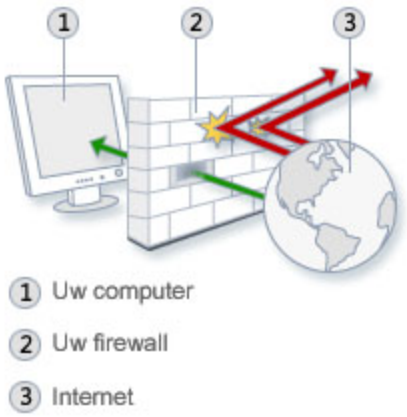
Labo Windows: Opdracht 09: Beveiliging en Schijfbeheer

Achtergrond

Windows Firewall

Een firewall is software of hardware die informatie die van internet of een netwerk binnenkomt, controleert en deze informatie vervolgens blokkeert of naar uw computer doorlaat, al naar gelang de firewallinstellingen. De naam firewall is goed gekozen: deze vormt een echte barrière/muur tussen jouw computer en de rest van het netwerk.



Figuur: Net als een stenen muur een fysieke barrière kan opwerpen, wordt tussen internet en uw computer een barrière gecreëerd met een firewall

Onder de naam “Internet Connection Firewall” werd bij Windows XP (oktober 2001) een firewall geleverd, doch stond deze standaard uitgeschakeld. Nadat in 2003 de Blaster worm en vervolgens de Sasser worm heel wat schade berokkenden besloot Microsoft om deze te verbeteren. Onder de naam “Windows Firewall” werd deze vernieuwde versie mee met Windows XP Service Pack 2, alsook Windows Server 2003, geleverd.

Een volwaardige Firewall was de Windows Firewall in Windows XP echter niet: deze blokkeerde enkel inkomende connecties. Bij de release van Windows Vista werd de Windows Firewall sterk verbeterd; Belangrijkste wijziging was dat deze nu ook uitgaande connecties kan blokkeren.

Logboeken

Gebeurtenislogboeken zijn speciale bestanden waarin belangrijke gebeurtenissen op de computer worden vastgelegd, zoals wanneer een gebruiker zich aanmeldt bij de computer of wanneer er een fout optreedt in een programma. Wanneer dergelijke gebeurtenissen zich voordoen, wordt de gebeurtenis in Windows vastgelegd in een gebeurtenislogboek die je kan lezen met Logboeken. Voor ervaren gebruikers kunnen de details in gebeurtenislogboeken nuttig zijn bij het oplossen van problemen in Windows en andere programma's.

Met Logboeken worden gegevens in verschillende logboeken gevolgd. Windows-logboeken bevatten:

1. **Toepassings-/programmagebeurtenissen.** Gebeurtenissen worden geclassificeerd als fout, waarschuwing of informatie, afhankelijk van de ernst van de gebeurtenis. Een fout is een ernstig probleem, zoals het verlies van gegevens. Een waarschuwing is een gebeurtenis die niet per se ernstig hoeft te zijn, maar wel kan wijzen om een mogelijk probleem in de toekomst. In een informatiegebeurtenis wordt de succesvolle bewerking van een programma, stuurprogramma of service beschreven.

2. **Beveiligingsgerelateerde gebeurtenissen.** Deze gebeurtenissen worden controles genoemd en worden beschreven als geslaagd of mislukt, afhankelijk van de gebeurtenis, bijvoorbeeld of een gebruiker zich al dan niet heeft kunnen aanmelden bij Windows.

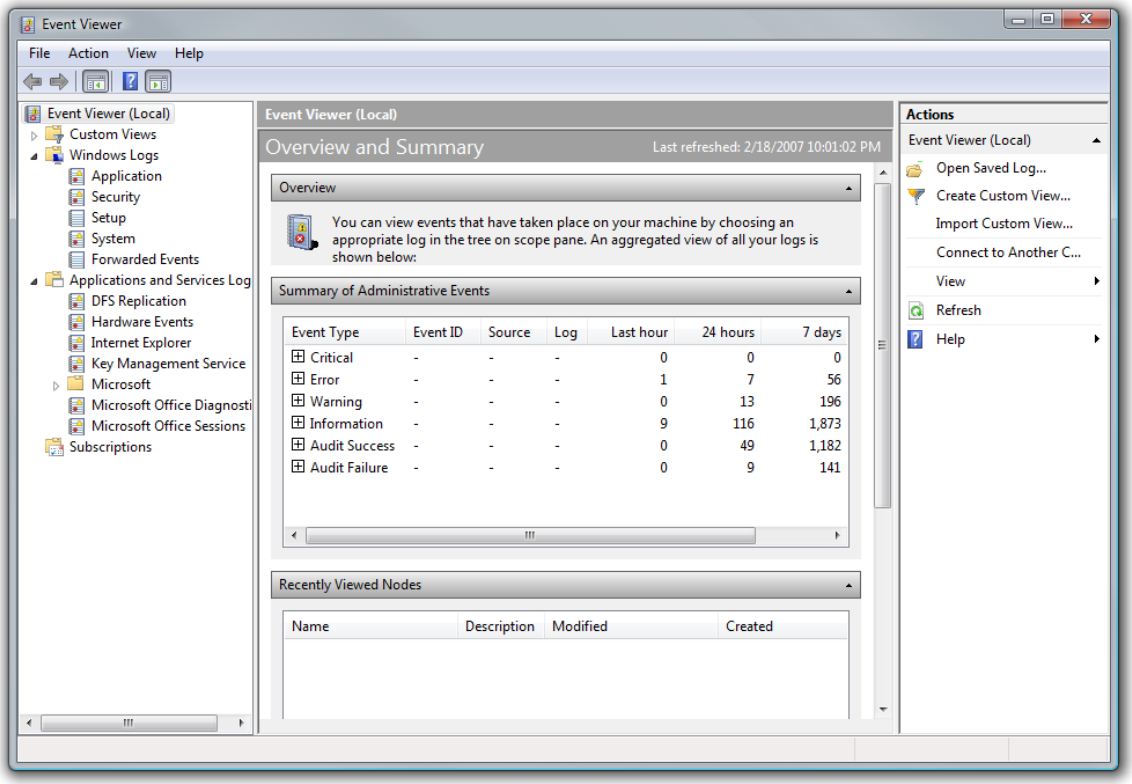
3. **Instellingsgebeurtenissen.** Voor computers die zijn geconfigureerd als domeincontrollers, worden hier aanvullende logboeken weergegeven.

4. **Systeemgebeurtenissen.** Systeemgebeurtenissen worden aan logboeken toegevoegd door Windows en Windows-systeemservices en ze worden geclassificeerd als fout, waarschuwing of informatie.

5. **Doorgestuurde gebeurtenissen.** Deze gebeurtenissen worden door andere computers naar dit logboek doorgestuurd.

Toepassings- en servicelogboeken verschillen. Ze bevatten afzonderlijke logboeken over de programma's die op de computer worden uitgevoerd alsmede gedetailleerdere logboeken die betrekking hebben op specifieke Windows-services.

De logboeken kan je bekijken met de bij Windows meegeleverde Event Viewer



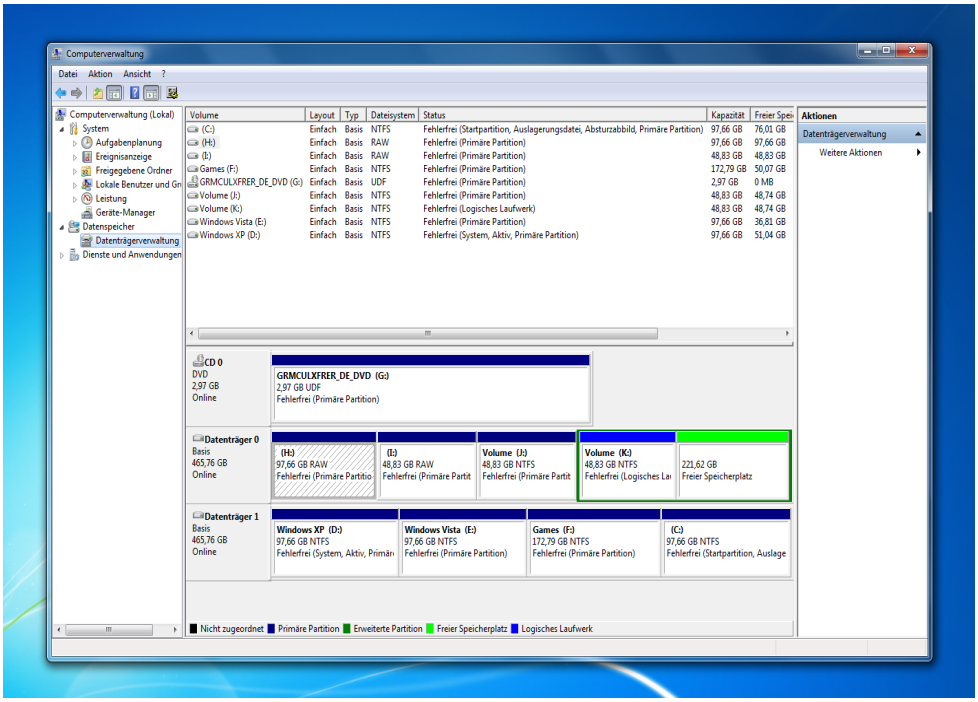
Figuur: Windows Event Viewer

Schijfbeheer

Eén van de tools bij Windows geleverd is Schijfbeheer (Disk Manager). Deze stelt je in staat om de schijven gekoppeld aan jouw computer, de partities en de logische stations te beheren.

Schijfbeheer kan je op twee manieren opstarten:

1. Via het configuratiescherm:
    a. Zorg er voor dat je als Administrator aangemeld bent.
    b. Klik op Start en klik op Configuratiescherm.
    c. Klik op Prestaties en onderhoud , klik op Systeembeheer en klik op Computerbeheer. Klik in de consolestructuur op Schijfbeheer.
2. Via het uitvoeren menu:
    a. Zorg er voor dat je als Administrator aangemeld bent.
    b. Klik op start Start > Uitvoeren en vul `compmgmt.msc` en bevestig met enter.
    c. Klik op schijfbeheer in de navigatie in de linkerkolom.



Figuur: Schijfbeheer in een Windows7 omgeving

Partities en Logische Stations

Een partitie, soms ook een volume genoemd, is een gebied op een vaste schijf dat kan worden geformatteerd met een bestandssysteem en kan worden aangeduid met een letter uit het alfabet. Station C is bijvoorbeeld op de meeste Windows-computers een partitie.

Als u in deze versie van Windows met Schijfbeheer, een module van MMC (Microsoft Management Console), partities maakt op een standaardschijf, zijn de eerste drie partities die u maakt primaire partities. Daarmee kunt een besturingssysteem opstarten. Als u meer dan drie partities wilt maken, wordt de vierde partitie gemaakt als een uitgebreide partitie.

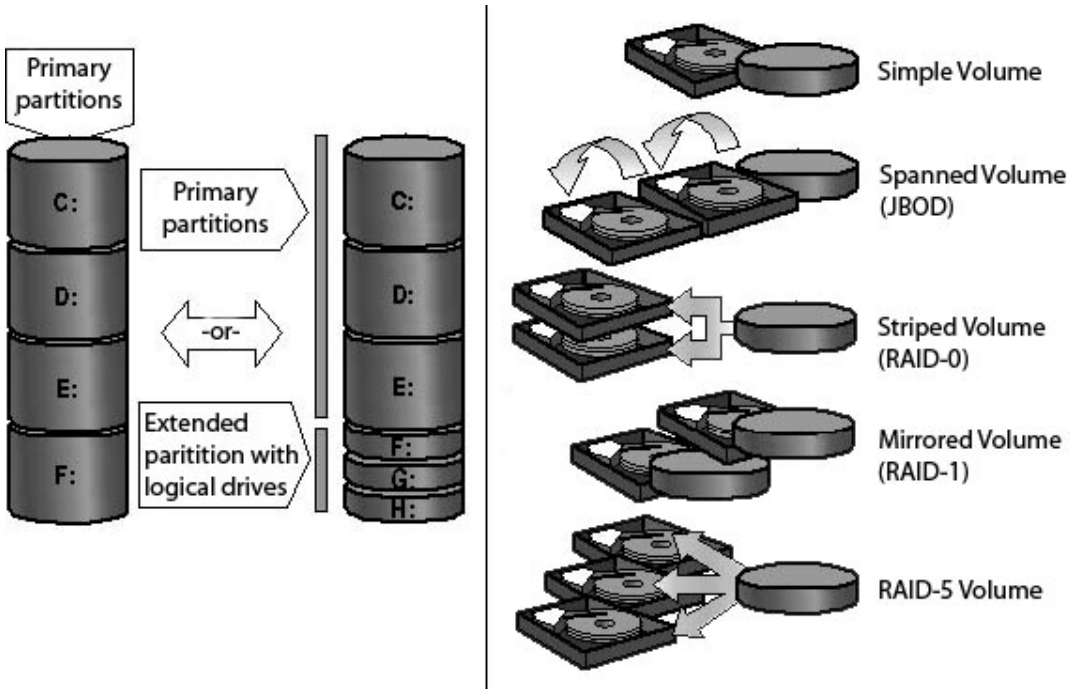
Met een uitgebreide partitie kunt u de limiet voor het aantal primaire partities op een standaardschijf omzeilen. Een uitgebreide partitie kan een of meer logische stations bevatten. Logische stations werken net als primaire partities. Het enige verschil met een primaire partitie is dat logische stations niet kunnen worden gebruikt om een besturingssysteem te starten.

Een vaste schijf moet worden gepartitioneerd en geformatteerd voordat u op de schijf gegevens kunt opslaan. Veel computers zijn gepartitioneerd als één partitie die even groot is als de gehele vaste schijf. Het partitioneren van een vaste schijf in verscheidene kleinere partities is niet verplicht, maar kan handig zijn voor het ordenen van gegevens op de vaste schijf. Sommige gebruikers prefereren afzonderlijke partities voor het

Windows-besturingssysteem, programma's en persoonlijk gegevens.

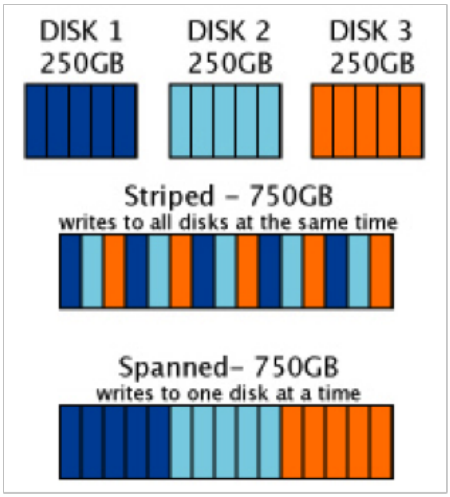
Standaardschijven en Dynamische Schijven

Een standaardschijf kan primaire partities, uitgebreide partities en logische stations bevatten voor het ordenen van gegevens. Een geformatteerde partitie wordt ook wel een volume genoemd (de termen 'volume' en 'partitie' worden vaak door elkaar gebruikt). In Windows 7 kunnen standaardschijven vier primaire partities of drie primaire partities en één uitgebreide partitie bevatten. De uitgebreide partitie kan meerdere logische stations bevatten (er worden maximaal 128 logische stations ondersteund). Op een standaardschijf kunnen geen gegevens worden gedeeld door meerdere partities of worden verdeeld over meerdere partities. Elke partitie op een standaardschijf is een afzonderlijke entiteit op de schijf.



Figuur: standaardschijven (links) vs dynamische schijven (rechts)

Dynamische stations kunnen een groot aantal dynamische volumes bevatten (ongeveer 2000) die als de primaire partities functioneren die op basisstations worden gebruikt. In sommige versies van Windows kan je afzonderlijke dynamische vaste schijven combineren in één enkel dynamisch volume (spanning of JBOD *(Just a Bunch Of Disks)* genaamd), gegevens tussen verschillende vaste schijven splitsen (striping of RAID 0 genaamd) voor hogere prestaties, of gegevens tussen verschillende vaste schijven dupliceren (mirroring of RAID 1 genaamd) voor meer betrouwbaarheid.



Figuur: Striped (RAID 0) vs. Spanning (JBOD) volumes.

De edities Windows Vista Ultimate en Windows Vista Enterprise ondersteunen spanning en striping van dynamische stations, maar niet mirroring (Windows Server 2008 ondersteunt mirroring).

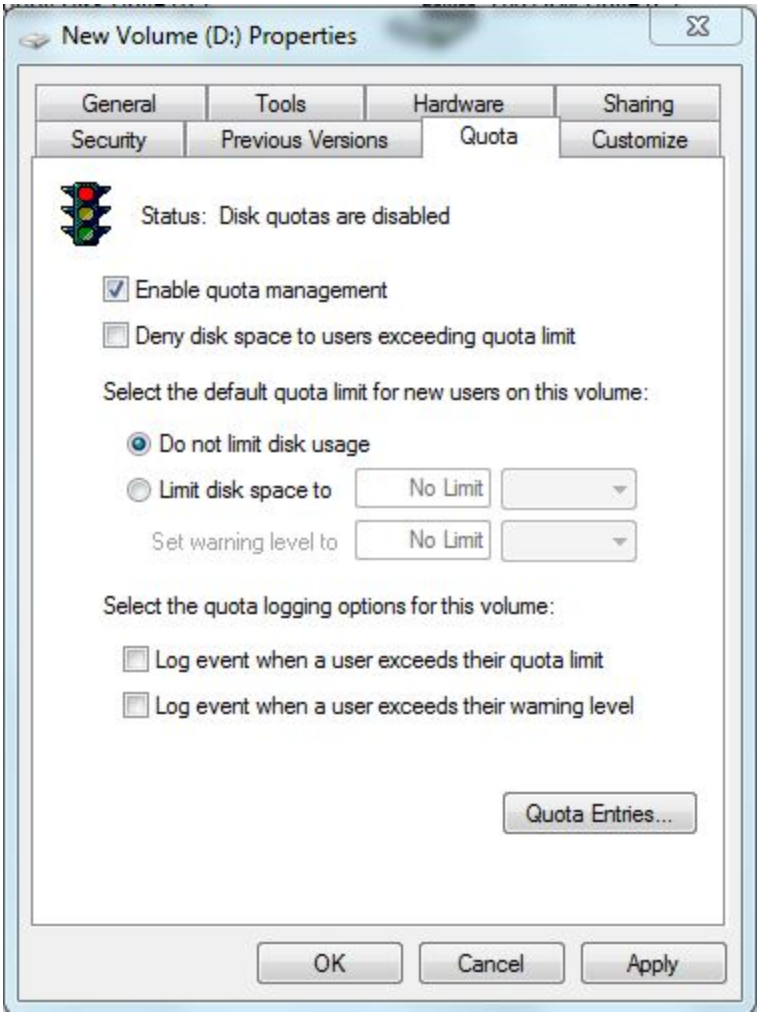
Quotumbeheer

Disk Quotas laten Administrators toe om het gebruik aan schijfruimte per gebruiker of groep van gebruikers op een volume te beperken.

Disk quotas kan je enkel op NTFS volumes instellen en zijn gebaseerd op file ownership: neemt een andere gebruiker het eigenaarsrecht van een bestand over, dan zal de originele zijn verbruik verkleinen en de nieuwe eigenaar zijn verbruik toenemen.

Je kan kiezen om bij het overschrijden dit enkel te loggen en de gebruiker verder schijfruimte laten innemen, of meteen de gebruiker weigeren om meer schijfruimte in beslag te nemen.

Disk Quotas stel je in via het tabblad Quota in het eigenschappenvenster van een volume.



Figuur: Quotum instellen.

Labo Gedeelte

Doelstellingen

- Een nieuwe harde schijf kunnen installeren
- Gebruikersquota kunnen beheren
- Kunnen werken met dynamische schijven
- De veiligheid van Windows kunnen verhogen

Opgaven

9.1 Windows Firewall

1. Pas de Windows-firewall aan en voeg een nieuwe regel toe. Blokkeer uitgaand verkeer op poort 80, schakel hiervoor eerst de firewall in via services. Test dit in een browser en verwijder nadien de toegevoegde regel.

2. Welk commando gebruik je om de firewall vanaf de command line te bedienen?
3. Wat is er veranderd, naast het filteren/blokkeren van uitgaande connecties, in de Windows Firewall sinds Windows Vista?
4. Probeer te weten te komen welke services luisteren op welke poorten met behulp van het `netstat` commando. Welke schakelopties heb je hiervoor gebruikt?

9.2 Logboeken

1. Open de Logboeken via computerbeheer.
2. Ga na wat er respectievelijk gelogd wordt in Systeem, Beveiliging en Toepassing.
3. Volgens welke drie types worden de gebeurtenissen gelogd ?
4. Bewaar het beveiligingslog in een bestand, wis daarna alle gebeurtenissen.
5. Gebruik de filter om enkel fout-gebeurtenissen te zien.
6. Stel de max. grootte van de logboeken in op 2048 kB.
7. Start `gpedit.msc` via uitvoeren en navigeer naar Computerconfiguratie > Windows-instellingen > Beveiligingsinstellingen > Lokaal beleid > Controlebeleid.
   Stel daar het juiste item in zodat Aanmeldingen geregistreerd worden in het beveiligingslogboek. Test dit uit door af en aan te melden.

9.3 Schijfbeheer

1. Sluit je VM af en voeg een extra nieuwe harde schijf toe, controleer of de optie “Allocate Disk Space Now” uitstaat.
2. Start uw virtuele Windows op en meld je aan als beheerder.
3. Open computerbeheer en selecteer vervolgens schijfbeheer, kies bij de wizard (met MBR) enkel voor initialiseren, niet voor converteren.
4. Maak een nieuwe primaire partitie (volume) aan (volumenaam: V1, 500MB, NTFS, N:).
5. Creëer een tweede primaire partitie op de overgebleven vrije ruimte (V2, FAT32, O:).
6. Wijzig achteraf de stationsaanduiding van V2 naar P:
7. Maak een tekstbestand aan in V2 (tekst.txt), kan ik er rechten aan toe kennen?
8. Converteer V2 naar NTFS via de opdrachtprompt. Welk commando heb je gebruikt?
9. Bestaat tekst.txt nog en kan ik er nu rechten aan toekennen?

9.4 Quotumbeheer

1. Maak twee nieuwe gebruikers aan in uw virtuele Windows, 1 Administrator en 1 gebruiker met beperkte rechten.
2. Beperk de schijfruimte voor alle gebruikers op N: tot 5 MB.
3. Zorg dat er een waarschuwing optreedt als 90 procent bezet is.
4. Test deze limieten uit en bekijk als administrator de logboeken. Zorg hiervoor dat de gebeurtenissen geregistreerd worden.
5. Gelden deze limieten ook voor de Administrators?
6. Test zowel een zachte en harde limiet uit, wat is het verschil?
7. Stel een quotum in voor slechts één gebruiker, test deze uit en bekijk terug de logboeken.

9.5 Dynamische Schijven

1. Sluit uw virtuele Windows af en voeg drie nieuwe schijven toe van 4GB (SCSI), controleer daarbij telkens of de optie “Allocate Disk Space Now” uitstaat.
2. Start Windows op en initialiseer de nieuwe schijven schijven.
3. Maak een eenvoudig, spanned en striped volume aan en test telkens de grootte en mogelijke uitbreiding:
    a. een eenvoudig volume van 1GB op de eerste SCSI-schijf
    b. een spanned volume van 6GB verdeeld over de 3 SCSI-schijven (3x 2GB, instellen per schijf !)
    c. een striped volume van 3GB verdeeld over de 2de en 3de SCSI-schijf (2x 1,5GB)
4. Breid achteraf het spanned volume uit met 1GB.

Bronnen

- http://windows.microsoft.com/nl-BE/windows7/What-is-a-firewall
- http://en.wikipedia.org/wiki/Windows_Firewall
- http://windows.microsoft.com/nl-BE/windows7/What-information-appears-in-event-logs-Event-Viewer
- http://en.wikipedia.org/wiki/Event_Viewer
- http://windows.microsoft.com/nl-BE/windows-vista/What-are-partitions-and-logical-drives
- http://windows.microsoft.com/nl-BE/windows-vista/What-are-basic-and-dynamic-disks
- http://support.microsoft.com/kb/183322