelen

Beheerhulpmiddelen

- Vrijwel alles beheren met grafische beheerhulpmiddelen
- Geen/beperkt command line interface
- Geen script taal
  - Perl beschikbaar via resource kit / public domain
- Remote beheer via applicaties (geen telnet)

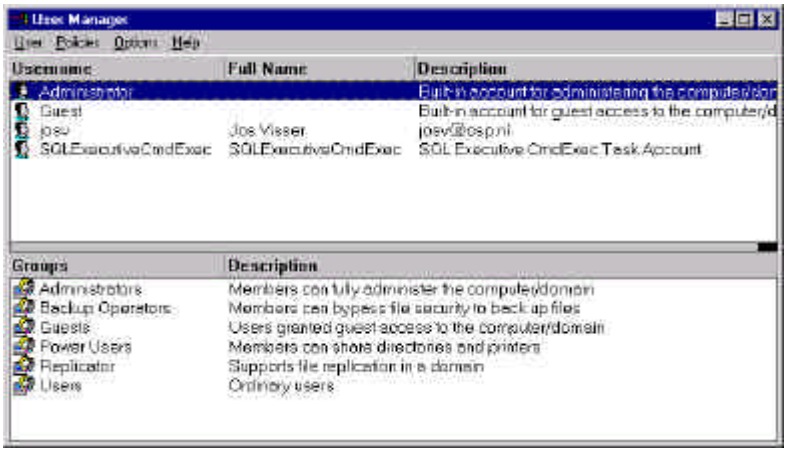
Notities

Iedere faciliteit van Windows/NT levert zijn eigen beheertool mee. In 99,9interactief beheer kan worden gepleegd. Er is meestal geen command line versie van de NT beheertools! Dit betekent onder andere dat het niet eenvoudig is om zelf beheertools in elkaar te knutselen in een of ander script taaltje. Op zich matched dit weer aardig met het gebrek aan een standaard script taal in NT. Voor een aantal beheerzaken zijn wel API's beschikbaar zodat eventueel in C/C++ een tool zou kunnen worden gebouwd. Een grote verzameling van dit soort tooltjes wordt gevormd door de NT resource kit.

De meeste beheerhulpmiddelen hebben een menuoptie waarmee de focus kan worden verlegd naar een ander systeem in het netwerk. Op die wijze kan een NT netwerk voor een groot gedeelte vanaf een centraal systeem worden beheerd. NT kent geen variant van de telnet daemon: als de applicatie geen ondersteuning heeft voor netwerk beheer dan kan het in zijn algemeenheid niet op afstand worden uitgevoerd! Een weg hieromheen wordt gevormd door applicaties zoals Carbon Copy en PC Anywhere, waarmee een geheel NT console (grafisch!) kan worden overgenomen. De snelheid hiervan is helaas nog al te vaak bedroevend.

2.20 Voorbeeld User Manager

Voorbeeld User Manager



Notities

Een voorbeeld van een NT beheertool staat op de slide: De Windows/NT User Manager. Met behulp van de User Manager kan het gebruikers en groepenbeheer van Windows/NT worden gevoerd. Het is een hele vriendelijke applicatie die zo ongeveer door iedereen wel te gebruiken is.

Waar je natuurlijk niet aan moet denken is om met behulp van deze applicatie duizend gebruikers toe te moeten voegen!

2.21 De Registry

De Registry

- Geconsolideerde systeeminformatie database
- Modificeerbaar via:
  - API
  - Registry Editor
- Beheerbaar over netwerk (API, editor)
- ACL per (sub)key

Notities

UNIX wordt (net als Windows 3.x) gekenmerkt door de aanwezigheid van een groot aantal kleine configuratiebestanden waarin van alles en nog wat in te stellen valt. Met name in Windows 3.x heeft dit nogal wat nadelen met zich meegebracht. Om die reden hebben de ontwikkelaars van Windows/NT ervoor gekozen om het nieuwe besturingsysteem uit te rusten met een soort configuratiedatabase waar iedereen en alles op het gebied van configuratie in diende te komen: de Registry.

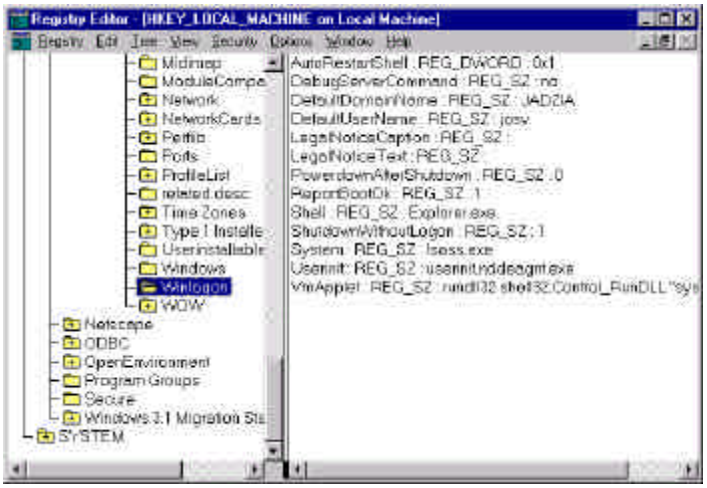
Windows/NT houdt zelf alle configuratieinformatie (drivers, subsystemen, wat te starten bij booten, printers etc. etc.) bij in de registry. Applicaties worden van harte uitgenodigd dit ook te doen. Hierdoor is een enkelvoudige geconsolideerde configuratiedatabase ontstaan waarin alle configuratieinformatie van het hele systeem bijeengebracht is. Met behulp van systeemaanroepen (WIN32 API) kunnen programma's de registry ondervragen en wijzigen. Met Windows/NT wordt een algemeen programma meegeleverd waarmee de registry interactief kan worden geraadpleegd en aangepast: de Registry Editor.

Ten tijde van het verschijnen van NT leek de registry een uitermate goed idee: weg met al die losse .ini files! Zo langzamerhand begint ook de keerzijde van de medaille zichtbaar te worden. De registry is uiterst complex van opbouw, bevat een enorme hoeveelheid informatie, is niet gemakkelijk gedeeltelijk veilig te stellen en is buiten NT om niet aan te passen (geen single user mode!). In

het geval de registry in ongerede is, is het vrijwel onmogelijk om dit goed te herstellen! Een goede backup/restore procedure voor de registry is een hele uitdaging!

2.22 Registry Voorbeeld

Registry Voorbeeld



Notities

Op de slide ziet u een voorbeeld van de Windows/NT Registry Editor. Via deze tool kan handmatig de inhoud van de registry worden gewijzigd. Hiermee dient uiterste zorgvuldigheid in acht te worden genomen. Sommige waardes in de registry hebben een interne afhankelijkheid met andere parameters! Een nadeel van de registry is dat sommige stukken eigenlijk alleen via configuratie programma's (bijvoorbeeld uit het Control Panel) mogen worden aangepast, terwijl andere waardes alleen handmatig zijn in te stellen.

2.23 Disk Administrator

Disk Administrator

- Partitionerings tool
- Standaard PC partities (max. 4 per schijf)
- Ondersteuning voor
  - Volume Sets (NTFS)
  - Mirroring en Striping (NTS: Raid-5)

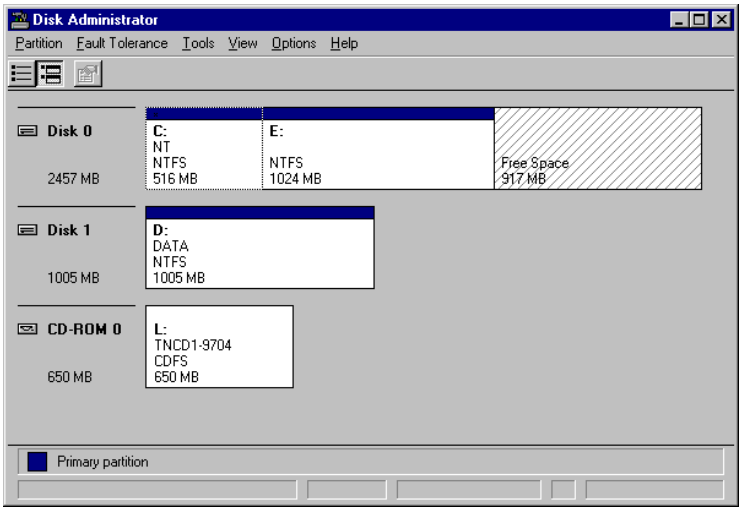
Notities

Voor de indeling van de schijven vertrouwt Windows/NT op het vertrouwde disk partitionerings schema van DOS: maximaal 4 partities per schijf met een trucje om dit aantal te verhogen (via een zogenaamde extended partitie die weer subpartities kan hebben). Wel zitten er in Windows/NT een aantal mogelijkheden om partities te mirroren, om RAID-5 stripe sets te maken en om partities met NTFS file systems samen te voegen tot een zogenaamde Volume Set.

Voor het beheer van de partitieindeling wordt een grafische tool meegeleverd: de Disk Administrator. Met behulp van de Disk Administrator kunnen ook de drive letters van de schijven (ook CDROM drives) worden bepaald.

2.24 Voorbeeld Disk Administrator

Voorbeeld Disk Administrator



Notities

Well, the title of this slide says it all.....

2.25 Performance Monitor

Performance Monitor

- Standaard onderdeel van Windows/NT
- Uitgebreide verzameling te monitoren objecten en attributen
  - CPU, geheugen
  - Disk, netwerk interfaces, protocollen
- Uitbreidbaar met eigen statistieken
  - Bijvoorbeeld SQL Server

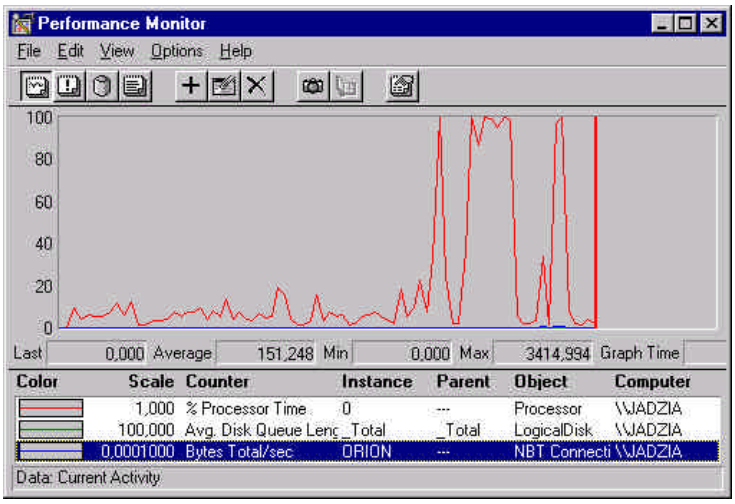
Notities

Om de systeembeheerder in staat te stellen de performance van een NT systeem te bekijken zit er standaard een performance monitor bij Windows/NT. Met die performance monitor kunnen van zeer veel verschillende OS objecten performance statistieken boven water worden getoverd, en worden omgezet in een rapport of een grafiek. De Performance Monitor biedt tevens mogelijkheden om een alarm te genereren zodra een bepaalde meetwaarde een vooraf ingestelde grens overschrijdt.

Een aardig aspect aan de Performance Monitor is dat applicaties hun eigen performance statistieken kunnen definiëren en bij de Performance Monitor aanleveren. Zo voegt SQL Server bijvoorbeeld een groot aantal performance objecten aan de Performance Monitor toe.

2.26 Voorbeeld Performance Monitor

Voorbeeld Performance Monitor



Notities

Op de slide ziet u een voorbeeld van een Performance Monitor grafiek. Een belangrijk nadeel van de Performance Monitor is dat het niet mogelijk is om in de achtergrond performance statistieken te verzamelen zonder dat het user interface van de Performance Monitor actief is, het is puur een interactief programma.

2.27 Domain

Domain

- Groep NT servers en workstations die gebruik maken van dezelfde User Account Database (user/group info)
- 1 Primary Domain Controller
- 0 of meer Backup Domain Controllers
- Automatische synchronisatie tussen PDC en BDC's
- Ook voor clients toegankelijk (wfw, w95)

Notities

Opmerking: voor een meer gedetailleerde uitleg over Windows/NT domains en de implicaties ervan verwijzen we naar bijlage A.

Windows/NT ondersteunt het groeperen van NT computers in zogenaamde Domains. Kenmerkend voor een domain is dat de NT systemen die lid zijn van het domain gebruik (kunnen) maken van één en dezelfde User Accounts Database (UAD). Één van de NT Servers in het domain heeft de rol van Primary Domain Controller (PDC). De UAD van de PDC vervult de rol van domain UAD. De user en group definities in die UAD zijn geldig op alle NT systemen in het domain. Dit betekent onder andere dat aan een NT Server of Workstation kan worden aangelogd met een userid uit het domain. Een ander gevolg is dat op een ACL op een lid van het domain users en groepen uit de domain UAD voor kunnen komen.

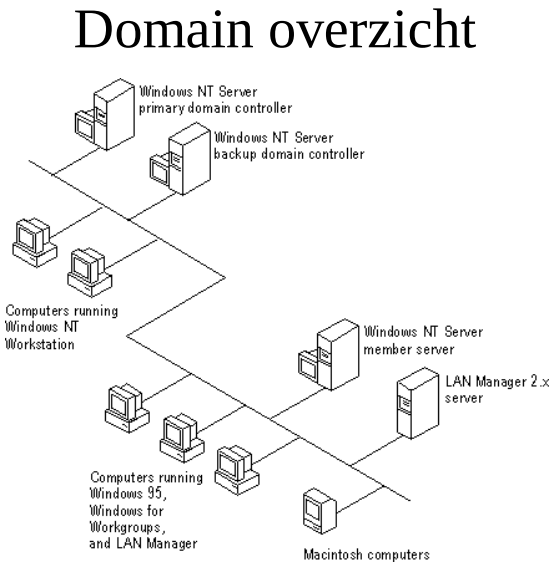
Als de PDC uitvalt is de domain UAD niet beschikbaar. Ten gevolge hiervan zou er niemand aan kunnen loggen op de NT systemen in het domain. Om dit te voorkomen kunnen één of meer Backup Domain Controllers (BDC's) worden ingericht. Via een synchronisatiemechanisme ontvangen de BDC's regelmatig updates van de PDC. Een client die aanlogt kan iedere domain controller (PDC of BDC) gebruiken om de logon te valideren. Als de PDC uitvalt heeft dit nu geen effect meer voor de beschikbaarheid van de UAD: de BDC's hebben immers een kopie van die UAD. Wijzigingen in de UAD kunnen alleen worden

aangebracht op de PDC. Deze distribueert ze dan automatisch naar de BDC's. Als de PDC is uitgevallen en langere tijd niet beschikbaar is kan één van de BDC's worden gepromoveerd tot PDC. Als de echte PDC dan weer opkomt kan die worden gedegradeerd tot BDC, of kan de huidige PDC terug worden gedegradeerd tot BDC.

NT domain controllers kunnen ook worden gebruikt om logons vanaf Windows 3.x en Windows 95 machines te valideren. Deze clients kunnen geen lid zijn van domains, maar kunnen wel worden geconfigureerd om bij het aanloggen de userid/password combinatie bij een domain controller aan te bieden voor validatie.

Het NT domain concept is grofweg vergelijkbaar met NIS.

2.28 Domain Overzicht



Notities

Op de slide ziet u een voorbeeld van een Windows/NT domain met een aantal clients. Een domain bestaat minimaal uit een Primary Domain Controller en eventueel nog een aantal leden (NT Workstations of NT Servers). Er is compatibiliteit met LanManager en LanServer. Deze oudere file en printer servers kunnen lid zijn van een NT domain, maar kunnen geen domain controller spelen. Op de slide staan ook een aantal niet-NT computers. Deze zijn geen lid van het domein, maar gebruiken alleen de resources van de leden van het domein.

Of een NT Server een domain controller is wordt bepaald bij de Windows/NT installatie. Is een NT Server geïnstalleerd als lid van een domain (geen domain controller) dan kan er geen domain controller meer van worden gemaakt (zonder herinstallatie). Een domain controller kan nog wel van rol wisselen (PDC of BDC) via het promotie/degradatie mechanisme.

Windows/NT domains kunnen meerdere LAN segmenten beslaan door gebruik te maken van TCP/IP als basis netwerkprotocol. Een probleem wat dan wel moet worden opgelost is de vertaling van NETBIOS namen naar IP adressen en vice versa. In een enkel LAN wordt die vertaling gedaan door broadcasts. In een internet omgeving lukt dit vanzelfsprekend niet meer. De eenvoudigste manier om die vertaling te regelen is door het implementeren van de Windows Name Server (WINS).

2.29 Trust

Trust

- Koppeling tussen twee domains
- Trusting domain vertrouwt de UAD van het trusted doman
- UAD van het trusted domain kan worden gebruikt in het trusting domain
  - Aanloggen
  - ACL's
  - Groepslidmaatschappen (beperkt)

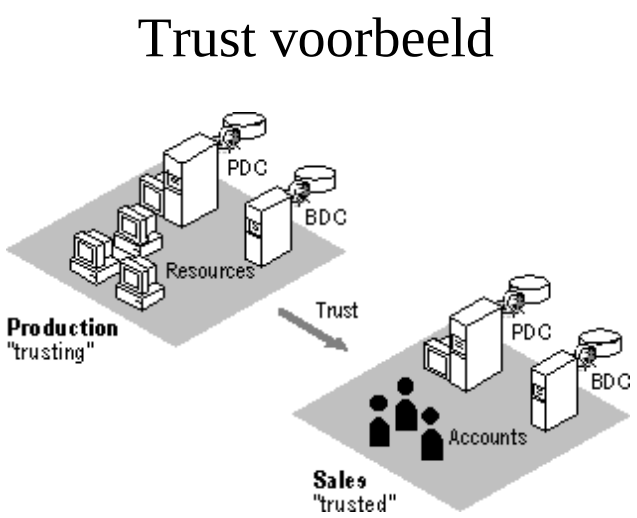
Notities

In omgevingen die om wat voor reden dan ook meerdere domains hebben is het mogelijk om die domains elkaar te laten vertrouwen door het leggen van een 'Trust' relatie. Zo'n trust relatie is een enkele, gerichte, niet overdraagbare verbinding tussen twee domains waarbij één domain (het trusting domain) de UAD van een ander domain (het trusted domain) vertrouwt. Dit heeft tot gevolg dat de NT computers in het trusting domains ook logons kunnen accepteren van users met een userid uit het trusted domain. Bij een aanlogpoging wordt naast het userid en wachtwoord in een NT omgeving ook altijd de naam meegegeven van het domain waar het userid thuishoort. Indien een NT computer een logon ontvangt van een userid uit een ander domain kan het de logon valideren bij een domain controller uit dat andere domain, mits dat andere domain maar vertrouwd wordt (een trusted domain is).

Een ander gevolg van trusts is dat de users en groepen van het trusted domain op ACL's in het trusting domain kunnen voorkomen.

De toepassing van trusts en groepen in de huidige versie van Windows/NT is nog ietwat beperkt. In het volgende release (Windows/NT 5.0) wordt de semantiek rondom trusts aanzienlijk uitgebreid.

2.30 Trust Voorbeeld



Notities

Op de slide ziet u een grafische weergave van een trust relatie tussen twee domains. Indien twee domains elkaar vertrouwen moeten er twee trust relaties worden geschapen: één heen en één terug. Om een trust relatie te maken dienen de beheerders van zowel het trusted als het trusting domain een actie te ondernemen. Via trusts kan worden gerealiseerd dat een gebruiker slechts in één domain een userid heeft, maar toch permissies heeft op servers in verschillende andere domains. Veel organisaties richten een apart domain op voor het vasthouden van alle userid's (een zogenaamd account domain).

2.31 Internet ondersteuning

Internet ondersteuning

- Internet Information Server
  - Web, Gopher, FTP
- Internet Explorer
  - Web, Mail, News
- DNS
- Standaard geen SMTP/POP server software

Notities

Nu ook Microsoft het bestaan van Internet niet langer kan ontkennen zetten ze alles op alles om Windows/NT als basis platform voor Internet servers aantrekkelijk te maken. De ondersteuning voor Internet vinden we zowel in het NT besturingssysteem als in de server applicaties terug.

Zo wordt NT 4.0 standaard uitgeleverd met de Internet Information Server: een eenvoudige, maar functionele, WWW, FTP en Gopher server. Verder wordt de Microsoft Internet Explorer meegeleverd: een Java enabled WWW browser en Mail/News client. Tot slot wordt er in NT 4.0 een NT implementatie van BIND meegeleverd waarmee een DNS kan worden ingericht. Volgens de beste Microsoft traditie is de NT DNS voorzien van een grafisch gebruikersinterface waarmee relatief eenvoudig een BIND zone file kan worden gemaakt en gevuld.

In de Microsoft BackOffice server applicatie reeks vinden we ook de nodige ondersteuning voor Internet terug: bijvoorbeeld in SQL Server, Merchant Server, Transaction Server en Exchange Server. Opvallend is dat onder NT standaard geen SMTP/POP server software wordt meegeleverd voor het opzetten van een Internet mail hub.

2.32 Overige goodies

Overige “goodies”

- Network Monitor
- Event Viewer
- NT Backup
- DFS (Distributed File System)
- UPS
- Conversie tool voor Netware

Notities

Er zitten in Windows/NT natuurlijk nog veel meer onderdelen die het vermelden waard zijn. Een aantal hiervan ziet u op de slide. In vergelijking met UNIX valt het op dat er met Windows/NT veel minder features worden meegeleverd. De features die onderdeel zijn van Windows/NT zijn doorgaans veel minder krachtig dan in UNIX, maar voor de beginnende systeembeheerder veel eenvoudiger te gebruiken.

2.33 Windows/NT 5.0

Windows/NT 5.0

- NT Directory Services
  - X.500-achtige directory
  - LDAP ondervraagbaar
  - Active Directory
- Microsoft Management Console
- Distributed File System
  - Preview beschikbaar in NT 4.0

Notities

Windows/NT is een nog jong besturingssysteem, wat toch al brede ingang heeft gevonden in de markt. Om problemen in Windows/NT weg te nemen, en het mogelijk te maken Windows/NT in grote, complexe, omgevingen in te zetten wordt door Microsoft momenteel hard gewerkt aan het uitbreiden van Windows/NT.

Het volgende grote release van Windows/NT is 5.0. De belangrijkste uitbreiding zal de implementatie van een uitgebreide Directory Service zijn. Hiermee hoopt Microsoft het beheer van allerhande definities (gebruikers, groepen, resources) aanzienlijk te verbeteren. De NT Directory Service maakt NT 5.0 een direkte concurrent van Netware 4.x (met de Netware Directory Service). Met NTDS moet het mogelijk worden om een organisatiebrede directory op te bouwen.

Hoofdstuk 3

Integratie Windows/NT en UNIX

3.1 Integratie Windows/NT en UNIX

Integratie Windows/NT en UNIX

Notities

In dit hoofdstuk worden de belangrijkste mogelijkheden om Windows/NT en UNIX systemen aaneen te smeden besproken. Veel van de hier besproken mogelijkheden bestaan uit de aanschaf en implementatie van allerlei additionele software produkten!

3.2 Integratiemogelijkheden

Integratiemogelijkheden

- TCP/IP ondersteuning
- File server/client
- X-Windows
- Printen
- NT op X-terminals
- Interprocess communicatie
- Aantal standaardfeatures
- Public domain software
- Derde partij software

Notities

Op de slide ziet u kort de meest belangrijke mogelijkheden voor integratie opgesomd. Zowel UNIX als Windows/NT kennen standaard slechts een zeer beperkt aantal mogelijkheden tot integratie. Dit heeft hoofdzakelijk te maken met het feit dat de besturingssystemen uit zeer verschillende hoek afkomstig zijn en ook een zeer verschillende opbouw en mogelijkheden hebben. Allerlei derde partijen zijn in deze markt gesprongen en leveren produkten die de integratie tussen UNIX en Windows/NT bevorderen. Veel van deze produkten zijn echter gloednieuw, en zijn daardoor nog lang niet uitontwikkeld.

3.3 TCP/IP implementatie in NT

TCP/IP implementatie in NT

- Clients voor:
  - telnet, FTP
  - rsh, rexec, rcp
- FTP server
- SNMP agent & API
- TCP/IP printing
  - lpr, lpq, lpd
- NETBIOS over TCP/IP (NBT)
- RIP (routing protocol)
- DNS client+server
- DHCP Server
  - BOOTP compliant sinds SP3
- RPC (DCE-achtig)
- Sockets (Berkeley compatibel)

Notities

Een groot gedeelte van de integratie tussen UNIX en Windows/NT wordt mogelijk gemaakt door een goede TCP/IP implementatie in NT. Zijn we echter in UNIX gewend dat een zeer groot aantal TCP/IP-gerelateerde utilities worden meegeleverd, in Windows/NT is de hoeveelheid commando's wat met TCP/IP wordt meegeleverd nog vrij gering. TCP/IP is in Windows/NT ook een optie, geen verplichting! (organisaties kunnen ook nog voor andere protocollen zoals IPX/SPX kiezen).

Opvallend is dat er met Windows/NT vrijwel geen TCP/IP server applicaties worden meegeleverd (uitgezonderd de WWW/FTP/Gopher server). Zo is er bijvoorbeeld geen telnet server of mail server. Wel wordt er een DNS server meegeleverd (BIND variant). Als toegift integreert de Windows/NT DNS met de andere Windows/NT name server: WINS.

3.4 File Server

File Server

- NFS file server voor Windows/NT
  - Marathon van NCD
  - SOS NFS Server (Public Domain)
- NT compatible file server voor UNIX
  - Samba (Public Domain)
  - AdvanceNet
  - TotalNet
  - LanManager/X

Notities

Één van de eerste dingen die organisaties die zowel UNIX als Windows/NT hebben willen is het gemakkelijk uitwisselen van bestanden. De FTP server is hier natuurlijk niet de meest aangewezen methode voor. Het zou veel leuker zijn als schijven van een NT machine gemount konden worden op een UNIX computer, of omgekeerd. In zijn algemeenheid kunnen we twee paden volgen:

1. Richt de Windows/NT machine in als NFS server
2. Richt de UNIX machine in als SMB server [1]

Voor de eerste mogelijkheid hebben we de keuze uit een aantal produkten waarmee van een Windows/NT server een NFS server kan worden gemaakt. Twee voorbeelden hiervan ziet u op de slide. Een conceptueel probleem hierbij is natuurlijk dat NFS gebruik maakt van standaard UNIX uid's om aan te geven welke gebruiker de NFS request doet. De Windows/NT NFS server moet dit op een of andere manier mappen op een Windows/NT SID of gebruikersnaam.

De andere mogelijkheid is om een UNIX machine zich te laten gedragen als een Windows/NT (compatible) file server. Er zijn een aantal produkten beschikbaar

[1] SMB is het netwerk file server protocol wat door Windows/NT en aanverwante wordt gebruikt

waarmee dit kan worden gerealiseerd. Met name het public domain produkt Samba is zeer populair en vrij goed. Een probleem met dit soort oplossingen is dat SMB servers bij het accepteren van een verbinding een challenge/response protocol uitvoeren om te controleren of de gebruiker op de client wel het juiste wachtwoord kent. Om dit goed te laten gaan moet er op de UNIX machine een dubbele user registratie worden bijgehouden (door verschillen in wachtwoord-mogelijkheden en encryptie in UNIX en Windows/NT). Er ontstaat dus een potentieel wachtwoordsynchronisatieprobleem.

Een algemeen probleem met dit soort file server produkten is dat ze meestal als applicatie draaien (niet als NT of UNIX kernel component). De performance kan nog wel eens te wensen over laten.

3.5 Client

Client

- NFS client voor Windows/NT
  - PCNFS
  - Marathon (NCD)

Bijzonder: smbfs

NT compatible VFS voor Linux!

Notities

Er bestaat ook altijd nog de optie om een Windows/NT systeem uit te rusten met een NFS client. De interne opbouw van Windows/NT is dusdanig dat het mogelijk is om ondersteuning voor andere typen (netwerk) file systems als modules toe te voegen (vergelijk met het VFS van UNIX). Er zijn een aantal pakketten op de markt waarmee dit kan worden gerealiseerd. Zodra een gebruiker aanlogt wordt het wachtwoord zowel door Windows/NT als door een UNIX machine gecontroleerd (rpc.pcnfsd). Dit geeft de NT machine de informatie die nodig is om bestanden per NFS te benaderen (UNIX uid van de gebruiker). Indien de wachtwoorden op UNIX en Windows/NT niet gelijk zijn verschijnt er meestal een tweede aanlogprompt waarop de gebruiker zijn UNIX wachtwoord kan inkloppen.

Een heel bijzonder verschijnsel wordt gevormd door het smbfs. Dit is een UNIX file system (VFS) voor Linux, via welke Linux machines als SMB client gebruik kunnen maken van gesharede directories op NT systemen.

3.6 X-Windows

X-Windows

- Diverse X servers voor Windows/NT
  - PC-Xware (NCD)
  - Reflection X (WRQ)

Bevatten meestal ook andere features zoals betere telnet clients
  - Meer en betere terminal emulatie

Notities

De grafische omgeving van Windows/NT is helaas niet gebaseerd op het X-Windows systeem. Dat betekent onder andere dat het niet zomaar mogelijk is om programma's op één systeem te draaien en de gebruikers interactie op een ander systeem te beleggen. Er zijn wel software pakketten op de markt waarmee van een NT machine een X-Server (zeg maar, een X-terminal) kan worden gemaakt. Hiermee wordt het dan mogelijk om grafische programma's op een UNIX machine te laten lopen en de grafische interactie op een Windows/NT computer te verrichten. Voor Windows 3.x bestonden dergelijke applicaties ook al, maar door de zeer geringe stabiliteit en functionaliteit van Windows 3.x liep het daar vrijwel nooit goed. Er moet wel rekening mee worden gehouden dat je een flinke computer nodig hebt om naast het NT besturingssysteem ook nog eens een X-terminal na te doen! Naast veel geheugen en een zeer goede videokaart kan ook een groot scherm geen kwaad.

3.7 Printen

Printen

- lpd compatible printer service (LPDSVC)
  - Standaard onderdeel van NT
  - Printen vanaf UNIX naar NT printer (/usr/bin/lpr)
- Printen vanaf NT naar UNIX printer
  - lprmon (lpd protocol printer poort driver)
  - LPR.EXE

Notities

Één van de weinige UNIX/NT integratiemogelijkheden die standaard met Windows/NT wordt meegeleverd is voor het gebruiken en delen van printers. Met TCP/IP voor Windows/NT worden twee componenten meegeleverd waarmee een UNIX remote printer client en server kan worden geïmplementeerd (gebaseerd op het Berkeley lpd protocol).

Deze twee componenten zijn:

1. Een NT printer monitor (soort printer driver) die het mogelijk maakt om af te drukken naar een UNIX (Berkeley LPD compatbile) printer spooler. Hiermee kan dus een Windows/NT printer worden gedefinieerd die zijn uitvoer naar een UNIX printer spooler stuurt.
2. Een service de Berkeley LPD spooler nadoet. Hiermee worden alle printers die op de Windows/NT machine zijn gedefinieerd ook gedeeld als remote printer voor UNIX systemen.

Daarnaast worden er nog een tweetal commandoregel programma's meegeleverd (lpr.exe en lpq.exe) waarmee rechtstreeks kan worden geprint naar een remote UNIX printer.

3.8 NT op X-terminals

NT op X-terminals

- Multi User NT versies!
  - WinCenter (NCD)
  - NTrigue
- X-terminals als NT terminals
- Krachtige server nodig
  - Enkele MB per gebruiker plus MB voor applicatie

Notities

Een hele bijzondere ontwikkeling wordt gevormd door pogingen van derde partijen om van Windows/NT een multi user operating system te maken. Een aantal van deze oplossingen maken het mogelijk om X-terminals te gebruiken als grafische terminals voor een Windows/NT machine. Door in te grijpen in de Windows/NT kernel worden meerdere logon processen gestart en wordt de grafische I/O via het X-protocol verstuurd en ontvangen. Het aardige is dat Windows/NT intern wel meerdere zogenaamde Window Stations en Desktops ondersteunt, maar dat de uitgeleverde versie hier niet of nauwelijks gebruik van maakt.

Een groot voordeel van deze oplossing is dat het niet meer nodig is om een PC op je bureau te hebben voor het draaien van PC applicaties. Deze draaien dan immers op de NT machine (100user interactie naar de X-terminal. Nadelen van deze oplossing zijn dat je een behoorlijk zware NT machine nodig hebt om die meerdere gebruikers te ondersteunen, en dat er allerlei niet door Microsoft ondersteunde ingrepen in Windows/NT zijn gedaan om dit mogelijk te maken. In een aantal gevallen (Citrix, NTrigue) gaat het zelfs om leveranciers die een source licentie van Windows/NT hebben en die compleet eigen wijzigingen in de NT executive hebben aangebracht!

Microsoft heeft aangekondigd in toekomstige versies van Windows/NT dit soort features standaard te gaan ondersteunen.

3.9 Interprocess Communicatie

Interprocess Communicatie

- Netwerkverbindingen tussen NT en UNIX:
  - Sockets (Microsoft WinSock)
  - RPC
    - DCOM
    - Corba

Notities

Voor de integratie van UNIX en Windows/NT systemen is het natuurlijk van groot belang dat programmatuur die op een NT computer draait kan communiceren met programma's op een UNIX machine. De basis hiervoor wordt gevormd door de ondersteuning van een gemeenschappelijk netwerkprotocol: TCP/IP. Bovenop TCP/IP dient er echter nog een sessielaag te zijn geïmplementeerd die ook door beide systemen wordt begrepen.

Voor wat betreft het opzetten van netwerkverbindingen via TCP/IP heeft Microsoft (gelukkig) gekozen voor een API die vrijwel geheel identiek is aan de onder UNIX gebruikelijke Berkeley Sockets. Inclusief wat aanpassingen gaat dit interface door het leven onder de naam WinSock. De hoge mate van gelijkvormigheid tussen WinSock en de Berkeley sockets maken het ook (relatief) eenvoudig om TCP/IP programma's te porten van UNIX naar NT. Een verschil is nog wel dat in WinSock niet de read(), write() en close() functies kunnen worden gebruikt om sockets te lezen, schrijven en sluiten. Dit komt doordat in Windows/NT een socket handle niet vergelijkbaar is met een file handle. Het besturingssysteem kan op basis van een handle niet beslissen wat voor een handle het is. In plaats daarvan dient recv(), send() en closesocket() te worden gebruikt. Een ander verschil is dat niet alle versies van Microsoft TCP/IP (bijvoorbeeld die voor WfW) alle setsockopt() socket opties ondersteunen.

Een andere mogelijkheid voor interprocess communicatie tussen UNIX en NT

machines wordt gevormd door Remote Procedure Calls. Windows/NT ondersteunt zogenaamde Microsoft RPC's, welke zo goed als volledig compatibel zijn met DCE RPC's. Daar RPC's weer de basis zijn voor andere standaarden als CORBA is het mogelijk om heterogene gedistribueerde systemen te bouwen op basis van RPC's.

3.10 Beheer

Beheer

- Cross platform beheer
- SNMP agent op Windows/NT
  - Diverse MIBs
- Derde partij produkten:
  - HP IT Operations (NT agent)
  - IBM Tivoli
  - Bull Integrated System Management
  - Microsoft SMS (met vierde partij uitbreidingen!)

Notities

Een uitdaging voor heterogene UNIX/NT omgevingen is om het systeembeheer van alle systemen te consolideren en te centraliseren. Er zijn nogal wat verschillen tussen het beheren van UNIX en Windows/NT. *Zie ook bijlage B.*

Zowel in Windows/NT als in UNIX zitten zo goed als geen faciliteiten voor het integraal beheren van een heterogeen UNIX/NT netwerk. De enige hulp die Windows/NT ons hier nog biedt is de ondersteuning van een SNMP agent (met bijbehorende MIB's voor NT, WINS en DHCP) waarmee de status van een Windows/NT machine op afstand kan worden opgevraagd (bijvoorbeeld in combinatie met een op SNMP gebaseerde management applicatie zoals Sun NetManager of HP OpenView Network Node Manager). Alle andere wijsheid op het gebied van integraal beheer dient van derde partij applicaties te komen.

Op de slide staan voorbeelden van commerciële produkten waarmee het in meer of mindere mate mogelijk is om integraal systeembeheer te voeren. Daar de UNIX/NT beheerproblematiek nog tamelijk nieuw is zijn er eigenlijk nog geen "perfecte" oplossingen: alle pakketten kunnen wel wat, maar op de meeste valt nog wel wat aan te merken.

3.11 Diversen

Diversen

- Frutsels in het Public Domain:
  - TFTP Server
  - Telnet/rlogin daemon
  - GNU-WIN32
  - Perl

Notities

Vanzelfsprekend wordt er ook in het public domain aardig wat afgeknutseld. Er zijn inmiddels diverse Web sites waar shareware of public domain software voor Windows/NT kan worden afgehaald. Zo zijn er bijvoorbeeld flink wat (geslaagde) pogingen ondernomen om UNIX(-achtige) programmatuur naar Windows/NT te porten.

Hoofdstuk 4

Kanttekeningen en op- en aanmerkingen

4.1 Kanttekeningen en op- en aanmerkingen

Kanttekeningen en op- en aanmerkingen

Notities

In het laatste hoofdstuk van deze tutorial plaatsen we nog een aantal opmerkingen en kanttekeningen bij het Windows/NT besturingssysteem en de inzetbaarheid van NT.

4.2 Aandachtspunten

Aandachtspunten

- Programmeerbaarheid
- Schaalbaarheid
  - Diepte
  - Breedte
- Gemak
- Volwassenheid
- Dan dit...

Notities

Het is in UNIX land natuurlijk bon ton om alles wat van Microsoft afkomt integraal af te zinken. Soms (meestal?) is dit terecht, soms (vaak?) ook niet. Een organisatie die besluit om Windows/NT te implementeren dient zich echter terdege bewust te zijn van de werkelijke aard en inzetbaarheid van het OS. Op de slide ziet u een aantal aandachtspunten die in de komende secties nader zullen worden uiteengezet.

4.3 Programmeerbaarheid

Programmeerbaarheid

- Geen meegeleverde script taal
  - Diverse ter beschikking in public domain
- Geen C compiler meegeleverd
  - Is in veel UNIXen ook al niet meer zo
- Complexe WIN32 API's
- Complexe class libraries (MFC)
- Ondersteuning door goede tools (VC++, Delphi, Visual Basic)

Notities

Een groot verschil tussen UNIX en Windows/NT zit hem in de wijze waarop programma's kunnen en moeten worden ontwikkeld. UNIX is echt een besturingssysteem voor en door systeemprogrammeurs. Het is duidelijk de bedoeling dat de systeembeheerders zelf nog allerlei uitbreidingen realiseren met behulp van de in overvloed aanwezige halffabrikaten, een aantal krachtige script talen en eventueel met de (meestal nog) bijgeleverde C compiler.

In Windows/NT gaat het er geheel anders aan toe. Dit OS is bedoeld om "out of the box" te worden gebruikt, zonder dat er nog iets moet worden bijgeknutseld. Het schrijven van een beetje zinvolle programmatuur voor Windows/NT is alleen weggelegd voor professionele software ontwikkelaars. De ontwikkelomgeving (API's, class libraries) is ontstellend complex, zowel in opzet als in gebruik. Gelukkig zijn er voor weinig geld zeer goede ontwikkeltools op de markt zoals Visual C++ en Delphi. Deze tools verzachten het ontwikkelleed wel iets, maar vereisen zelf echter een zeer krachtige machines en zijn helaas ook niet altijd even gemakkelijk en doorzichtig in het gebruik. Het schrijven van een klein/simpel programmaatje is op Windows/NT eigenlijk niet mogelijk!

4.4 Schaalbaarheid I

Schaalbaarheid I

- Schaalt goed tot 4 a 5 processoren
- +/- 7.000 tpmC
- Minder dan $100,= per tpmC
- Clustering nog nauwelijks ondersteund

Notities

Over de schaalbaarheid van Windows/NT is nogal wat afgeschreven en gepraat. UNIX heeft zijn huidige schaalbaarheid pas bereikt na jaren rijpen en zorgvuldige ontwikkeling, dus het mag geen wonder heten dat Windows/NT (dat eigenlijk pas 4 jaar op de markt is!) nog lang niet op hetzelfde niveau is als UNIX. Een recent literatuuronderzoek van de Open Solution Providers heeft uitgewezen dat Windows/NT goed schaalt tot ongeveer vier processoren. Daarna neemt het grensnut van een extra processor dramatisch af. Tot en met die vier processoren schaalt het echter aardig goed, en biedt het zo ongeveer de laagste kosten per tpmC (een maateenheid voor het aantal transakties per minuut). Dit wordt natuurlijk hoofdzakelijk veroorzaakt door de enorme volumes die in de Intel markt kunnen worden gehaald.

UNIX systemen schalen veel verder, en halen daarom ook meer transakties per minuut in combinatie met geavanceerde server software zoals Oracle Parallel Server. Bedenk echter wel dat ongeveer 95bestaat uit systemen met minder dan 15.000 tpmC! In die markt heeft Windows/NT grote kansen!

Windows/NT ondersteunt momenteel nog nauwelijks enige vorm van clustering. Wel wordt hier door diverse leveranciers (onder aanvoering van Microsoft) heel hard aan gewerkt. De Microsoft specificatie op dit gebied (WolfPack) is al enige tijd in beta beschikbaar en is door diverse leveranciers (NCR, HP, CompaQ e.d.) omarmd. Windows/NT is echter (net als UNIX) van origine niet verzonnen

als een fault tolerant, clustering, operating system. Clustering features zullen moeten worden geleverd door extra OS componenten, wellicht in combinatie met ondersteuning van clustering in de applicaties.

4.5 Schaalbaarheid II

Schaalbaarheid II

- Grote NT netwerken nog moeilijk te realiseren:
  - File server gestoeld op oude (LAN) technologie
  - Beperkingen in "Trust" model
  - Beheer op afstand beperkt (geen telnet!)
  - Ondersteunende services nodig (WINS)

Notities

Alhoewel de huidige versie van Windows/NT wel allerlei mogelijkheden biedt voor gebruik in Wide Area Networks, kleven er nogal wat praktische bezwaren aan het breed inzetten van NT. De netwerktechnologie van NT (domains, NETBIOS, trusts) hebben hun oorsprong in LAN technologie en Microsoft is er naar ons inzicht niet geheel in geslaagd om die oudere technologie aan te passen voor het inzetten in grote netwerken.

Een voorbeeld hiervan is de selectie van welke domain controller een client gebruikt om de logon te valideren. De client doet om te beginnen een broadcast op het lokale LAN. Indien daar geen domain controller zit doet hij een query in de Windows Name Server (WINS) om de IP-adressen te achterhalen van de domain controllers van het logon domain. In het antwoord van de WINS server zitten maximaal 25 IP-adressen (waaronder altijd dat van de primary domain controller). Vervolgens stuurt de client naar alle (maximaal 25) domain controllers een logon pakketje. Met degene die het eerste antwoord wordt vervolgens de logon afgemaakt.

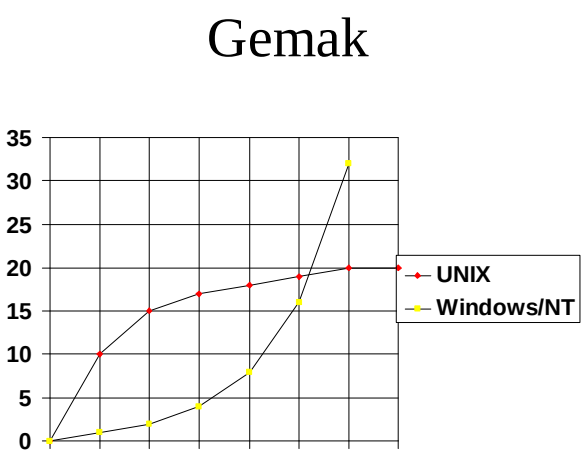
In een groot, gedistribueerd, netwerk met meer dan 25 domain controllers werkt deze procedure natuurlijk niet zo fijn [1]. Ook aan het mechanisme van trusts kleven een aantal bezwaren: het staat niet alle gewenste combinaties van cross

[1] The proof of this is left to the reader as an exercise

domain groepslidmaatschappen toe die in een groot netwerk gewenst zijn.

Voor het beheer op afstand is het vervelend dat niet alle NT beheerapplicaties een "remote mode" kennen. Windows/NT heeft standaard geen telnet daemon (wel in public domain), en de meeste NT beheercommando's kunnen toch niet vanaf de commandoregel worden uitgevoerd (het zijn meestal grafische applicaties). Ditprobleem kan worden verholpen door het implementeren van remote console software zoals "PC Anywhere" of "Carbon Copy 32".

4.6 Gemak



Notities

Wat wel een heel groot voordeel van Windows/NT is, is dat de drempel om iets met NT te gaan doen behoorlijk laag is. Kennis opgedaan met DOS, Windows 3.x of Windows 95 kan worden meegenomen naar Windows/NT (zoals bijvoorbeeld welke kant de directory scheider slash op wijst). UNIX kent daarentegen een hele hoge drempel.

Kort samengevat kun je stellen dat het in Windows/NT heel makkelijk is om iets makkelijks te doen (zoals het toevoegen van een gebruiker), maar heel moeilijk om iets moeilijks te doen (zoals het schrijven van een printer driver). In UNIX is het tamelijk moeilijk om iets makkelijks te doen, maar niet zo heel veel moeilijker om iets moeilijks te doen.

4.7 Volwassenheid

Volwassenheid

- Jong OS
- Nieuwe spectaculaire features worden nog regelmatig toegevoegd
- Service Pack strategie (jumbo-patch)

Notities

Tegen Windows/NT spreekt dat het een vrij jong OS is waar nog met de regelmaat van de klok significante wijzigingen (uitbreidingen) in geschieden. UNIX is wat dat betreft een stuk stabieler. Microsoft heeft ook nog weinig ervaring met het structureel uitbrengen van patches op een besturingssysteem. Fouten in Windows/NT worden opgelost door het periodiek uitbrengen van Service Pack. Zo'n service pack is in feite een mega patch die verbeterde of extra componenten op het besturingssysteem aanbrengt. Dergelijkse Service Packs zijn incrementeel: in SP3 zitten alle wijzigingen die ook in SP2 zitten. Recente ervaringen met dit principe zijn niet zo gunstig. Binnen drie weken na het uitkomen van SP3 op Windows/NT 4.0 waren er al weer vier "hot fixes" die fouten oplosten die door het service pack werden geïntroduceerd. Het terugdraaien van een Service Pack installatie is lang niet altijd mogelijk!

4.8 Dan dit ...

Dan dit nog...

- Microsoft Marketing Machine
- Zeer veel ondersteuning door derde partijen
- Ogenschijnlijk gemakkelijk opstap vanaf DOS, Win3X, W95
- 90% van de IT-branche bestaat uit eenvoudige problemen
- NT heeft lage instapdrempel!

Notities

Kort en goed kunnen we stellen dat de UNIX wereld Windows/NT natuurlijk niet kan negeren! De marketing machine van Microsoft is fenomenaal, en het is zeer opvallend dat features die al jaren in UNIX zitten uitbundig worden bejubeld als Microsoft aankondigt het ook in Windows/NT te gaan ondersteunen. De meeste Windows/NT componenten zijn door de bank genomen matig tot voldoende: zodra je een NT component nader bestudeert ben je meestal teleurgesteld, maar het is vrijwel altijd beter dan wat je hebt dus je bent toch blij.

De ondersteuning van Windows/NT door derde partijen is overweldigend. Vrijwel alle grote IT leveranciers ondersteunen Windows/NT, hetzij van harte (HP), hetzij plichtmatig (IBM). Slechts weinigen wijzen het totaal af (Sun). Met UNIX kunnen complexere omgevingen worden ingericht. De meeste klanten hebben echter eenvoudige omgevingen, en die zijn met Windows/NT heel eenvoudig vorm te geven! Met name de lage instapdrempel van Windows/NT verklaart volgens ons het succes. UNIX wordt toch nog door veel klanten als (te) moeilijk ervaren.

Bijlage A

A short course in Windows/NT domains

A.1 Domain

An NT domain is a logical grouping of network servers and workstations that have access to a common User Accounts Database (UAD). The members of a domain can be NT Servers, NT Workstations and reputedly OS/2 servers. Please note that DOS, Windows 3.x and Windows95 workstations are not members of a domain!

One NT server fullfills the role of the primary domain controller (PDC). This computers maintains the UAD for the entire domain. Changes to the UAD can only be made in the UAD that is maintained by the PDC. Several other NT servers can be assigned the task of backup domain controller (BDC). Upon installation the BDC receives a copy of the UAD of the PDC. Thereafter, the UAD's are synchronised across the network. Both the interval, frequency and speed of the synchronisation process can be parameterised through settings in the NT registry. All domain controllers answer userid/password queries sent to it by interested parties. Such interested parties can be other domain members or a 16/24 bit client (DOS, Windows 3.x, Windows 95).

Due to the synchronisation delay it can occur that the UAD of a domain controller contains outdated information. For instance, when users change their password, this change is implemented in the UAD of the PDC. If the user logs off and immediately logs on again it can happen that this second logon is validated by a backup domain controller that has not been synchronised yet. The user gets an 'invalid password' error. The NT Server Manager application contains an option to manually synchronise a BDC or the entire domain.

When the PDC fails the userid/password validation function is not impaired in any way as long as there are one or more BDC's online. However, as long as the PDC remains unavailable it is not possible to add, delete or change entries in the domain UAD. This means that all functions that need the PDC are unavailable. Apart from adding, deleting and changing users and groups this also includes

creating trusts, installing a new BDC or adding new member computers to the domain. As soon as the PDC comes online it resumes it's function.

The NT Server Manager application makes it possible to promote a backup domain controller to primary domain controller. There are basically two possibilities:

1. PDC is online
   In this case the PDC synchronises with the PDC-to-be, the BDC is promoted to PDC and the PDC is demoted to BDC.

2. PDC is offline
   In this case the BDC is promoted to PDC without the PDC knowing about it! This is usually done in case of an unexpected PDC failure which is reckoned to last some time. When the original PDC comes online again it 'sees' that it is no longer to PDC of the domain and it demotes itself to a halfway state from which it can be manually demoted to a BDC. Promoting a BDC to PDC with an offline original PDC can have severe implications for the integrity and content of the domain UAD. First of all there might be unsynchronised entries in the original PDC's UAD. These may never be synchronised to the other BDC's. Furthermore, depending on a few factors the old PDC when it comes back online might not figure out that another domain controller is now the PDC. You might end up with two PDC's in your domain! It is very important that the switch back to the original PDC is done in an orderly fashion.

The general recommendation for NT domains is to have at least one backup domain controller.

A.2 The User Accounts Database

Each NT computer has it's own User Accounts Database. This means that a domain made up of ten NT workstations, two member servers, a backup domain controller and a primary domain controller contains a grand total of fourteen User Accounts Databases! The UAD's of the PDC and BDC double as the domain UAD, so this adds up to a total of thirteen different UAD's (ten NTW UAD's, two NTS UAD's and the PDC/BDC UAD's which contain exactly the same data due to the intradomain UAD synchronisation).

When denoting a userid or group it is important to specify the UAD in which this userid/group is defined. So in our sample domain (MYDOM) we could have the following userid's: josv on NTW01, josv on NTW02, josv on NTS01 and josv in the domain UAD MYDOM. All those userid's, although seemingly belonging to the same person, are part of a different security context.

A UAD can contain the following entries:

- Userid
  The definition of a user of this computer/domain.

- Local group
  A logical grouping of users and global groups.
- Global group
  A logical grouping of domain users (*)
- Computer account
  The definition of a member computer of the domain. (*)
- Interdomain trust account
  The definition of a trusted or trusting domain. (*)
- User right
  A security definition stating which users and/or groups are allowed to perform a certain function on this computer.

The entries marked with (*) can only occur in a domain UAD, that is, the UAD of an NT server that functions as a domain controller.

An important fact is that apart from the user and group records, the UAD also contains the User Rights that pertain to a computer. This means that rights such as 'Shutdown the system', 'Logon interactively' and 'Change the system time' are stored in the UAD of a computer. Because the content of the UAD's of the domain controllers is identical this means that all domain controllers share the same set of users, groups and user rights! E.g.: the right to shutdown a domain controller automatically applies to all domain controllers!

A.3 Logging on to Windows/NT

There are four ways of logging on to a computer running Windows/NT:

1. Interactive logon
   An 'interactive logon' is performed by a user that logs on to an NT computer through the console and keyboard of the computer. It is governed by the 'Logon interactively' user right.
2. Network logon
   Clients connecting to an NT computer through the network perform a 'network logon' (also called 'remote logon'). The right to do so is checked through the 'Connect to this computer from the network' user right. Clients that want to use resources from this NT computer (NET USE) authenticate themselves by sending a userid and password with their request. The NT computer implicitly logs them on by checking the userid and password before verifying the resource access.
3. Service logon
   A 'service logon' is performed by programs that runs as an NT service (i.e., a background task under control of the NT service manager). This facility is secured by the 'Log on as a service' user right.

4. Batch job logon
   There is currently no standard facility in Windows/NT for running batch jobs. The LogonUser() call however supports a "batch job logon"mode which is authorised by the "Logon as a batch jobüser right.

When logging on to a domain controller there is no question about which UAD is used to validate the logon . A domain controller has no 'own' UAD, it's UAD is (a copy of) the domain UAD. When logging on to a member of the domain (an NT workstation or server), there are two UAD's that can be used to validate the logon request: the domain UAD and the computer's own UAD. Which UAD is used depends on the type of logon and the userid specified.

When logging on interactively the user at the console determines the UAD in which the logon will be verified. The Windows/NT logon box contains three fields: Userid, Password and From. The 'From' field is a drop down box that contains a list of the UAD's the user may logon to. Normally this list includes the computer's own UAD and the domain UAD.

When connecting to an NT computer from another computer through the network the Netlogon service of the NT computer forwards the logon validation to a domain controller. This forwarding of a logon request is called 'Pass-through authentication'. Network logons are therefore always validated by a domain controller, and not in the local UAD of the computer being connected to (unless the computer being connected to is a domain controller).

An NT service that logs uses the userid and password configured in the registry of the NT computer for this service. By specifying 'UAD
userid' the system administrator can influence the UAD used to validate the service logon (this has to be the local UAD or the UAD of the domain).

A.4 Sidestep: what about logging on from a 16/24-bit client?

Logging on from a 16/24-bit client from outside the domain (these clients are not members of a domain) is essentially a network logon. If a client is configured to perform a domain logon, the client OS contacts a domain controller to have the userid and password of the user verified. In case a logon scripts has been specified this is sent to the client for execution. When using resources in the domain, the client sends the userid and password of the user with each new connection to a new server, thereby executing a 'network logon'. 16/24-bit clients can not logon interactively or logon as a service. Therefore, they always use the domain UAD.

A.5 Global and local groups

Windows/NT supports the use of groups to pool users together for easy granting and revoking of permissions. In a domain context, two different kind of groups can be created:

1. Global groups
   A global group can only be created in the domain UAD. It's members are users from the domain UAD.

2. Local groups
   Local groups can be created in any UAD. It's members can be

   (a) Local users (defined in the local UAD)

   (b) Domain users (defined in the domain UAD)

   (c) Global groups from the local domain (also defined in the domain UAD)

This means that to a certain extent, Windows/NT allows groups to be members of other groups! More specifically, a global group in a domain can be a member of a local group on any member of the domain. Hence the name 'global group', the group definition is valid throughout the entire domain.

Likewise, an NT access control list (or user right permission list) of an NT computer in a domain can contain:

1. Local users

2. Local groups

3. Domain users

4. Global groups from the local domain

Global groups are a powerfull way of centralizing the security management in an NT domain!

A.6 User Rights

One of the more exotic aspects of Windows/NT security is that user rights are always checked in the UAD of the local NT computer! This means that when a user logs on to an NT workstation with his/her domain userid, the right to logon interactively is still checked in the local UAD! To give a user permission to logon to any NT computer in the domain would require the system administrator to give the user the 'logon interactively' right on each and every NT computer!

Fortunately this 'problem' can be solved elegantly through global groups. The administrator can create a global group called 'Interactive Users' in the domain UAD. This global group can then be given the 'logon interactively' user right on every NT computer. Then, by managing the membership of the 'Interactive Users' group can the administrator grant and revoke the permission to logon to the NT computers in the domain.

A.7 Why we need trusts

Domains are an excellent tool to centralise the (security) management of a group of NT computers. The domain gives us a tool to create a user on one computer (the PDC), but still allow him/her to access resources throughout the entire domain based on that one security definition. However, problems may arise as soon as we create multiple domains (for reasons of network connectivity or systems management). Each domain has it's own domain UAD, and therefore it's own users and global groups. A user that needs to access resources in more than one domain must have a userid in each domain! Furthermore it is usually nescessary for all those to userid's to have the same password!

Suppose we have two domains, DOM1 and DOM2, and a user wants to access resources in both domains. First, the user logs on to DOM1, her 'home' domain. The domain controllers in DOM1 validate the logon and as this user accesses resources, the servers in DOM1 forward the authentication requests (due to the network logon) to the domain controllers in DOM1. Now, when the user accesses a resource of a server in DOM2, this server will forward the network logon to a domain controller in DOM2. This domain controller recognises that the userid belongs to someone from DOM1 (the format of the userid is DOM1 id), but still uses it's own UAD (the domain UAD of DOM2) to verify and validate the userid and password. If the userid of our user does not exist in the domain UAD of DOM2 (or has a different password), the logon is rejected or the user is given 'guest' access (depending on the type of the error and the configuration of the servers in DOM2).

In a large multidomain network where some or all users must be able to access resources throughout the entire network this situation is not acceptable.

A.8 Trust

Microsofts solution to this problem is called trust. An NT domain can be configured to explictly trust another domain. This trust relationship enables the domain controller of the trusting domain to forward a validation request to a domain controller of the trusted domain (another example of pass-through authentication). In the example of the previous section, we could have configured a trust from DOM2 to DOM1. In this case, the domain controller of DOM2 that receives the logon validation request from a server in DOM2 would have relayed the request to a domain controller of DOM1. The user would have only needed a userid in DOM1 to access resources in DOM1 and DOM2!

Trusts are reflexive, non-transitive, one-way relationships.

Reflexive
Every domain trusts itself. There is an implicit trust between an NT computer and it's domain controllers.

Non-transitive
A domain does not implictly trusts domains that are trusted by it's trusted domain. If DOM-A trusts DOM-B, and DOM-B trusts DOM-C, DOM-A does

not nescessarily trust DOM-C.

One-way
If DOM-A trusts DOM-B it does not automatically follow that DOM-B also trusts DOM-A.

In a trust environment the userids and global groups of a trusted domain become available in the trusting domain. This means that local groups in the trusting domain can contain users and global groups of both the local domain and all trusted domains! Likewise, an access control list in a trusting domain can refer to users and groups from trusted domains!

A.9 Domain models

The possibility of creating trust relationships between domains has led to four models of structuring domains in which users are created only once, but are visible throughout the entire network (in all domains). These models are:

1. The single domain model
2. The master domain model
3. The multiple master domain model
4. The complete trust model

In the 'single domain model' the entire network consists of only one domain. This model is off course unsuitable for larger environments with a lot of users and locations.

In the 'master domain model' a special domain is created to hold all the userids in the entire organisation. This domain is called the 'Master domain' or account domain. The other domains (that contain the actual network servers and NT workstations) are called the resource domains. A trust relationship is created from all resource domains to the master domain (not vice versa!). Users are created only in the master domain. The resource domains (although fully capable to do so) contain no local userids (apart from a few built-in and service ids).

Because of the trust relationship, the master domain users and global groups are available in all domains. The resource domain administrators can create local groups and access control lists that refer to the global groups and users of the master domain. With this model it is possible to grant and revoke permissions by manipulating global group memberships in the master domain.

A disadvantage of this model is that it only suffices for 'small' organisations. An NT UAD can only hold about 40.000 entries. The number of trust relationships needed is the same as the number of resource domains.

Larger organisations might need the 'multiple master domain model'. In this model we have several master domains whose only task it is to contain userids

and global groups. A master domain in this model trusts all other master domains, and is trusted by all resource domains. A userid or global group defined in a master domain is available in all other domains (because of the trust relationships). The complexity of implementing centralised security management in this model is slightly higher then in the single master domain case, but the multiple master domain model has no inherent upper boundary in the number of users it supports. By adding master domains we can accommodate any number of users. For instance, we could create master domains based on geographic distinctions (e.g. continent). The number of trusts needed is considerably larger then in the single master domain model, but still manageable.

In the 'complete trust' model we create a number of domains, each holding its 'own' users and groups and trusting all other domains. This model is suited for organisation without central user and security management but with stringent demands that all users and groups must be available in all domains.

Bijlage B

Systeembeheer: UNIX vs Windows/NT

Bijgevoegde artikel is weergegeven met vriendelijke toestemming van uitgeverij Array Publications B.V.