VDAB
TRAINING & OPLEIDING

Samen sterk voor werk

Windows Server Administration

Serverbeheer

Inhoud

1 INLEIDING

In deze module worden een aantal in Windows Server ingebouwde tools besproken die je kunnen helpen om

- een systeem vanop afstand te benaderen
- de belasting van een systeem op te volgen
- nakende problemen te ontdekken
- problemen op te lossen

2 REMOTE DESKTOP

Zoals vermeld in het onderdeel “Opzetten van een domein” zal in de praktijk een Server dikwijls draaien op een toestel dat zich ergens in een rack in een serverruimte bevindt of in de cloud. Het beheer van de server gebeurt dan ook grotendeels of volledig remote vanop een client toestel.

Remote desktop is één van de middelen die daarvoor ter beschikking zijn.

2.1.1 Wat is remote desktop?

Remote desktop zorgt er enerzijds voor dat de grafische interface van een ander Windows systeem, het remote systeem, via het netwerk getoond kan worden op het lokale systeem. Anderzijds worden handelingen op het toetsenbord of met de muis van de lokale machine doorgestuurd naar het remote systeem. Ook een printer verbonden met het lokale systeem of een harde schijf van het lokale systeem kunnen tijdens de verbinding ter beschikking gesteld worden van het remote systeem.

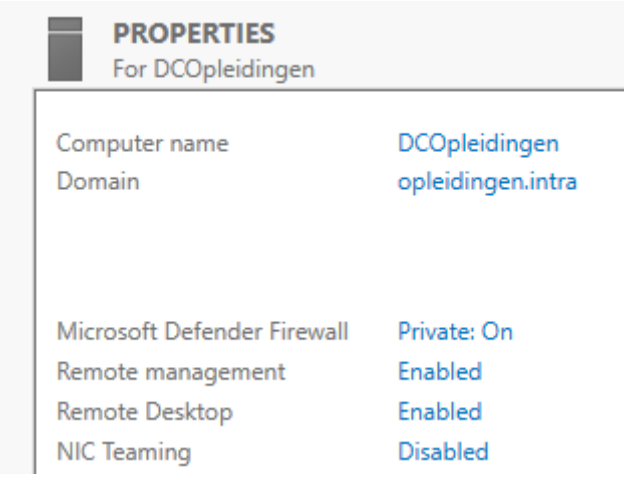
Een verbinding kan zowel tot stand gebracht worden over een WAN, een LAN als over het Internet.

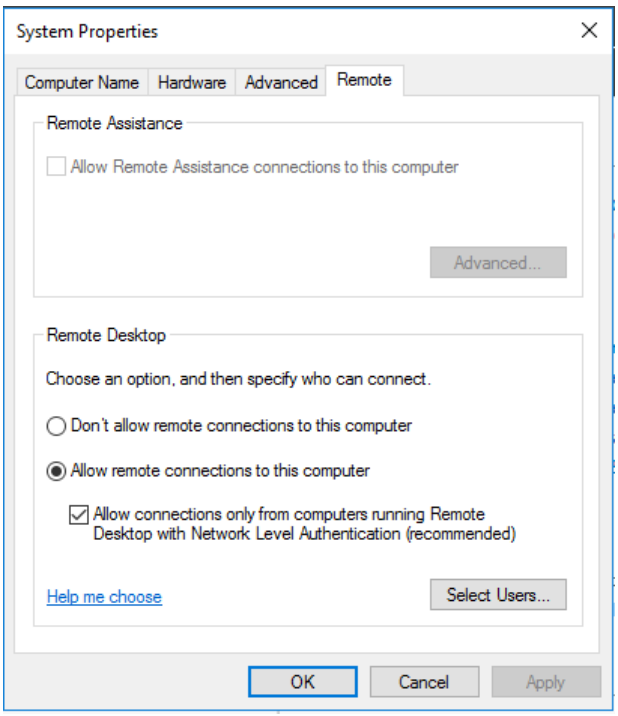
Op het remote systeem moet daartoe de service Remote Desktop services (TermService) draaien, op het lokale systeem de Remote Desktop Connection (RDC) client.

2.1.2 Remote desktop activeren op de remote server

Al wordt de remote desktop functionaliteit op de server geleverd via Terminal services, toch moet deze service niet expliciet geactiveerd worden om de server te kunnen beheren via remote desktop. Het volstaat “Remote destop” te activeren op de server die je vanop afstand wenst te beheren.

Dit kan via het dashboard van de Server Manager





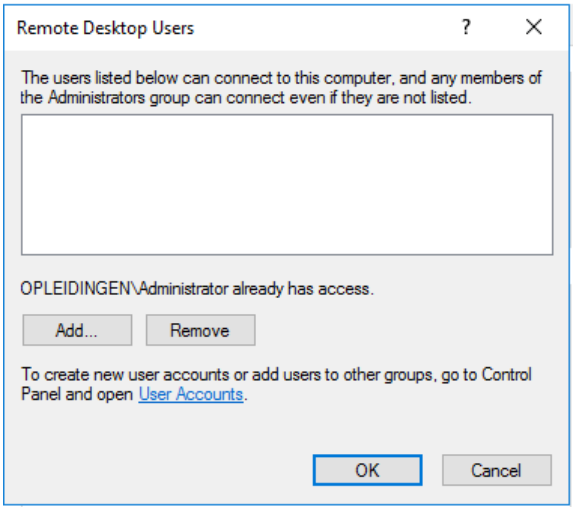
Standaard is de optie **Don't allow connections to this computer** geactiveerd.

De tweede optie, **Allow remote connections to this computer,** staat connecties toe via eender welke versie van de remote desktop client.

De bijkomende instelling **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended),** is veiliger en laat alleen connecties toe via remote desktop clients die Network Level Authentication ondersteunen. In de praktijk geldt dit voor clients vanaf Vista en voor servers vanaf Windows Server 2008.

Het toelaten van van Remote desktop verbindingen zal er meteen ook voor zorgen dat de firewall een uitzondering maakt voor het remote desktop protocol (RDP) en verkeer doorlaat op TCP poort 3389.

Standaard heeft de Administrator account vanzelf het recht om een connectie te leggen. Als er ook andere accounts zijn die een verbinding moeten kunnen leggen dan kunnen die gedefinieerd worden via de knop **Select Users**.



De knop **Add** laat toe ook andere gebruikers te selecteren.

Opmerkingen

Indien een gebruiker geen administratorrechten heeft en toch een verbinding moet kunnen leggen met een domeincontroller, dan moet die gebruiker ook nog het recht **log on through terminals services** krijgen op die domeincontroller.

Een verbinding maken met een computer die in slaap of hibernate mode is kan niet. Zorg er dus voor dat de instellingen van het power plan zo zijn dat de computer nooit in die mode terecht komt.

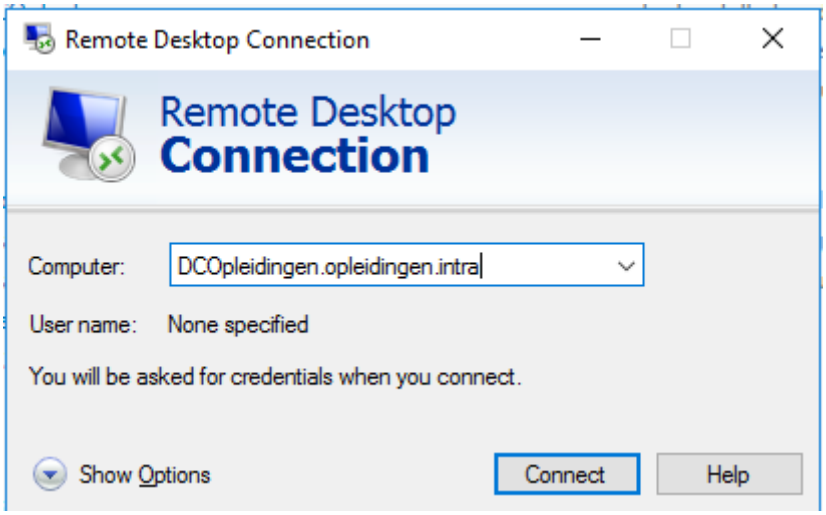
2.1.3 Een verbinding maken vanop een client

Start / Search > Remote Destop Connection

Of

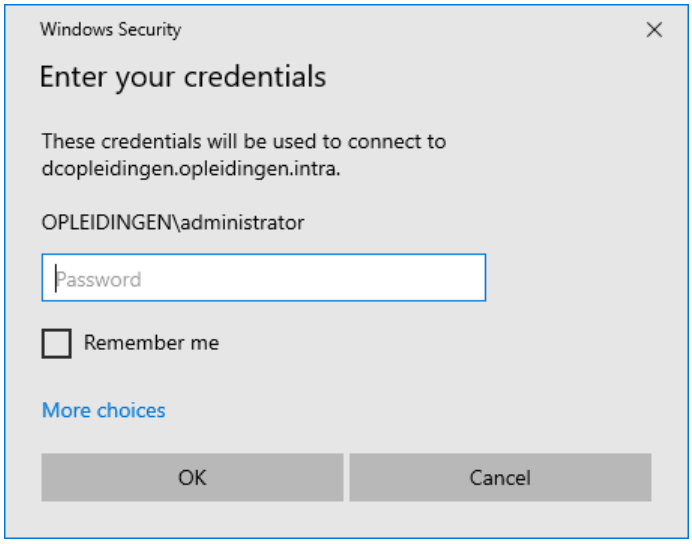
Typ **mstsc** in het vak **Search** van het startmenu.

Er verschijnt een venster dat vraagt met welke computer je een verbinding wenst te maken.



In het vak **Computer** kan je ofwel de naam van de remote computer typen ofwel zijn IP-adres.

- Klik op **Connect**. Het systeem vraagt met welke accountgegevens de verbinding zal gemaakt worden.

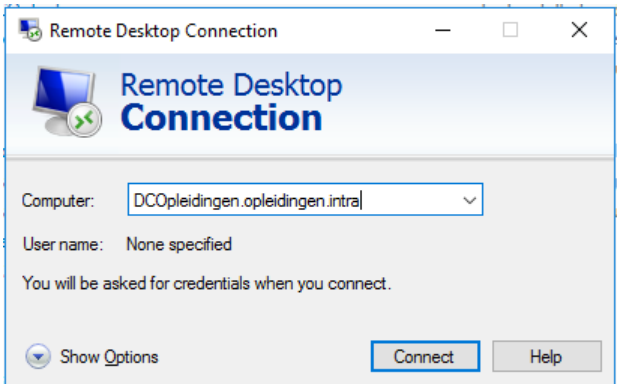


- Vul de accountgegevens in van de gebruiker die de connectie zal maken.
  Als dit de op de client aangemelde gebruiker is, volstaat het het wachtwoord in te vullen.
  Klik op **More choices** en dan **Use a different account** om de verbinding te maken met de credentials van een andere gebruiker.

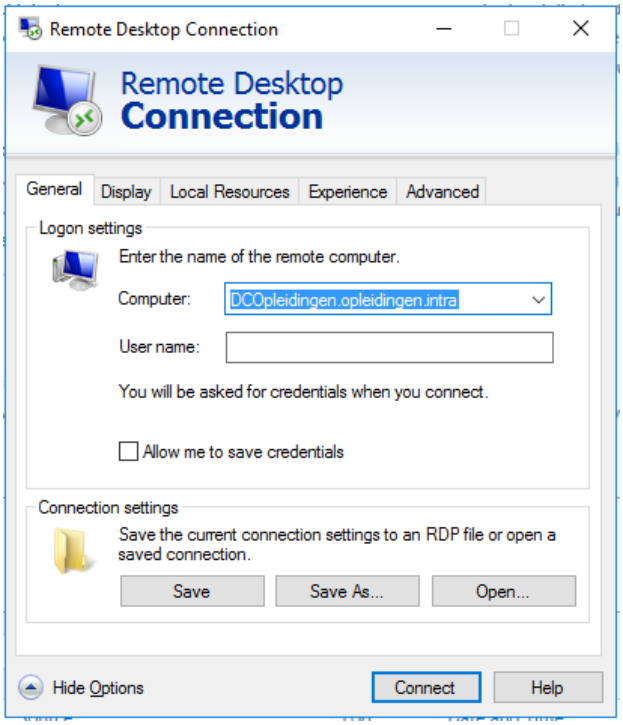
Een beetje later verschijnt de desktop van de server op het lokale computerscherm.

2.1.4 Bijkomende configuratie opties

De knop **Show Options** opent een dialoogvenster met 6 tabbladen om bijkomende instellingen mee te geven.

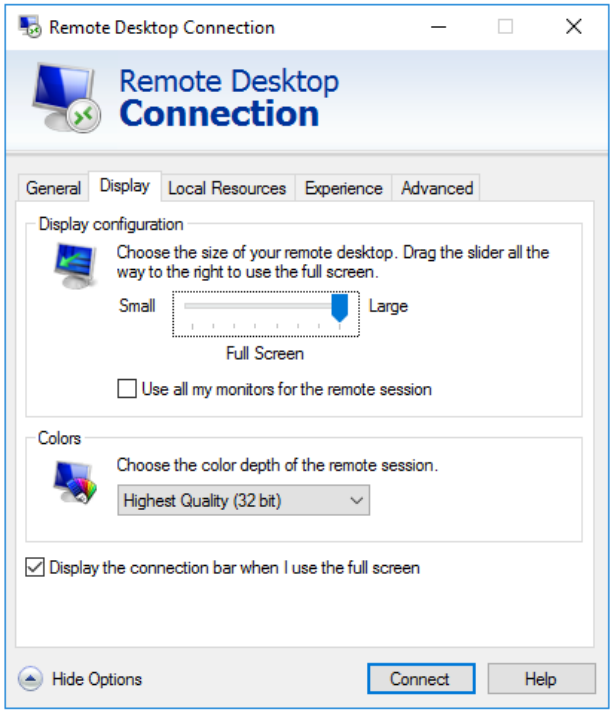


Op het eerste tabblad, het tabblad **General**, kunnen login gegevens en informatie i.v.m. de sessie meegegeven worden.

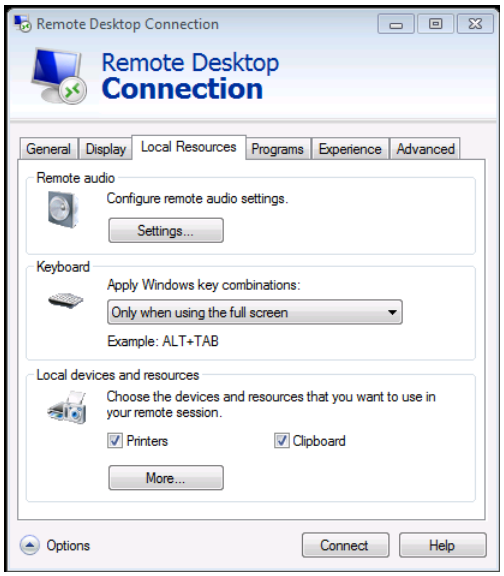


Via de knoppen **Save** en **Save as** kunnen de instellingen van een connectie opgeslagen worden in een .rdp bestand. Via de knop **Open** kan dan bij een volgende gelegenheid dat bestand gebruikt worden om opnieuw een connectie te leggen met exact dezelfde instellingen.

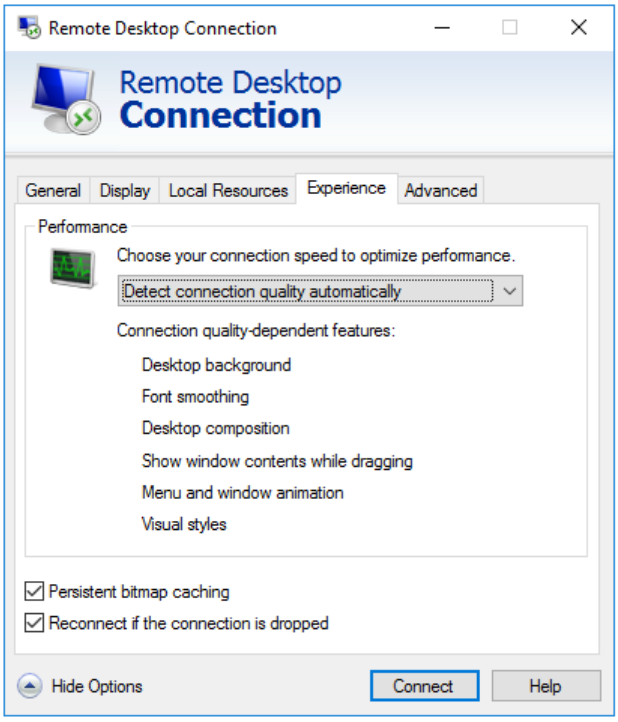
Het tabblad **Display** configureert de resolutie en kleurinstellingen van de weergave van de remote desktop op het lokale systeem.



Local resouces specificeert welke lokale middelen (geluid, harde schijven, printers, etc.) toegankelijk moeten gemaakt worden voor het remote systeem tijdens de sessie. Dit tabblad biedt ook de mogelijkheid te definiëren of bijzondere toetsencombinaties, zoals Ctrl Alt Del,door het lokale systeem of door het remote systeem moeten geïnterpreteerd worden.



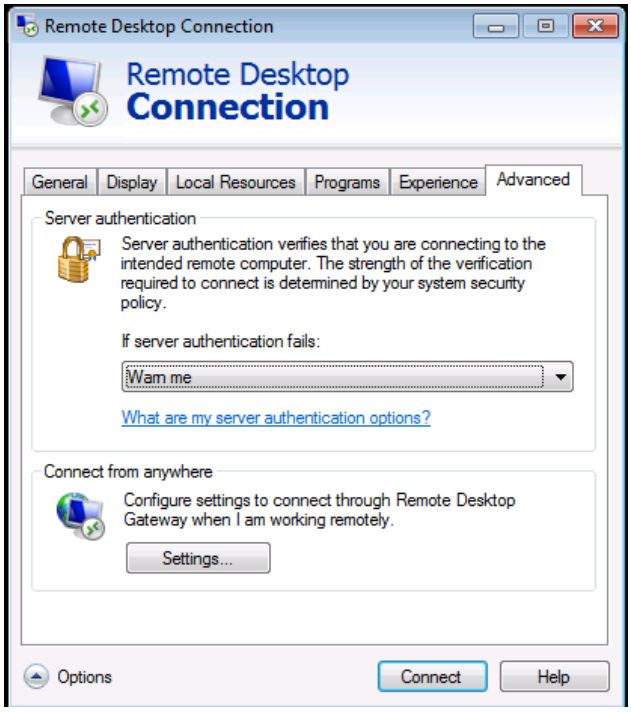
Experience controleert welke instellingen wel of niet overgenomen worden tijdens de remote desktop sessie. Bij een trage verbinding kan het bv. beter zijn de achtergrond niet mee over te nemen.



Het tabblad **Advanced** gaat over Authenticatie van de remote server. Dit garandeert dat de server waarmee de verbinding gemaakt wordt wel degelijk de juiste server is. Zo kan je vermijden dat je zonder het te weten vertrouwelijke informatie verspreidt.

Er zijn drie mogelijkheden:

Connect and don't warn me	Ook als de remote desktop connection de identiteit van de remote server niet kan verifiëren wordt de verbinding tot stand gebracht.
Warn me	Als de identiteit van de remote server niet kan geverifieerd worden verschijnt een waarschuwing zodat je op dat moment kunt beslissen of je de verbinding toch tot stand wilt brengen.
Do not connect	Als de verficatie van de remote server niet lukt zal er geen verbinding gemaakt worden.



2.1.5 Een remote verbinding beëindigen

Als een remote connection afgesloten wordt met een klik op 'X' dan blijft de verbinding open, ook al is er geen client verbonden.

Om de connectie echt af te sluiten kies je **Start > Disconnect**. Dit sluit de verbinding en de remote desktop client af.

3 MICROSOFT MANAGEMENT CONSOLE

Tot nog toe hebben we de standaardconsoles gebruikt om de server te beheren.

MMC is een framework voor beheertoepassingen dat een algemene interface biedt voor Microsoft beheerprogramma's, ook voor beheerprogramma's die horen bij toepassingen gemaakt door andere leveranciers. Die laatste gebruiken dan de MMC application programming interface.

MMC beschikt zelf over geen enkele ingebouwde functie om te beheren. MMC speelt wel gastheer voor componenten, snap-ins genoemd, die de beheerfuncties leveren.

Als beheerder kan je dankzij MMC zelf consoles aanmaken. Een console is een MMC waarin één of meerdere beheertools opgenomen zijn.

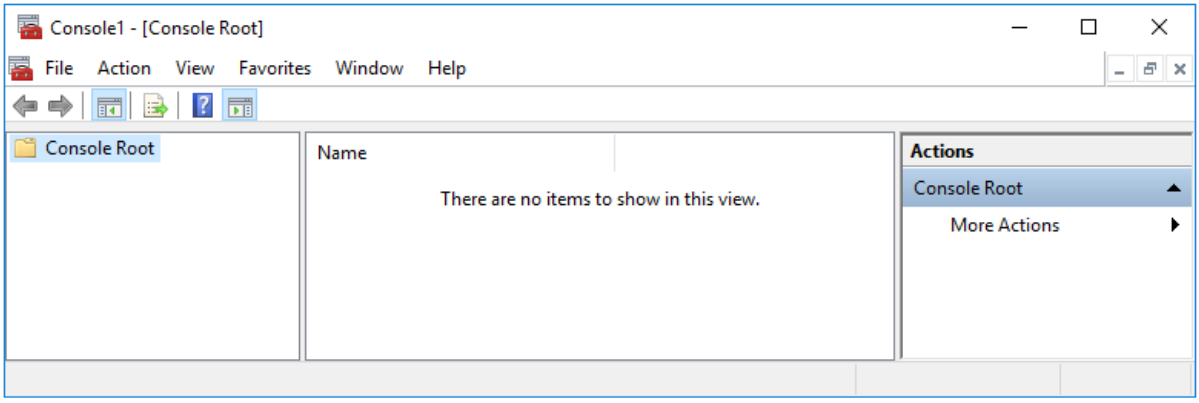
Voor administrators kan je zo een console per specifieke groep taken maken, bv. een console om alle taken uit te voeren die met beveiliging te maken hebben, een andere om netwerkbeheertaken uit te voeren en nog een andere met alle opdrachten die te maken hebben met het beheer van gebruikers.

Voor junior administrators of gebruikers die instaan voor bijzondere taken (delegatie), kan een taskpad van pas komen waarin de taken beperkt zijn tot diegene die ze ook echt mogen uitvoeren.

3.1 Een eigen console maken

- Start mmc.exe op.

Een venster met een lege console wordt geopend.



Daaraan kan je nu een aantal tools toevoegen.

- Selecteer de console root en open het menu **File**.
- Kies daar Add/Remove Snap-in...

Links verschijnen de beschikbare snap-ins.

Naast beheertools kan je in de console ook een folder opnemen, om structuur te brengen, of een hyperlink naar sites met belangrijke documentatie.

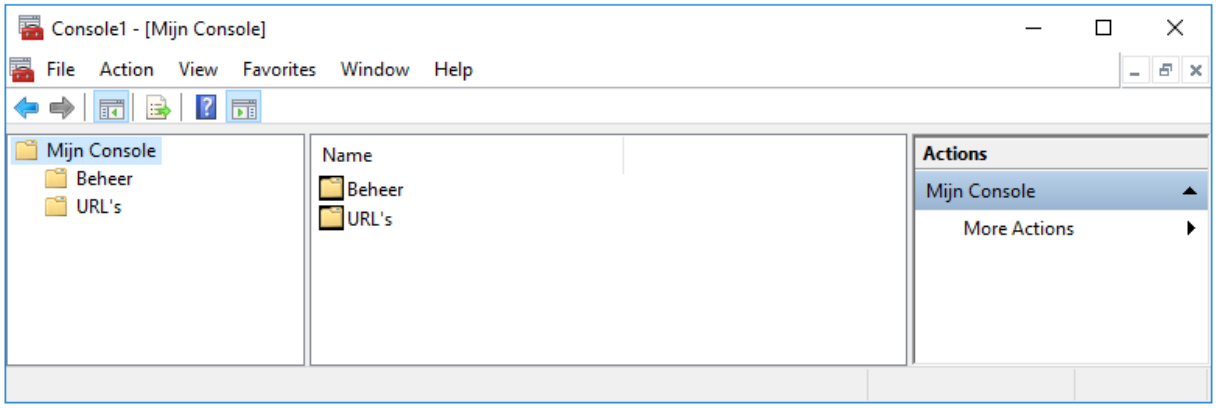
We maken een console met twee folders om structuur te brengen: een folder **Beheer** en een folder **URL's**.

- Selecteer folder in de linkse lijst en klik twee keer op **Add**.

Er verschijnen twee folders in de lijst met **Selected snap-ins**.

De naam **Folder** is weinig verduidelijkend. Je kunt de structuur wat duidelijker maken door meer beschrijvende namen te geven aan de folders. Dit kan echter alleen via het venster van de console.

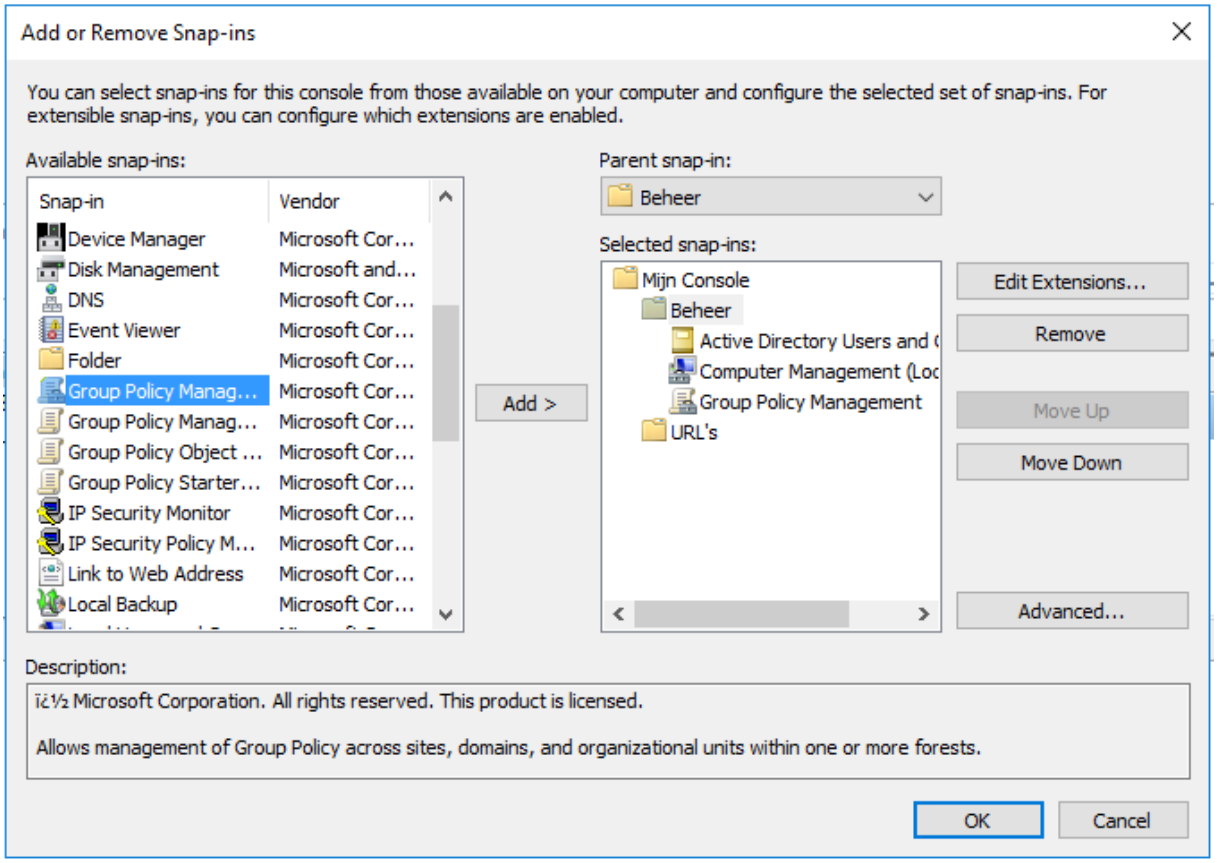
- Klik dan ook op **OK** om daarnaar terug te keren.
- Klik met de rechtermuisknop op elk van de folders en verander de naam via de opdracht **Rename** in respectievelijk **Beheer** en **URL's**.
- Verander meteen op dezelfde manier ook de naam **Console Root** in **Mijn Console**.



- Kies nu opnieuw **File > Add/Remove snap-in.**
- Om snap-ins in de juiste folder te kunnen toevoegen klik je op **Advanced**.

Het systeem vraag of het vak om de parent snap-in te wijzigen, mag toegevoegd worden.

- Plaats het vinkje bij **Allow changing the parent snap-in** en klik op **OK**.
- Selecteer in de lijst **Parent snap-in** de folder **Beheer** en voeg via **Add** de snap-ins **Active Directory Users and Computers**, **Computermanagement op de lokale machine** en **Group policy management** toe.



- Selecteer dan in het vak **Parent snap-in** de folder URL's en kies in de linkse lijst **Link to Web Address**.
- Vul bij **Path or URL** de URL van de site in, b.v. www.hp.com.
- Vul in het volgende venster een zelf gekozen verwijzing naar de site in, b.v. HP.
- Klik op OK om terug te keren naar de console.
- Kies **File > Save** en sla op als MijnConsole. Standaard komt het bestand terecht onder *C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows Administrative Tools* en krijgt het extensie .msc
- Sluit de console.

De console opnieuw openen:

- Klik dubbel op het opgeslagen bestand.

Een console kan geopend worden in twee verschillende modes: author mode en usermode.

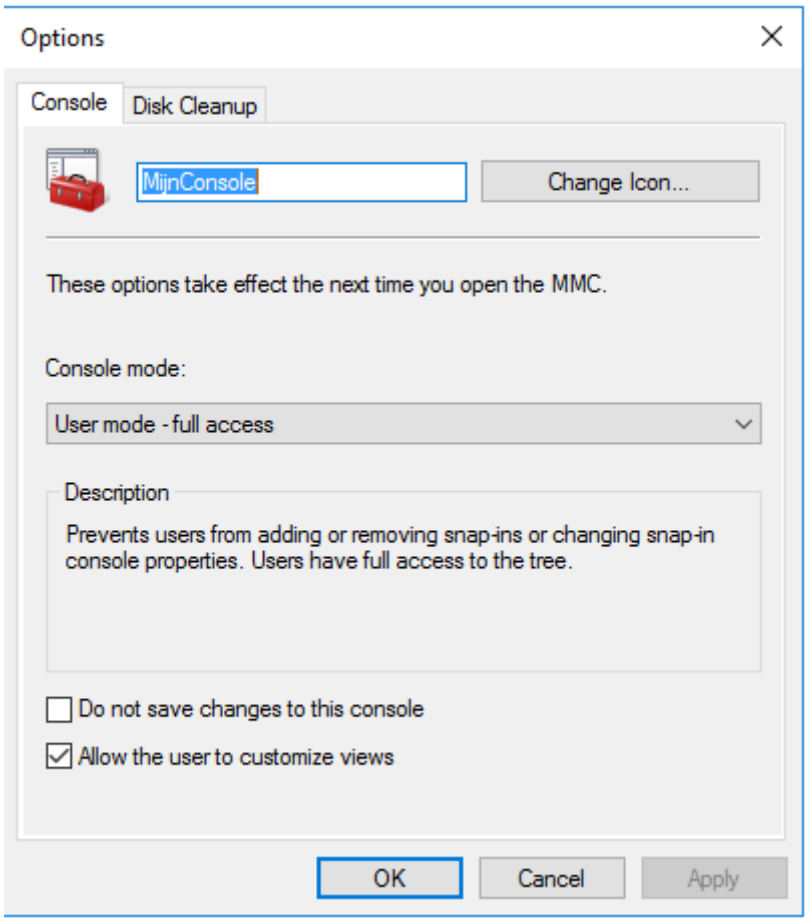
De standaardconsoles die je terugvindt onder Administrative tools openen in user mode. Dit betekent dat er geen wijzigingen aan de console kunnen gemaakt worden,

noch qua layout, noch qua samenstelling. Een console gebruiken zou altijd in user mode moeten gebeuren.

In Author mode kan de console wel aangepast worden, snap-ins kunnen verwijderd en toegevoegd worden, taskpads kunnen aangemaakt worden. Ook de menu's zijn in author mode uitgebreider dan in user mode.

Om een bestaande console toch in authormode te openen klik je met de rechtermuisknop op het pictogram van de console en kies je Author in het contextmenu of open je de console via de command prompt met switch /a.

Via **File > Options** in de MMC kan je bepalen in welke mode de console geopend wordt bij een volgend gebruik.



View > Customize laat toe te bepalen welke menu-onderdelen en werkbalken al dan niet getoond worden.

3.2 Taskpads

Via delegatie kunnen gebruikers het recht krijgen bepaalde taken uit te voeren in AD DS, ook al zijn ze geen lid van één van de beheerder groepen.

Die gebruikers moeten dan wel de nodige programma's ter beschikking krijgen om die taken uit te voeren.

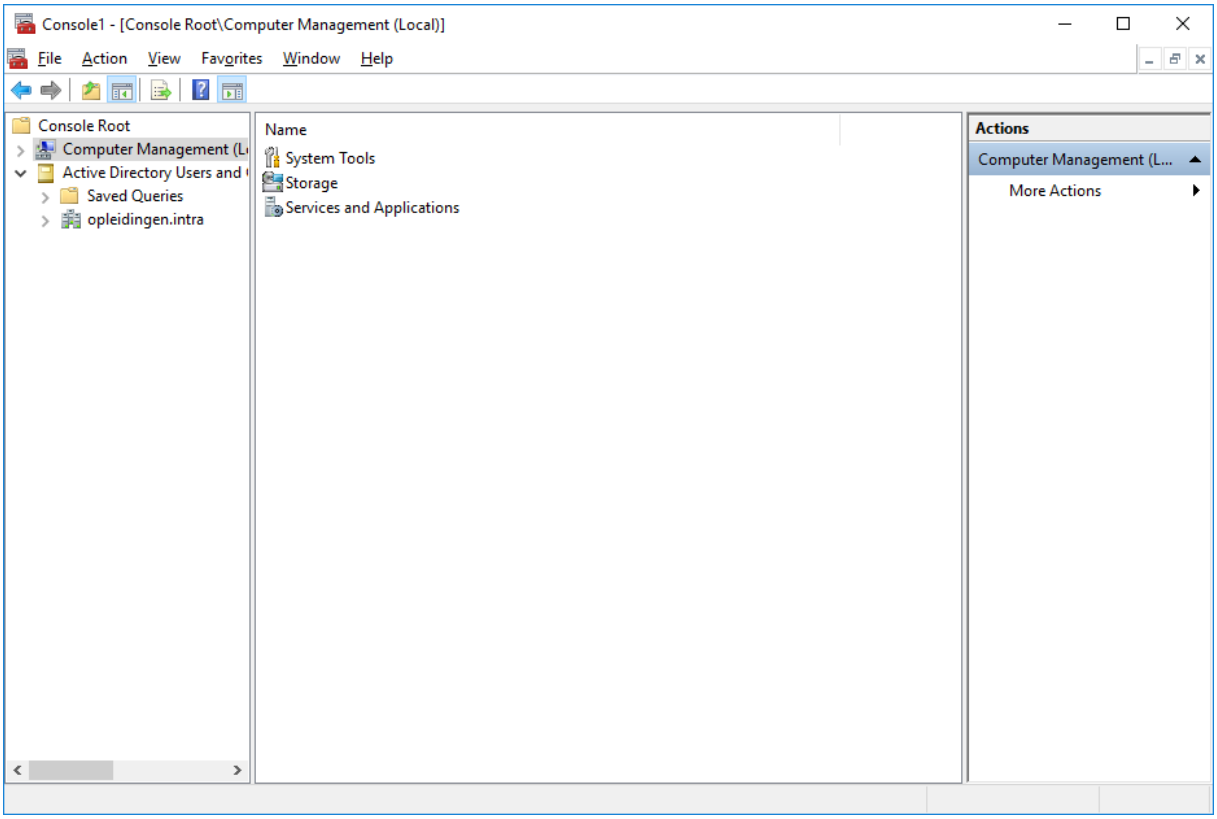
Een taskpad toont slechts een deel van een mmc, zodat een gebruiker alleen middelen ter beschikking krijgt om taken uit te voeren waartoe hij/zij het recht heeft.

3.2.1 Een taskpad aanmaken

We maken een taskpad om via computermanagement te connecteren naar een andere computer en daar een gedeelde map aan te maken en om te zoeken naar objecten in het domein.

Voorbereidend werk

- Maak een nieuwe console met daarin **Computermanagement (local)** en **Active Directory Users and Computers**.
- Voeg **Computermanagement (local)** toe aan Favorieten door de corresponderende node te selecteren, op **Favorites** te klikken en **Add to Favorites** te kiezen.
- Vouw ADUC open en klik op je domein (opleidingen.intra). Voeg dit ook toe aan de favorieten.
- Klik met de rechtermuisknop op **Computermanagement** en kies **New Taskpad View** in het contextmenu.



Een wizard start met een welkomscherm.

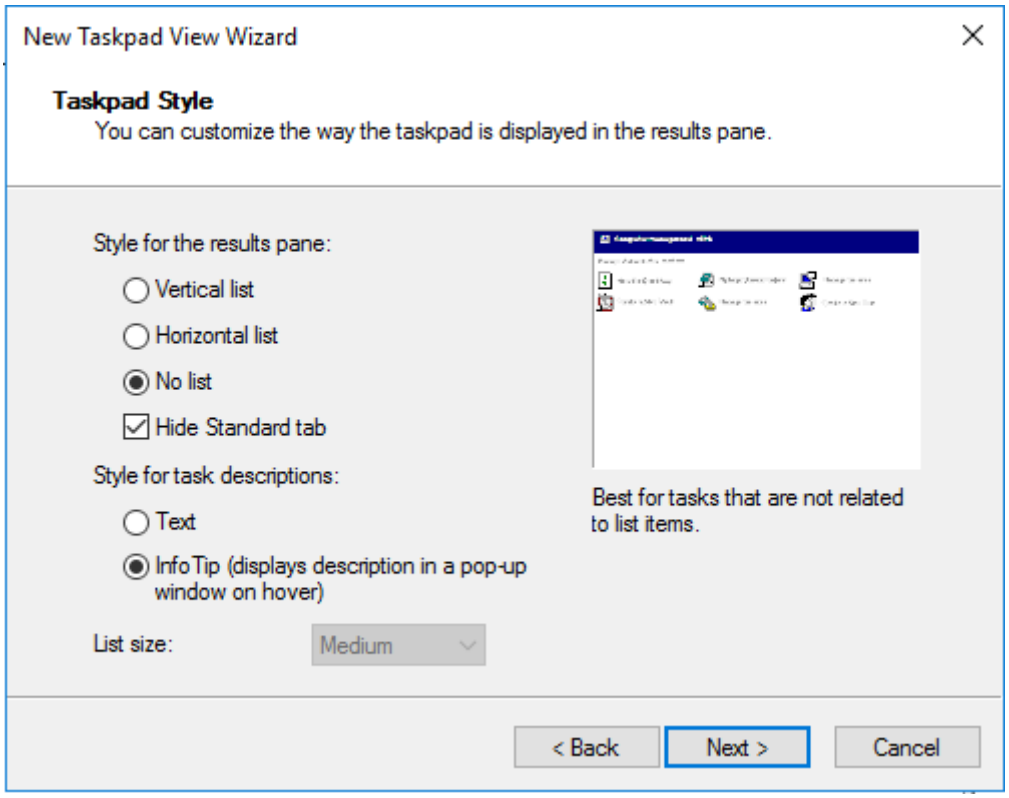
- Klik op **Next**.

In een volgend venster kan je bepalen hoe het taskpad eruit moet zien.

Hoe moet de lijst in het middelste paneel eruit zien? Een verticale lijst, een horizontale lijst of is er geen lijst nodig. Een lijst is nodig als je opdrachten opneemt in het taskpad die alleen beschikbaar zijn nadat je een object in het middelste paneel geselecteerd hebt.

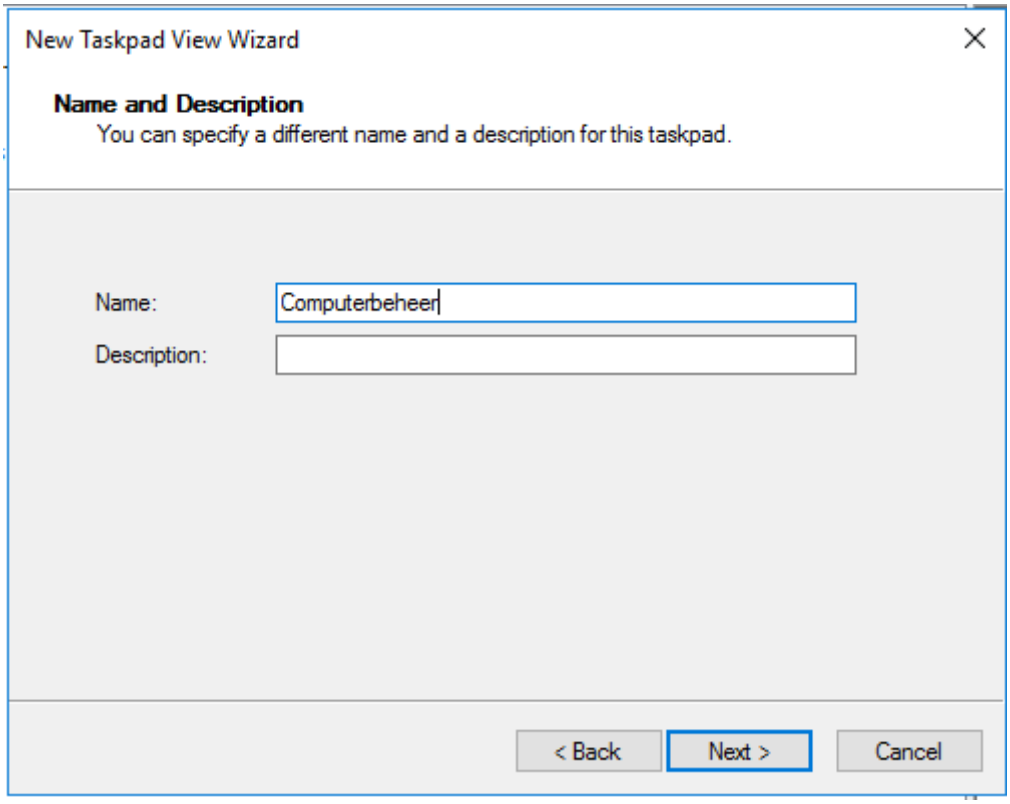
Je kunt hier ook kiezen hoe extra uitleg getoond wordt, als tekst of als Info Tip.

- Kies **No list** en behoud de andere instellingen.
- Klik op **Next**.



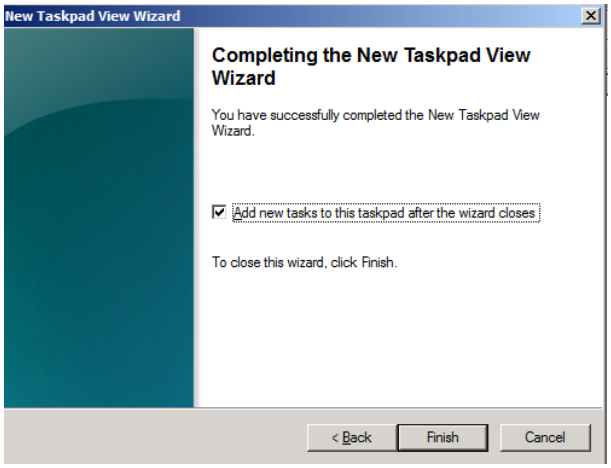
Zal het taskpad alleen van toepassing zijn op het geselecteerde item in het linkse paneel (Selected tree item) of moet het kunnen werken met alle items gelijkaardig met het geselecteerde item (de tweede optie).

- Kies de eerste optie, **Selected tree item**.



T4

- Behoud de naam en klik op **Next**.



Het taskpad is nu gemaakt. Je krijgt de keuze om onmiddellijk taken aan het taskpad toe te voegen of om te stoppen met de wizard.

- Laat het vinkje bij **Add new tasks to this taskpad after the wizard closes** staan en klik op **Finish**.

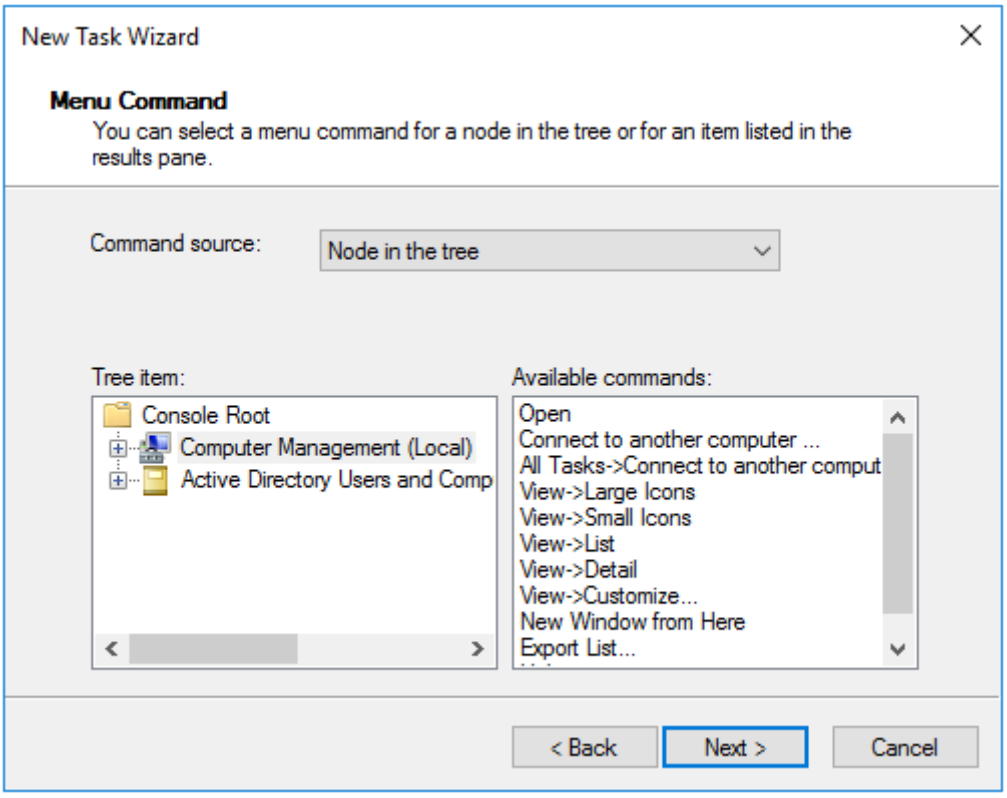
Onmiddellijk start een nieuwe wizard om taken toe te voegen aan het taskpad.

- Klik op **Next** in het welkomvenster. Het venster **Command Type** verschijnt.

Drie soorten taken kunnen opgenomen worden in een taskpad:

- een opdracht die je normaal via de snap-in in de mmc zou geven (**Menu command**).
- een script uitvoeren of een Webpagina openen (**Shell command**).
- een toegang tot een ander venster van het taskpad (**Navigation**).

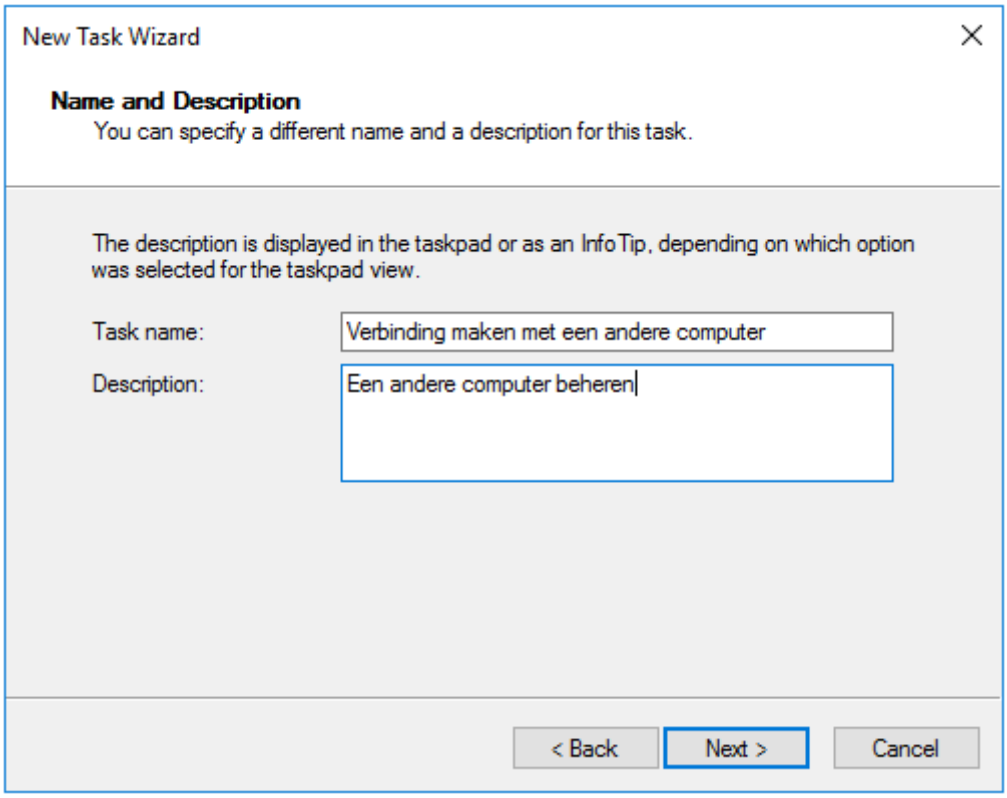
🛠 Kies **Menu** command.



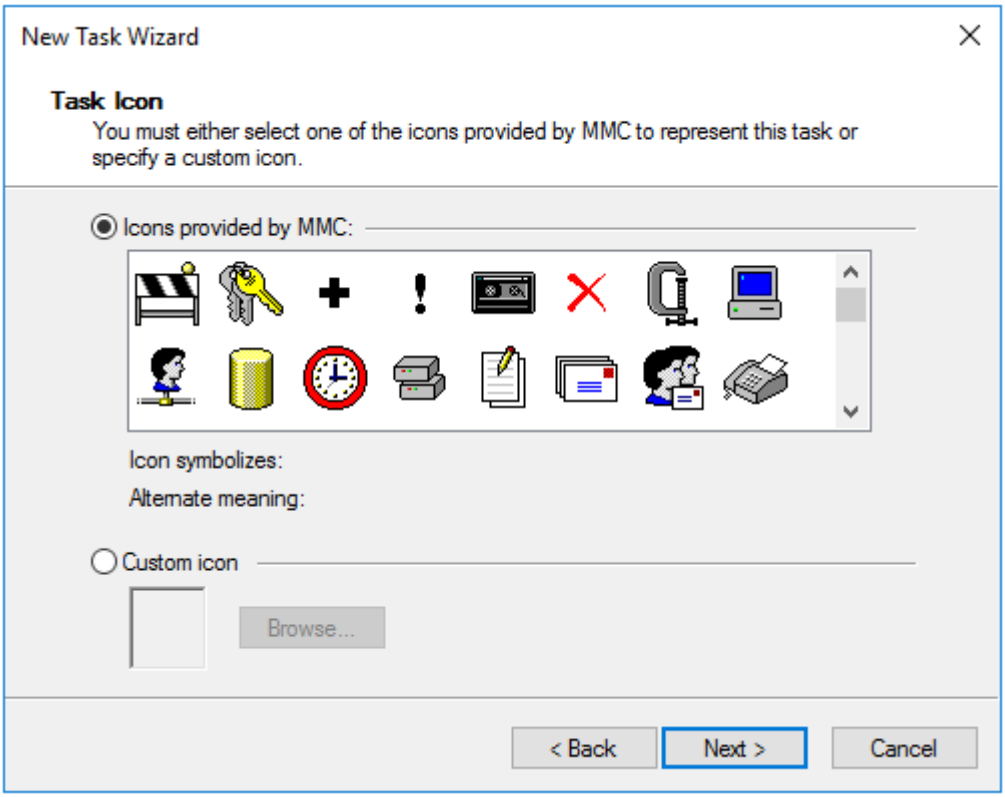
In de lijst Command source duid je aan of de opdracht hoort bij een node in de tree van het linkse paneel of bij een item in het middelste paneel van de mmc.

🛠 Selecteer **Node in tree**. De lijst met beschikbare opdrachten wordt aangepast.

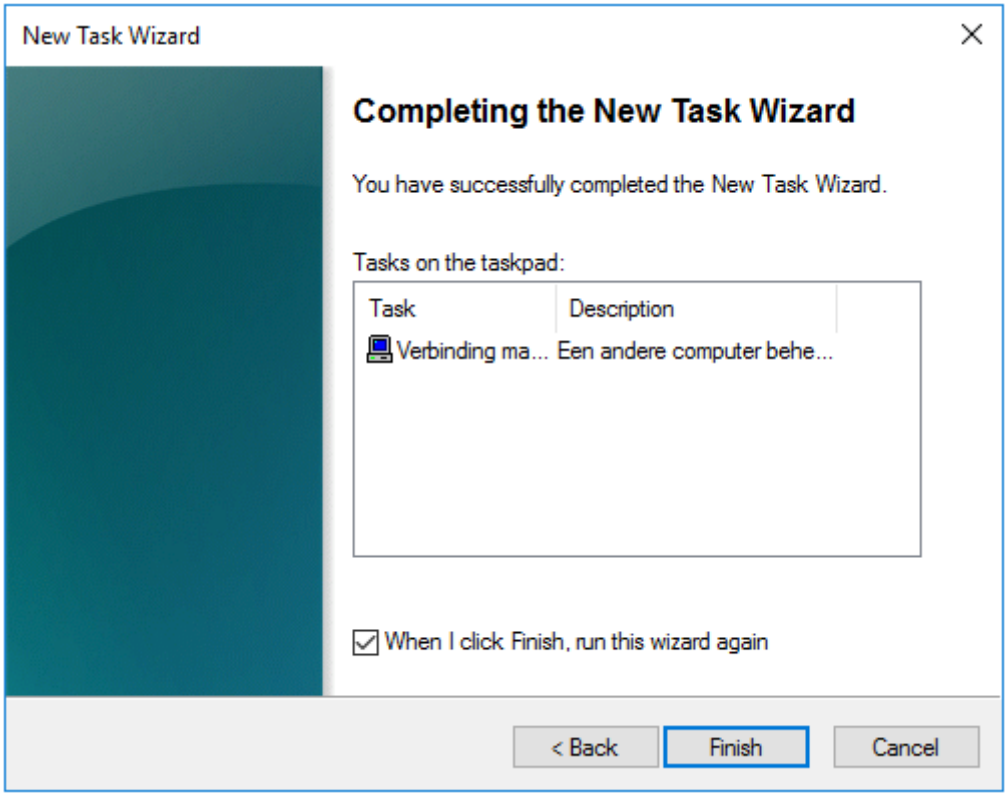
🛠 Selecteer **Connect to another computer** in de lijst en klik op **Next**.



- Geef de taak een naam bij **Task name** en vul een omschrijving in bij **Description**.
- Klik op **Next**.



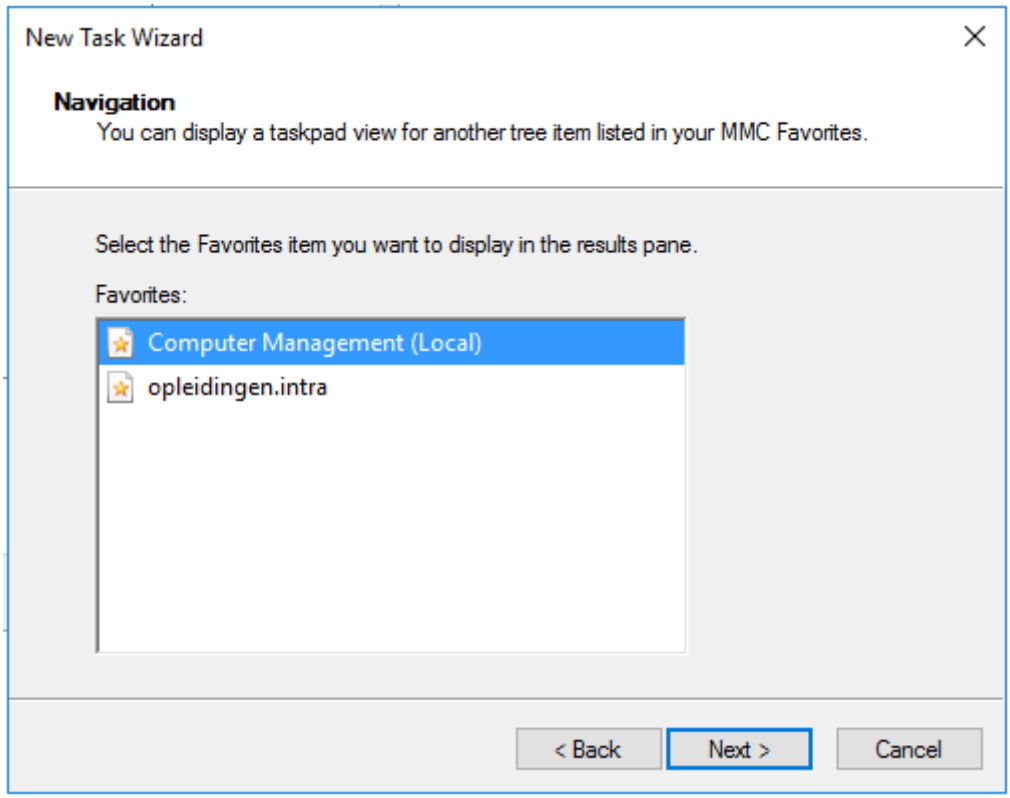
- Kies een passend pictogram voor de taak en klik op **Next**.



- Plaats een vinkje bij **When I click Finish, run the wizard again** om aan te geven dat je nog een taak aan het taskpad wenst toe te voegen.

De wizard om een taak toe te voegen wordt opnieuw gestart.

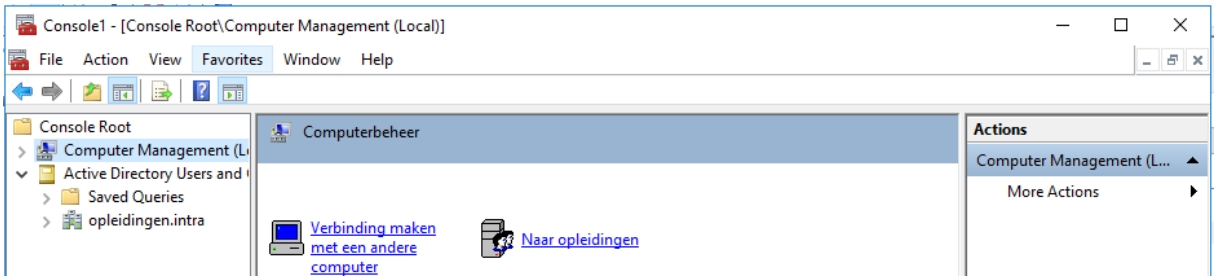
- Klik in het welkomscherm op **Next**.
- Kies deze keer in het venster **Command Type** voor **Navigation** en klik op **Next**.



- Selecteer **Opleidingen.intra** om aan te geven dat je naar de domeinnode wenst te gaan via de taak. Klik op **Next**.

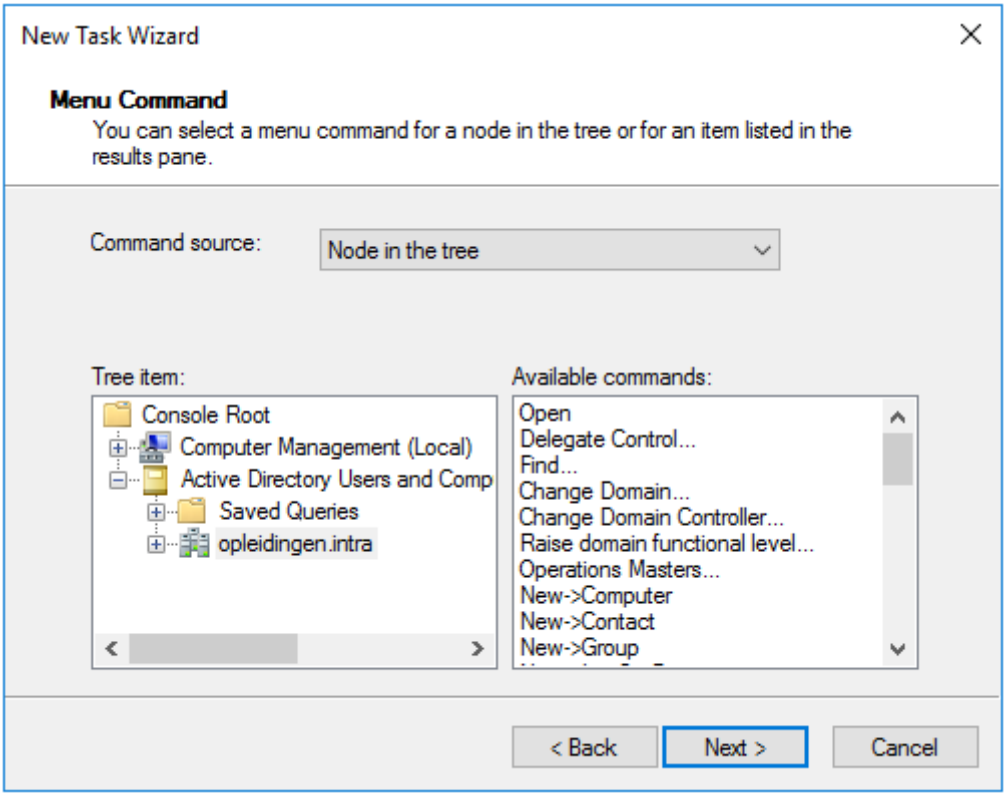
Opmerking In de lijst verschijnen alleen nodes die eerst zijn toegevoegd aan de Favorieten.

- Vule een gepaste naam in voor de taak, b.v. “Naar opleidingen”
- Kies ook een passend pictogram en klik op **Next**.
- Laat deze keer het vinkje bij When I click Finish, run this wizard again weg en klik op **Finish**.
- Klik dan op **OK**



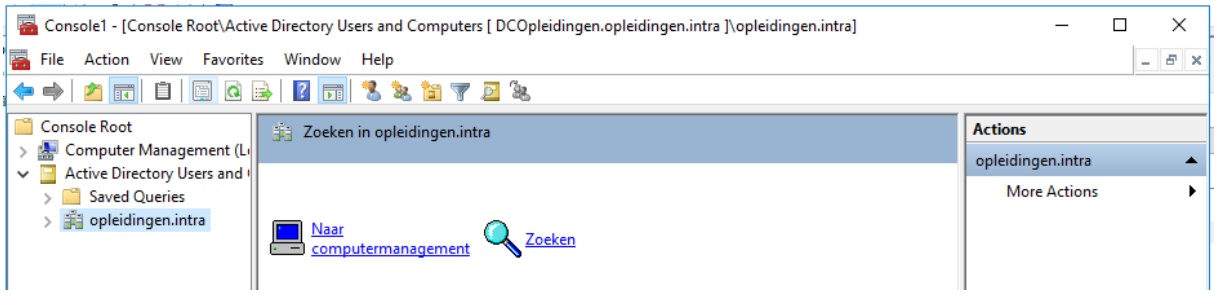
We willen via het taskpad ook kunnen zoeken in ADUC.

- Klik met de rechtermuisknop op **Opleidingen.intra** en kies **New Taskpad View**.
- Klik op **Next** in het welkomscherm.
- Selecteer in het venster Taskpad Style voor **No list, Hide Standard tab** en **Info Tip** en klik op **Next**.
- Kies in het venster **Taskpad Reuse** de optie **Selected tree item** en klik op **Next**.
- Geef als naam Zoeken in opleidingen.intra.
- Voeg meteen een nieuwe taak toe van het type **Menu Command**.
- Kies in het venster **Menu Command** bij **Command source** voor **Node in the tree**, selecteer in de lijst **Tree item** de node **opleidingen.intra** en in de lijst **Available commands** de opdracht **Find**.

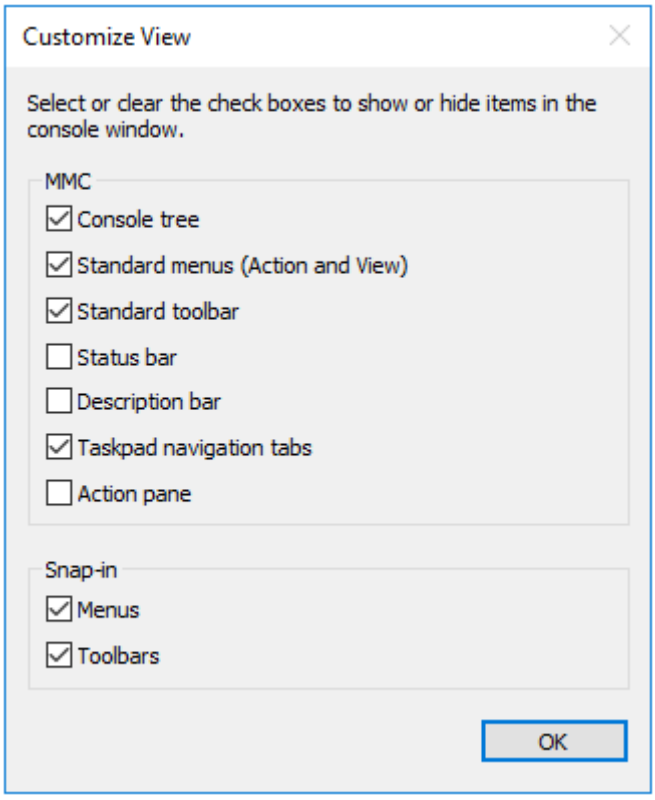


- Vul bij **Task name** b.v. Zoeken in en als **Description** de tekst Objecten zoeken in opleidingen.intra.
- Kies een gepast pictogram in het venster **Task Icon** en klik op **Next**.
- Voeg nog een nieuwe taak toe van het type **Navigation** om terug te keren naar **Computermanagement**.

Het resultaat ziet er nu ongeveer als volgt uit.



Via View > Customize… kan je nu nog alle overtollige panelen, werkbalken, menu's, ... verwijderen.

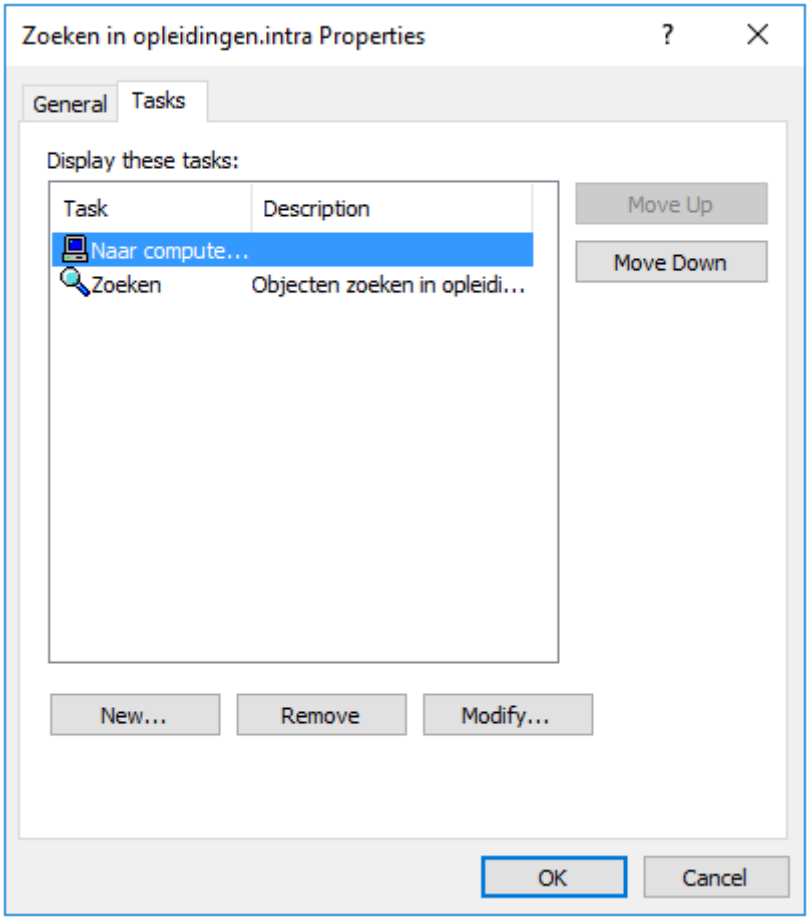


🛠 Sla de console ten slotte op in usermode.

3.2.2 Een taak aanpassen

Wil je achteraf nog aanpassingen doorvoeren aan de instellingen meegegeven via de wizard, dan kan dit door in het linkse paneel op dezelfde node te klikken en daar Edit taskpad view te kiezen.

Op het tabblad General kan je de algemene, op het tabblad tasks de meer specifieke instellingen van de taak wijzigen.



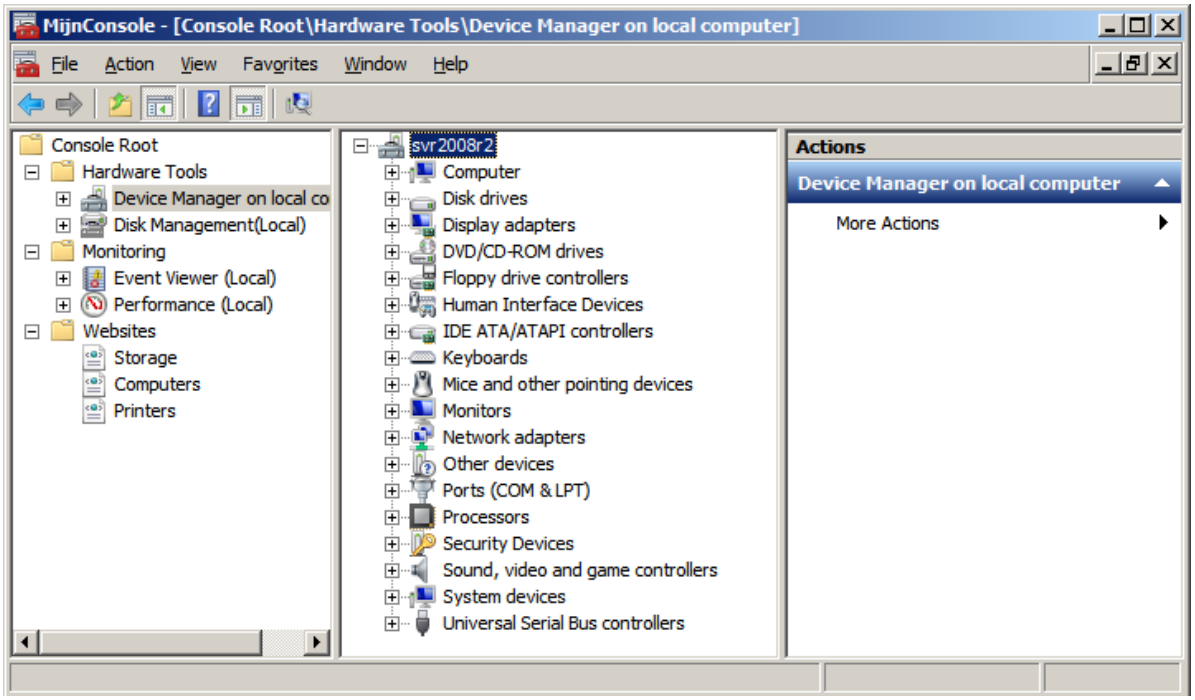
3.2.3 Een taskpad verspreiden

Consoles worden opgeslagen als gewone bestanden. Je kunt ze dan ook verspreiden als elk ander bestand: op de desktop van de gedelegeerde gebruiker plaatsen, per mail bezorgen of in een gedeelde map ter beschikking stellen.

Gebruikers zullen alleen met een console kunnen werken als ze over de nodige gebruikersrechten beschikken en over de nodige toegangsrechten tot de console.

3.3 Toepassingen

3.3.1 Maak onderstaande MMC na.



3.3.2 Maken van een eigen Taskpad

1. Geef alle instructeurs infrastructuur het recht nieuwe gebruikers aan te maken en wachtwoorden te wijzigen in hun eigen OU.

2. Maak een taskpad waarin ze alleen in hun eigen OU deze opdrachten kunnen uitvoeren.

3. Bezorg elk taskpad aan de juiste infrastructuur (plaats deze in een gedeelde folder waarop ze minimaal leesrechten hebben).

4. Test vanop de client of het taskpad werkt.

4 TAAKBEHEER

Taakbeheer geeft onmiddellijk een idee van de belasting van een toestel.

Er zijn verschillende manieren om de taakbeheer op te starten:

- Druk op de toetsencombinatie Ctrl+Alt+Del en klik dan op de knop **Task Manager**.

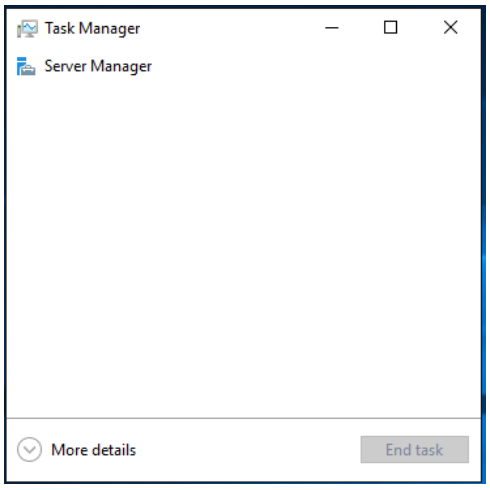
of

- Klik met de rechtermuisknop op de taakbalk en selecteer **Task Manager**.

4.1 Actieve toepassingen opvolgen

De versie zonder details toont een lijst met de toepassingen die opgestart zijn. Een vastgelopen toepassing krijgt de status Not responding en kan via de knop **End Task** elegant beëindigd worden.

Door rechts te klikken op een applicatie kan je de applicatie activeren of beëindigen, de locatie openen waar het programma staat, de eigenschappen van het bestand opvragen.



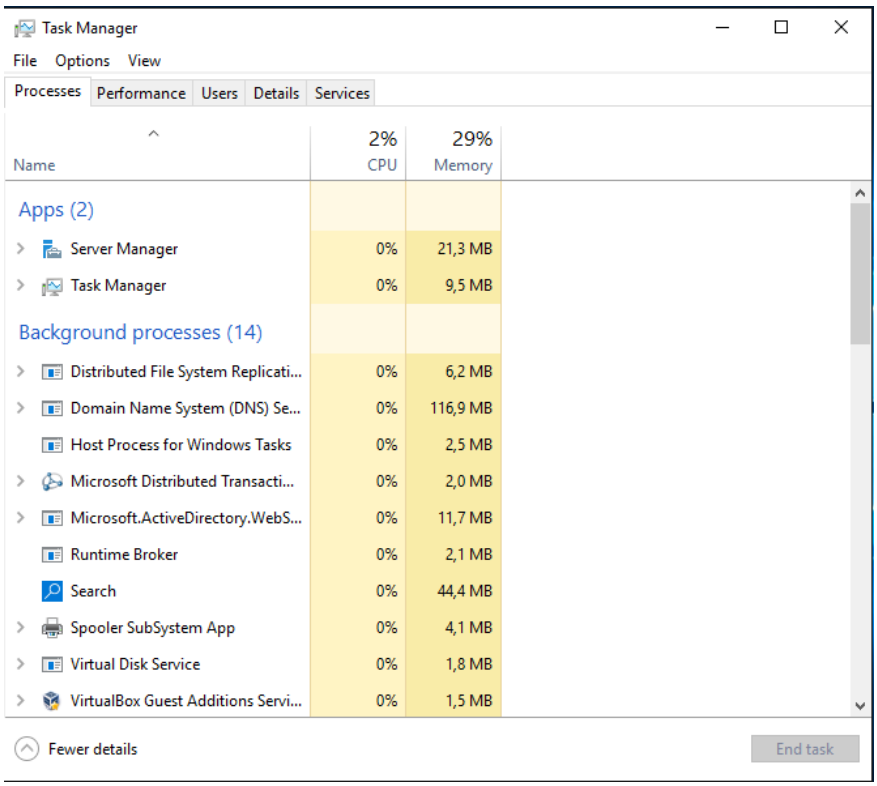
🛠 Druk je op **More Details**, dan krijg je meer informatie over alle programma's die actief zijn.

4.2 Processen opvolgen

Het tabblad **Processes** breidt de informatie uit.

In de kolom **Name** vind je de executable geassocieerd met de applicaties van het tabblad **Details**, samen met alle executables in uitvoering van het besturingssysteem.

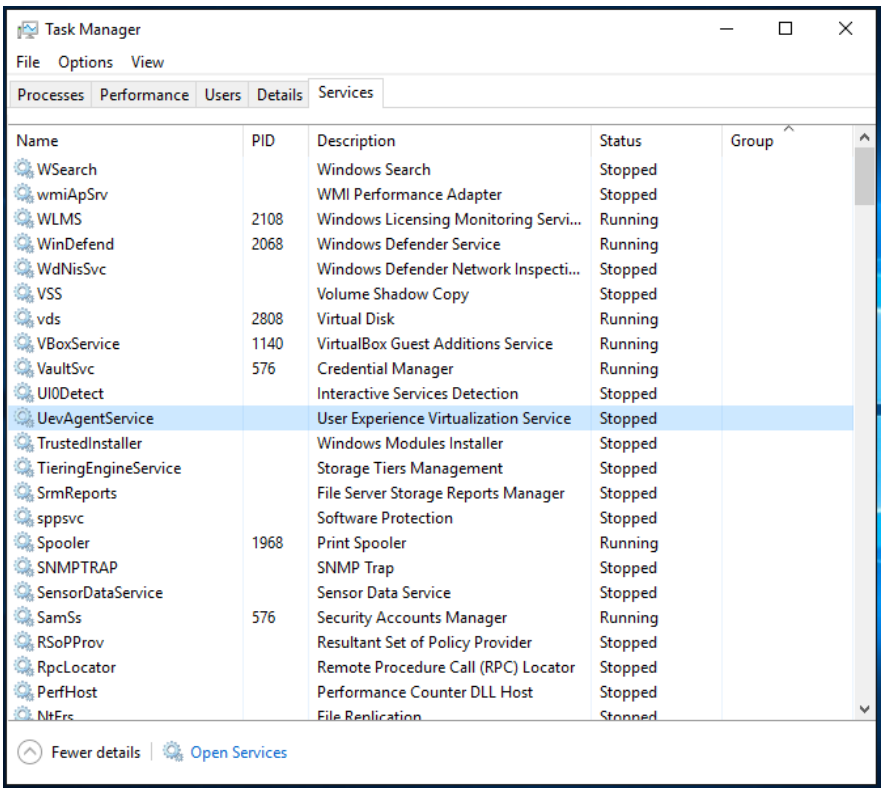
Naast de naam van de verschillende processen, vind je hier ook hoeveel procent van de processorcapaciteit en hoeveel geheugen het proces in beslag.



4.3 Services opvolgen

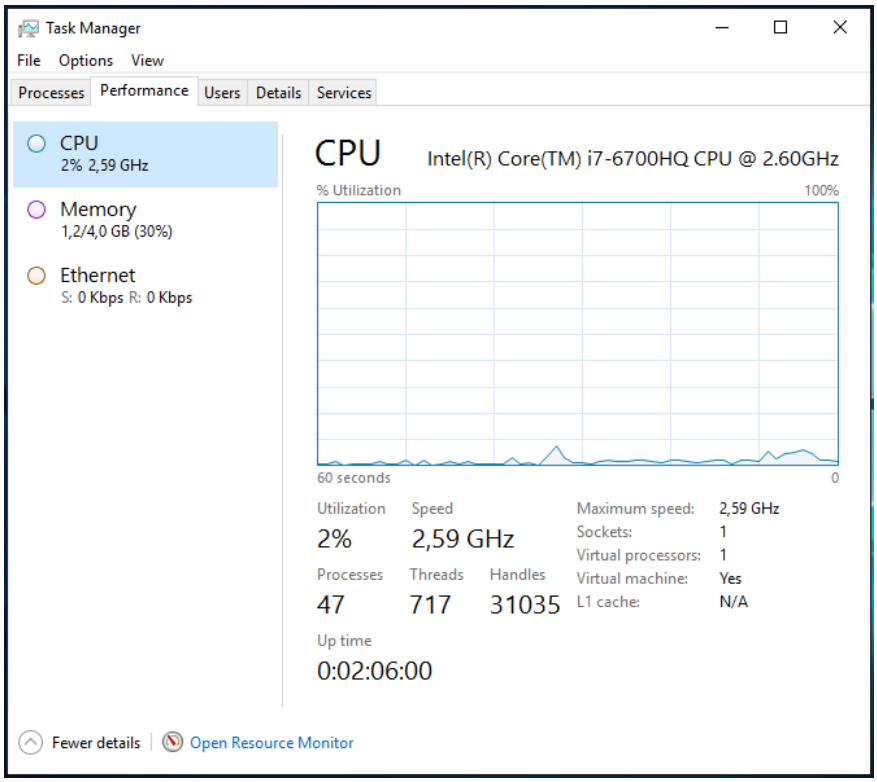
Nieuw vanaf Windows Server 2008 is het tabblad **Services**. Hier kan je in de kolom Status met één oogopslag zien of een service nog uitgevoerd wordt. De andere kolommen tonen de naam van de service, de PID (proces identifier), een omschrijving en de groep waarvan de service deel uitmaakt.

Je kunt van hieruit ook via de knop **Open Services** de Services snap-in oproepen om indien nodig in te grijpen in de instellingen van een bepaalde service.



4.4 Het gebruik van de processor en van het geheugen

Het tabblad **Performance** geeft een grafische voorstelling van het gebruik van de processor, het geheugen en netwerk, zowel van het gebruik op dit moment als van dat juist ervoor.



Rechtermuisknop op de grafiek > Show Kernel Times toont op de grafiek **CPU Usage** met een rode lijn ook het percentage van de proccessortijd besteed aan Kernel mode. De kernel tijd weerspiegelt in welke mate toepassingen gebruik maken van de services van het besturingssysteem. De overige processor tijd wordt besteed aan het uitvoeren van threads binnen de applicaties (user mode).

Op een server die over meerdere processoren beschikt kan je ook een grafiek per processor opvragen. Dit doe je via **Rechtermuisknop op de grafiek > Change graph to**. Kies daar **Logical processors**.

Het deel **CPU** geeft met **Processes** een ruw idee van het aantal executables dat momenteel uitgevoerd wordt, met **Threads** het aantal threads in uitvoering en met **Handles** het aantal connecties met interne resources. **Up time** vertelt je hoelang het systeem al ononderbroken draait.

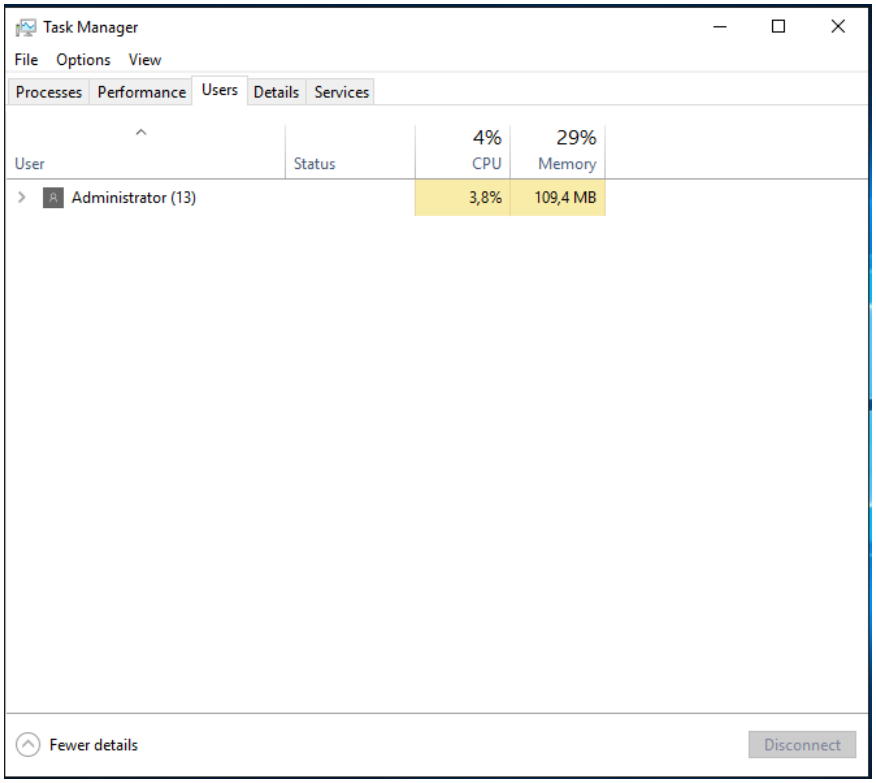
Het deel **Memory** onderaan meldt hoeveel RAM geheugen er in totaal ter beschikking is en hoeveel van het geheugen in gebruik is.

Het stuk **Ethernet** toont een overzicht van het netwerkverkeer op elk van de netwerkadapter van de server, of ze momenteel actief zijn en welk deel van hun capaciteit ze gebruiken.

De informatie wordt opgesplitst in Bytes Sent en Bytes Received.

4.5 Gebruikers die verbonden zijn met de server opvolgen

Het tabblad, **Users** geeft een overzicht van alle gebruikers die aangemeld zijn bij de server rechtstreeks of remote.



5 EVENT VIEWER

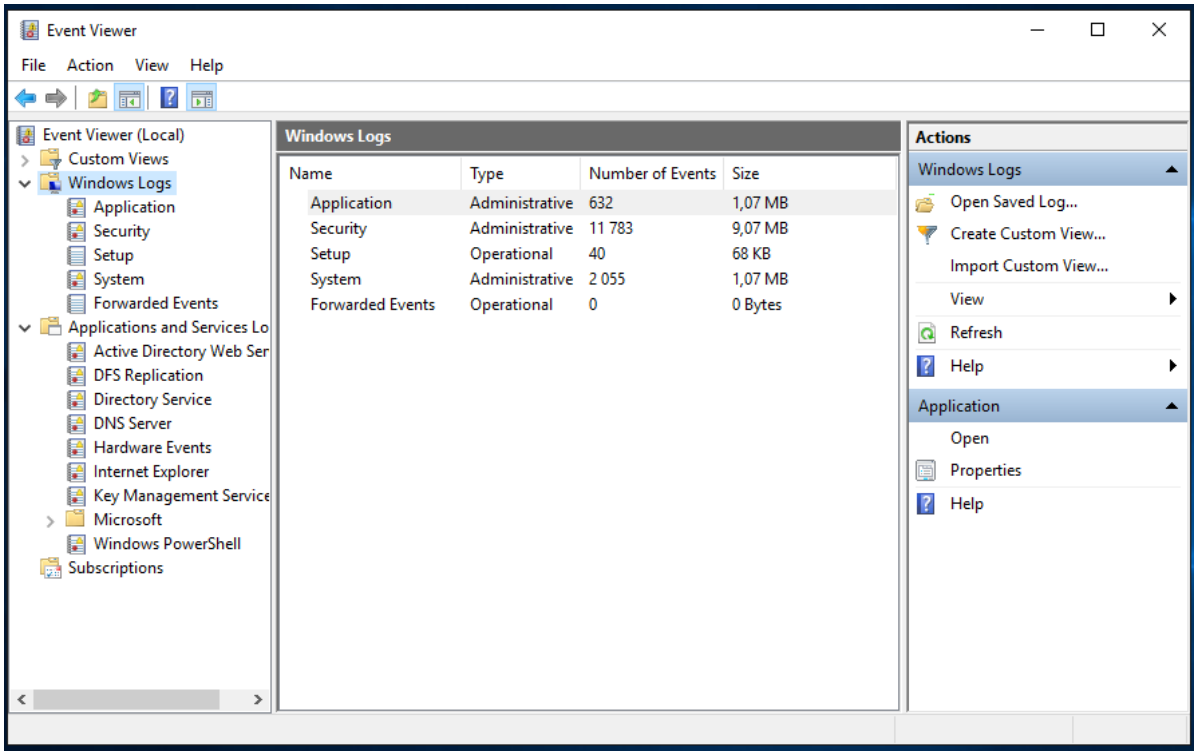
Kritieke gebeurtenissen, die de beschikbaarheid van de server in gevaar kunnen brengen, worden onmiddellijk gemeld op het beeldscherm, zonder dat daar één of andere instelling aan te pas komt.

Niet kritieke maar wel belangrijke gebeurtenissen worden geregistreerd in de logboeken te bekijken met de event viewer. Een gebeurtenis hoeft niet negatief te zijn. Een aanmelding die met succes afgehandeld werd, replicatie van data die zonder problemen verliep, ... kunnen ook meldingen in één van de logboeken genereren.

Als een server of een toepassing problemen geeft, is de event viewer een goed startpunt om informatie i.v.m. de problemen te verzamelen.

De Event Log service is verantwoordelijk voor het registreren van gebeurtenissen in één van de beschikbare logboeken.

Je vindt het programma bij de **tools** in de server manager**.**



Opmerking

Je kunt ook de logboeken van een ander toestel bekijken. Open daartoe Event Viewer via Administrative tools. Klik op de node **Even Viewer (Local)** en kies in het menu **Action** de optie **Connect to Another Computer**.

5.1 Gebeurtenissen bekijken in de verschillende logboeken

5.1.1 Beschikbare logboeken

De logbestanden worden in eerste instantie onderverdeeld in twee categorieën:

Windows logs waarin het besturingssysteem algemene systeem events registreert die te maken hebben met applicaties, beveiliging, setup en systeemcomponenten. Hieronder vind je ook de logboeken terug die al in oudere server versies bestonden.

Applications and Services logs waarin specifieke toepassingen en services gebeurtenissen registreren die applicatie- of servicegebonden zijn.

De Windows logs zijn verder onderverdeeld in

Application	Hierin registreren toepassingen zoals Microsoft Exchange Server, SQL Server, IIS, ... gebeurtenissen. Hierin komen ook gebeurtenissen gemeld door printers en alerts. Bestand: %systemroot%\System32\Winevt\Logs\Application.evtx
Security	Bevat alle gebeurtenissen die met auditing te maken hebben. Standaard krijgen alleen administrators toegang to het beveiligingslogboek. Bestand: %systemroot%\System32\Winevt\Logs\Security.evtx
Setup	Hierin registreren de componenten van het besturingssysteem alles wat te maken heeft met de installatie van toepassingen, roles en features. Dit logboek werd ingevoerd in Windows Server versie 2008. Bestand: %systemroot%\System32\Winevt\Logs\Setup.evtx
System	Gebeurtenissen die te maken hebben met het besturingssysteem of aanverwante services en drivers, vind je terug in het systeem logboek. Bestand: %systemroot%\System32\Winevt\Logs\System.evtx
Forwarded events	Verschillende computers kunnen feiten registreren die met hetzelfde probleem te maken hebben. Event forwarding is beschikbaar vanaf Windows Server 2008 en maakt het mogelijk de registratie van events te verzamelen in één container. Op voorwaarde dat event forwarding geconfigureerd is, bevat dit logbestand de doorgestuurde gebeurtenissen van andere servers met de bedoeling een identificatie van het probleem gemakkelijker te maken. Bestand: %systemroot%\System32\Winevt\Logs\ForwardedEvens.evtx

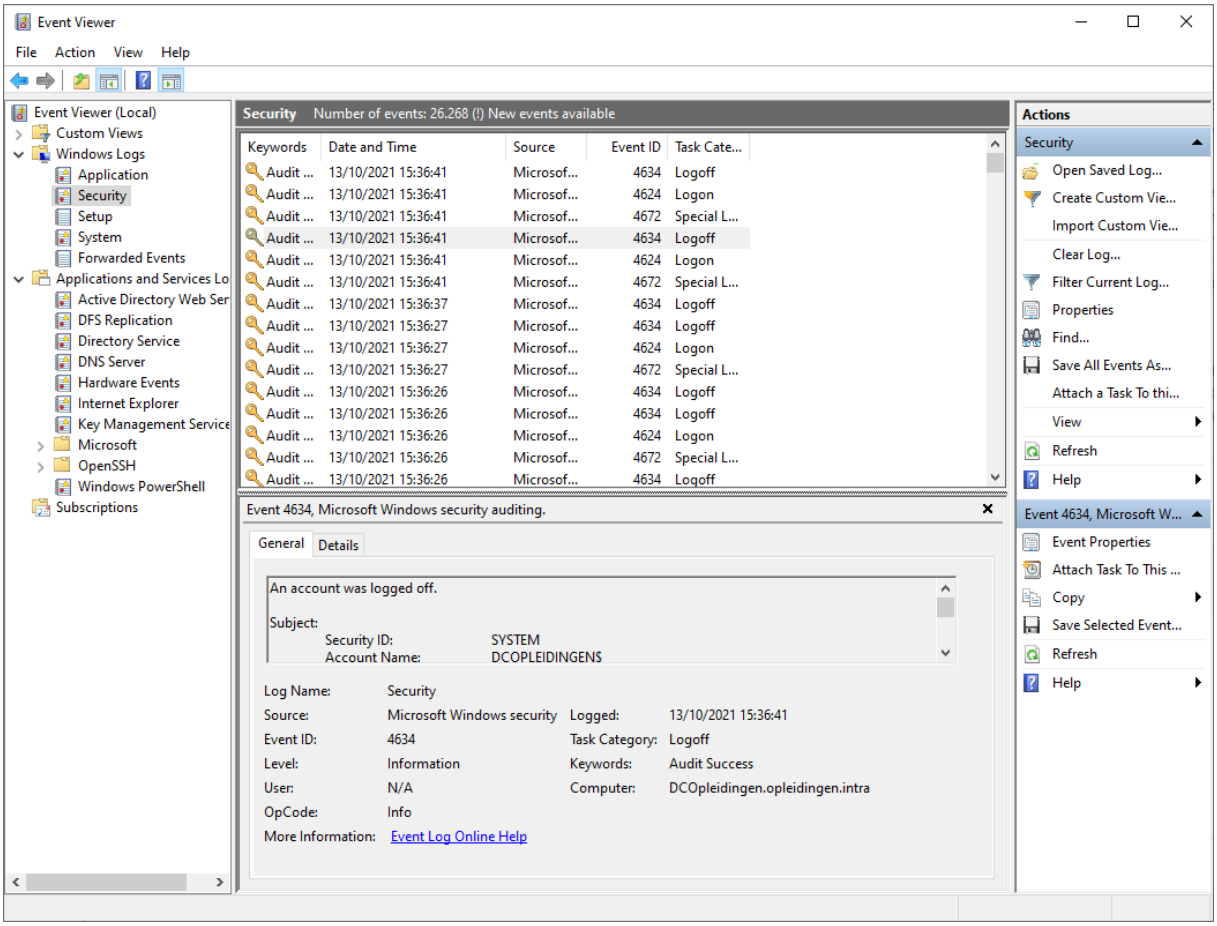
Welke logbestanden je onder het knooppunt **Applications and Services** vindt hangt samen met de rollen, features, bijkomende services... die op de server geïnstalleerd werden. In deze logboeken komen gebeurtenissen die met één enkele toepassing of component te maken hebben en geen invloed hebben op de algemene werking van het systeem.

Hier vind je de logbestanden terug die te maken hebben met DFS Replication, Active Directory Service, DNS server, ...

5.1.2 Events bekijken

- 🛠 Klik in het linkse venster op het logboek dat je wilt bekijken, rechts verschijnen de in het logboek geregistreerde events.

Als je een event selecteert verschijnt onderaan extra uitleg bij het event



Dubbel klikken op een event opent diezelfde uitleg in een apart venster.

Extra informatie is dikwijls te vinden op het Internet op basis van het event ID.

Welke eigenschappen van een event getoond worden in het middelste paneel, kan aangepast worden via **View > Add/Remove columns**

Events kunnen ook volgens een bepaalde eigenschap gesorteerd of gegroepeerd worden door met de rechtermuisknop op de hoofding van de bijbehorende kolom te klikken en Sort events by this Column of Group Events by this column te kiezen.

5.2 Custom Views

Door een filter te definiëren kunnen administrators zich beperken tot het bekijken van die gebeurtenissen die op dat moment voor hen relevant zijn. Sinds Windows server

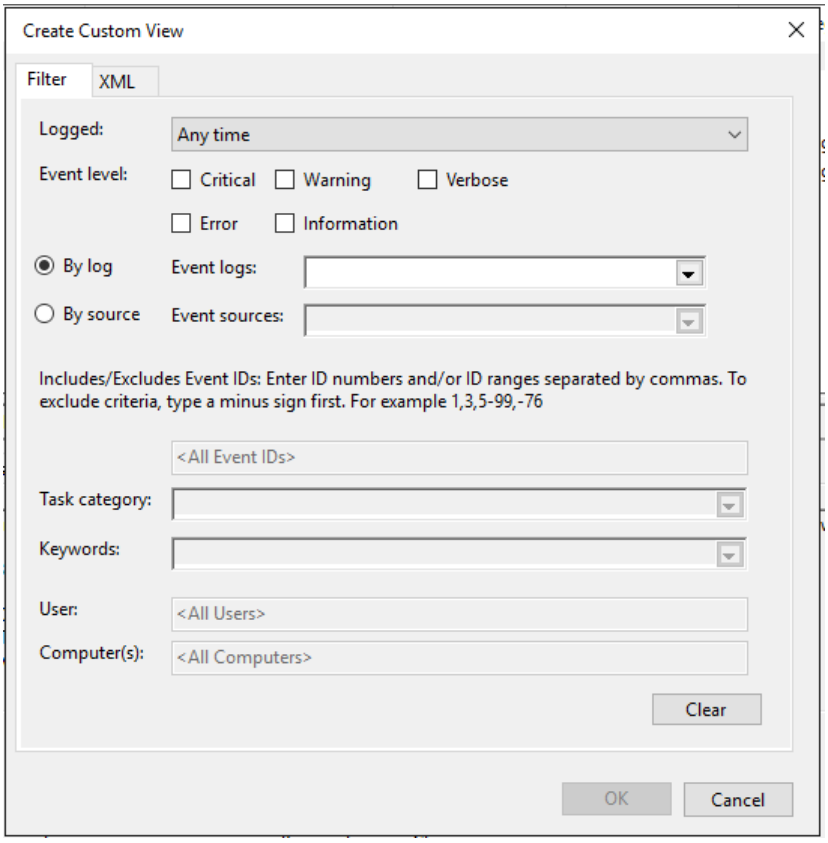
2008 kan je een filter ook opslaan. Die komt dan terecht onder het knooppunt **Custom Views**.

Onder Custom Views vindt een beheerder naast de zelf aangemaakte filters ook een aantal filters die automatisch aangemaakt worden door Windows Server bij de installatie van een nieuwe rol of toepassing zoals DHCP server, File server, ... Deze filters kunnen wel geraadpleegd worden, maar niet aangepast.

Een andere standaard filter is **Administrative events**. Hierin verschijnen automatisch alle events die te maken hebben met het systeem vanuit een beheer perspectief.

Een filter aanmaken

- Klik met de rechtermuisknop op **Custom Views** en kies **Create Custom View** of klik op deze actie in het rechtse paneel.



- Definieer de filter in het dialoogvenster **Create Custom View**.

Je kunt filteren op allerlei eigenschappen van een event: het tijdstip waarop het zich voordeed, het error level, het logboek waarin het geregistreerd werd, de bron die het event gegenereerd heeft, trefwoorden, enz. Via de radioknoppen **By log** en **By source** kan je ook een groepering van de gebeurtenissen vragen.

- Klik op **OK** nadat je alles naar wens hebt ingevuld.

- 🛠 Vul in onder welke naam en waar in de structuur onder Custom Views je de filter wilt opslaan.

Opmerkingen

Ingewikkelde filters kunnen de performantie van een systeem nadelig beïnvloeden.

Filters kunnen geëxporteerd worden als een XML bestand en dan op een ander toestel geïmporteerd.

Filters kunnen ook rechtstreeks in XML aangemaakt of gewijzigd worden. Dergelijke filter kan achteraf echter niet bewerkt worden via de grafische interface.

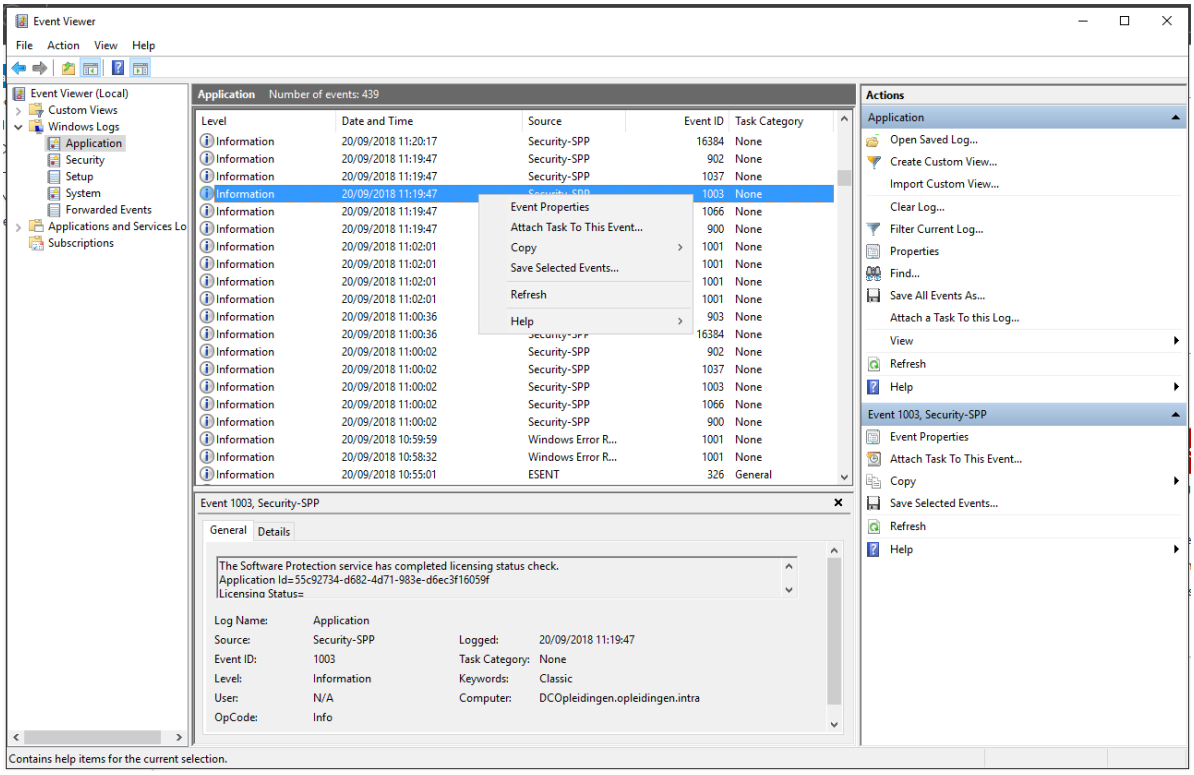
5.3 Een taak uitvoeren naar aanleiding van een event

Naar aanleiding van een gebeurtenis kan je ook automatisch een bepaalde taak laten uitvoeren zoals een programma dat gestart wordt, een e-mail die verzonden wordt, een bericht dat op het scherm verschijnt ...

Het programma Task scheduler houdt de logboeken voortdurend in de gaten om dit mogelijk te maken.

- 🛠 Ga in de logboeken op zoek naar een gebeurtenis van het type waaraan je een taak wenst te koppelen. Kies zelf een of andere warning in één van de logboeken.

- 🛠 Selecteer de gebeurtenis en geef de opdracht **Attach Task To This** event in het paneel Action.



De wizard **Create Basic Task** wordt opgestart.

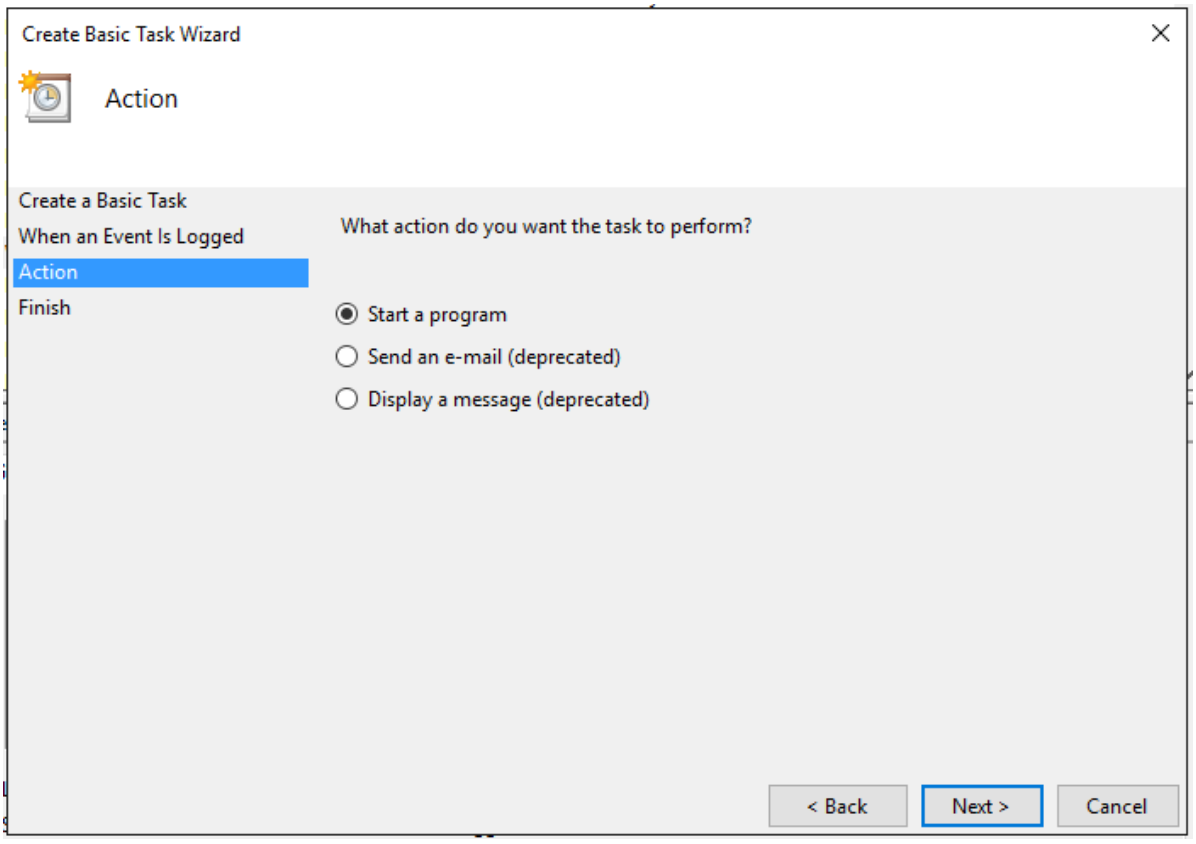
Opmerking

Om een taak te koppelen aan een event dat zich nog niet heeft voorgedaan, vertrek je van de **Task Scheduler** en geef je daar de opdracht **Create Basic Task**.

Je kunt een taak ook koppelen aan het feit dat er een event geregistreerd wordt in een bepaald logboek. Selecteer in dat geval het logboek en geef de opdracht Attach a task to this Log... onder Actions.

- Geef de taak een naam en eventueel een omschrijving.
- Klik op **Next**. Het venster **When a specific event is logged** verschijnt. De trigger en event informatie zijn al ingevuld.
- Klik op **Next**.

In het venster **Action** kan je bepalen welk type taak er moet uitgevoerd worden, een programma opstarten (een batchbestand, een anti-virus scanner,...) ,een e-mail verzenden (naar de beheerder of iemand anders) of een bericht tonen op het scherm van het toestel. De laatste 2 opties staan nog vermeld, maar zullen in een volgende release niet meer beschikbaar zijn.



- Kies Start a program en klik op Next.
- Vul de naam van programma of script in, bijkomend ook parameters en path van waaruit het moet gestart worden.

- Klik op **Next**.
- Klik **Finish** in het venster met de samenvatting.

Je kunt de taak achteraf ook testen.

- Ga naar Server Manager > Tools > Task Scheduler > Task Scheduler Library > Event Viewer Tasks

Daar vind je de taak in het middelste panel.

- Klik met de rechtermuisknop op de taak en kies **Run**. Het bericht verschijnt op het scherm.

5.4 Subscriptions en Forwarded events

In een bedrijf kan het nuttig zijn dat servers bepaalde gebeurtenissen doorsturen naar een centrale logging server. Om dit te bereiken kan je event forwarding inschakelen op de servers die de registratie van bepaalde events moeten doorsturen (broncomputer) en subscriptions configureren op de centrale logging server.

5.4.1 Voorbereidend werk

Voer onderstaande opdrachten uit op elke deelnemende computer, dus zowel op de computers die hun events doorsturen als op de computer die de events verzamelt.

- Open een command prompt met administratorrechten
- Typ *winrm quickconfig*

Dit maakt een WinRM listener op http://* aan die WS-Man requests aanvaardt op eender welk IP-adres op de broncomputer. Daarnaast wordt ook de service WinRM gestart (mogelijk krijg je een melding dat deze reeds gestart is).

- Beantwoord de vraag **Enable these changes** met **Y** en druk op enter.
- Indien je de vraag krijgt dat een aanpassing aan de firewall moet gedaan worden, dan antwoordt je deze vraag positief.

5.4.2 De nodige toegangsrechten organiseren

- Maak de computer account van de centrale logging server lid van de lokale administrator group op elk van de broncomputers.

5.4.3 De collector service activeren op de centrale logging server

- Open een command prompt met administratorrechten
- Typ wecutil qc

Deze opdracht start de Windows Event Collector Service

5.4.4 Een Inschrijving aanmaken

- Open de Event Viewer op de centrale logging server en selecteer de node **Subscriptions**.
- Klik op **Create Subscription** bij **Actions**.
- Geef de inschrijving een naam, b.v. alle file servers en eventueel een omschrijving.

De standaard locatie waar de events zullen terecht komen is het Forwarded Events logboek. Meestal voldoet dit.

Het initiatief laten uitgaan van de verzamelende computer (**Collector initiated**) is het eenvoudigst te configureren en dit is ook de standaard instelling.

- Klik op de knop Select Computers
- Klik op **Add Domain Computers** en voeg de broncomputer(s) toe.
- Klik op **OK** als alle broncomputers voorkomen in de lijst.
- Klik vervolgens op **Select Events.** Het Query filter dialoogvenster verschijnt.
- Klik de lijst open bij **Event Logs** en kies daar het logboek **DFS Replication** onder **Applications and Services Logs**.
- De lijst Event Sources vul je niet in.
- Klik op **OK**. Er wordt een nieuwe inschrijving aangemaakt.

5.4.5 Controle

- Start DFS management en voeg een map met twee targets toe in een bestaande naamruimte.
- Organiseer meteen de replicatie tussen de twee targets.
- Controleer achteraf of er in het logboek Forwarded events items zijn bijgekomen op de collector server.

5.5 De logboeken beheren

5.5.1 Een logboek leeg maken

Om een logboek leeg te maken selecteer je het logboek en kies je **Clear Log...** in het rechtse paneel onder Actions.

5.5.2 Een logboek opslaan

Het opslaan van een logboek kan nuttig zijn om een beeld te creëren van een normale situatie, om het te openen op een andere computer of alvorens een logboek leeg te maken. Dit kan in vier formaten:

.evtx	het kan achteraf met de event viewer geopend worden Opmerking Oudere versies van Windows besturingssystemen gebruiken .evt. Alleen Vista of nieuwere besturingssystemen van Windows kunnen overweg met dit formaat.
.txt	een tekstbestand, met tab als scheidingsteken
.csv	een tekstbestand, met comma als scheidingsteken, het bestand kan achteraf b.v. in Excel geïmporteerd worden.
.XML	Het bestand wordt in zuiver XML formaat weggeschreven.

5.5.3 De eigenschappen van een logboek instellen

Klik met de rechtermuisknop op het logboek en kies **Properties** of selecteer het logboek in kies **Properties** in het rechtse paneel onder **Actions**.

Hier kan je aflezen waar het logboek opgeslagen wordt.

Door de voortdurende registratie van gebeurtenissen, wordt het logboek altijd maar groter.
Standaard is de maximale grootte ingesteld op 20480 KB. Nog standaard gaat de event viewer de oudste items in het logboek overschrijven naarmate dat nodig is (**Overwrite events as needed (oldest events first)**).

Alternatieven zijn dat het logboek automatisch opgeslagen en leeggemaakt wordt (**Archive the log when full, do not overwrite events**) of dat items nooit overschreven worden (**Do not overwrite events**). In het laatste geval kan het dat een logboek volloopt en dat een beheerder het logboek manueel moet leeg maken door op de knop **Clear log** te klikken.

6 AUDIT

Audits worden gebruikt om een aantal activiteiten te kunnen opvolgen. Je kan op de hoogte blijven van hoe bepaalde acties afgelopen zijn.

Voor het auditen wordt er gebruik gemaakt van het security logboek van de Windows Logs die bekeken kunnen worden met Event Viewer.

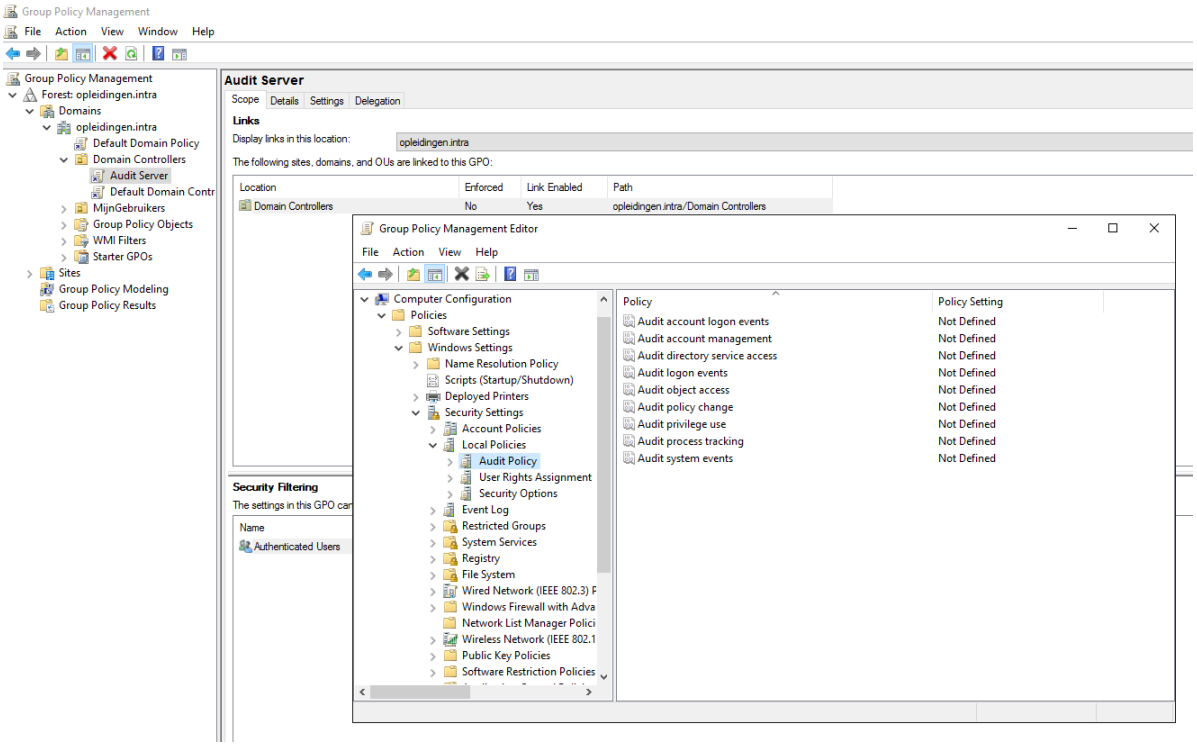
Het instellen van audits gebeurt via group policies.

6.1 Instellen audits via GPO

- 🛠 Start Group Policy Management.

Aangezien hetgeen we willen controleren zich bevindt op de domein controller, zullen we ook een GPO gebruiken die van toepassing is op de DC (en niet op de gewone PC's in het domein) . Hiervoor worden in een domein de DC's in een aparte organzational unit (OU) gezet: Domain Controllers. Standaard staat in deze OU een GPO gekoppeld : Default Domain Controllers Policy. Deze is dus perfect bruikbaar voor onze instellingen. Wens je aan deze default policy niet te veel wijzigingen te doen, dan kan je een nieuwe GPO maken en deze dan in de juiste OU.

- 🛠 Open het context menu van de juiste GPO en kies voor Edit
- 🛠 Gan naar Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy



Hier vind je alle settings ivm audit die instelbaar zijn via group policies:

Policy	Uitleg
Audit account logon events	Registratie van het valideren van de credentials van een gebruiker.
Audit account management	Registreren van wijzigingen aan gebruikers (ook wijzigen van paswoord)
Audit directory service access	Registratie van elke toegang tot Active Directory
Audit logon events	Regsitratie van iedere poging van een gebruiker om aan of af te melden.
Audit object access	Regsitratie van het gebruik van en toegang tot objecten zoals bestanden, printers,… Extra instellingen bij het object zelf zijn nodig.
Audit policy change	Registratie van wijzigingen in het audit-beleid en het beleid vna gebruikersrechten.
Audit privelege use	Registratie van het gebruik van priveleges door een gebruikers. Voorbeeld: Server operators krijgen het privelege “Allow log on locally” op een DC. Zodra zij dat doen wordt dit gelogd.
Audit process tracking	Registratie ivm vooruitgang van bepaalde processen.
Audit system events	Registratie van gebeurtenissen zoals starten en stoppen van de server.

Voor elke setting heb je volgende mogelijkheden om in te stellen:

- Success: de actie is met succes uitgevoerd:
  bv. Aanmelden met correct paswoord.

- Failure: de actie is niet correct kunnen uitgevoerd worden.
  bv. Wijzigen van een bestand waarvoor je enkel leesrechten hebt.

Beide instellingen kunnen samen geactiveerd worden. Zowel het succesvol uitvoeren van een actie als het niet succesvol uitvoeren van een actie kan nuttige informatie opleveren.

Enkele voorbeelden:

- Het correct aanmelden van een gebruiker op een toestel terwijl deze persoon met vakantie is. Heeft een collega zijn rechten nodig? Is er een virus aanwezig? …

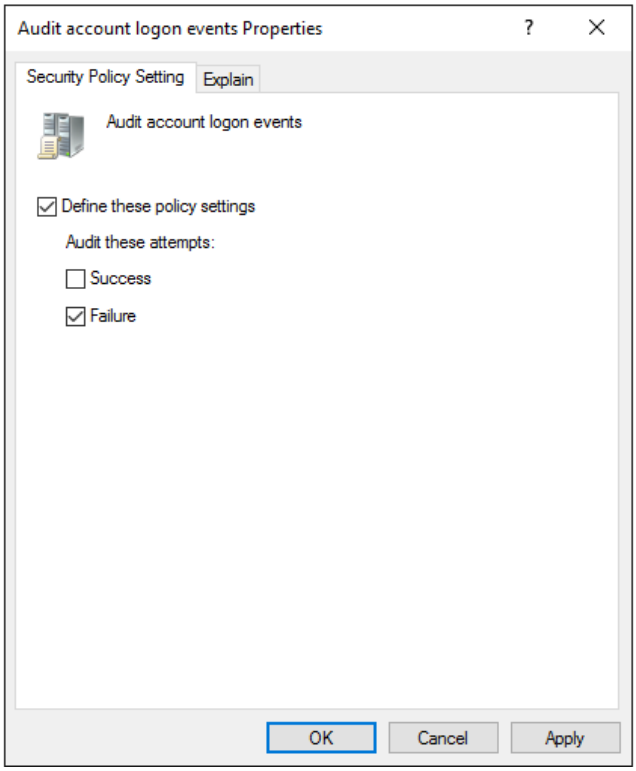
- Het foutieve paswoord wordt ingegeven van een gebruiker. Is de persoon het zelf vergeten of probeert iemand anders aan te melden?

- Het proberen wijzigen van een bestand door een persoon. Mag deze persoon wijzigingen aanbrengen? Mocht deze persoon misschien zelfs lees-rechten hebben op dat bestand?

6.2 Controle audit

Mislukte inlogpogingen

- 🛠 Dubbelklik op “Audit account logon events”
- 🛠 Het eigenschappen venster komt tevoorschijn
- 🛠 Zet een vink bij Define these polcy settings en daarna ook bij Failure. Het vinkje bij Succes mag verwijderd worden.



- 🛠 Druk op OK.

Om te testen moet je de group policy actualiseren. Beste even het programma *gpupdate* in een command prompt uitvoeren.

Je kan deze setting nu testen:

- Start je client toestel op
- Geef een gebruikersnaam in maar met verkeerd paswoord.
- Start op de server de event viewer en bekijk de Security log bij de Windows Logs.

Wijzigen van accounts in AD

- Dubbelklik op “Audit account management”
- Het eigenschappen venster komt tevoorschijn
- Zet een vink bij Define these polcy settings. Zorg ervoor dat er zowel bij Succes als bij Failure het vinkje staat.
- Druk op OK.

Om te testen moet je de group policy actualiseren. Beste even het programma *gpupdate* in een command prompt uitvoeren.

Testen kan je doen door bv. op de server in Active Directory Users and Computers een gebruiker bij te maken en terug te verwijderen. Of wijzig het paswood van een bestaande gebruiker.

Mislukte toegang tot netwerkobjecten

- Dubbelklik op “Audit object access”
- Het eigenschappen venster komt tevoorschijn
- Zet een vink bij Define these polcy settings en daarna ook bij Failure. Het vinkje bij Succes zet je momenteel best niet aan.
- Druk op OK.

Om te testen moet je de group policy actualiseren. Beste even het programma *gpupdate* in een command prompt uitvoeren.

Naast de instelling in group policy, moet de audit ook op het object geactiveerd worden.

- Maak op de server de map e:\AuditTest aan
- Vraag de eigenschappen op van deze map.
- Tabblad Sharing: via knop Advanced sharing wordt de map gedeeld met de standaard permissies.
- Tabblad Security, knop Advanced

- Disable inheritance, kies ‘convert inherited permissions into explicit permissions on this object’

- Op tabblad Permissions : verwijder de 2 lijnen in het overzicht waar ‘User (..)’ staat

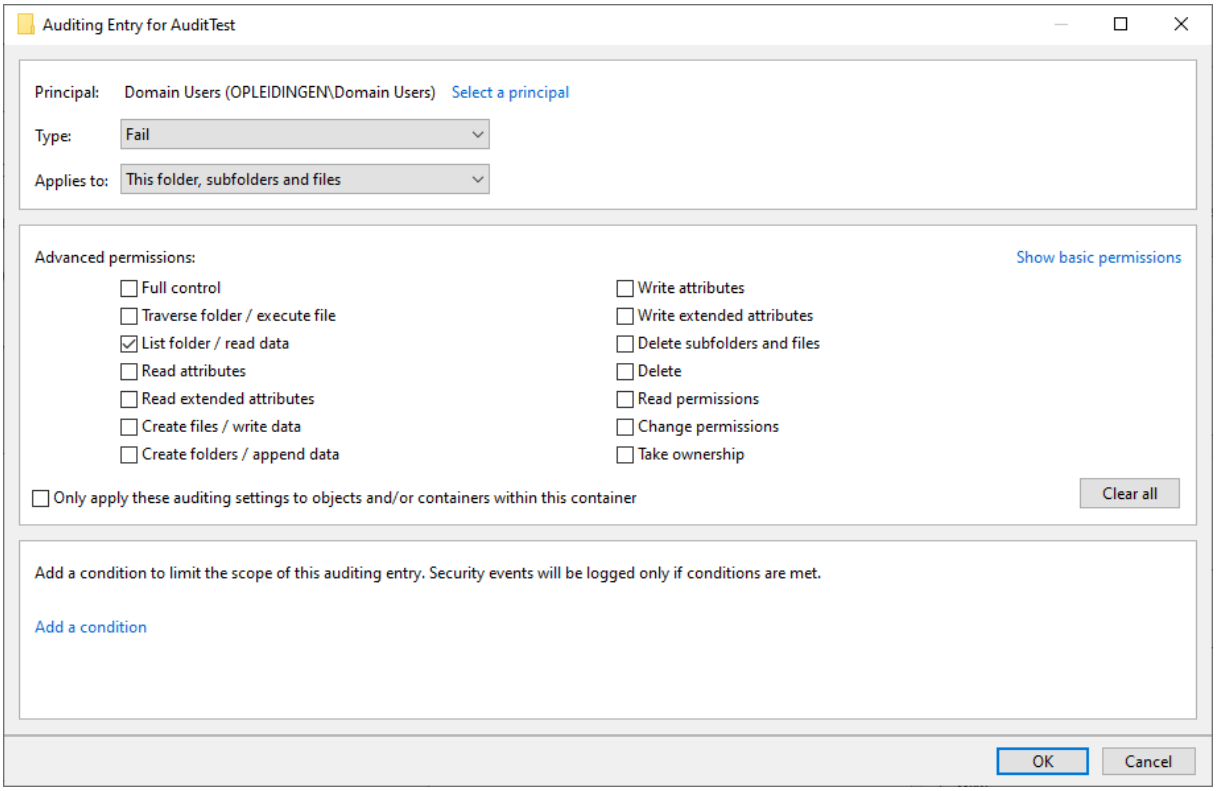
- Ga naar tabblad Auditing: klik op de knop Add om een lijn toe te voegen. Vul onderstaande gegevens in :

  Principal: Users

  Type: Failure

  Applies to: This folder, subfolders and files

  Advanced Permissions (klik hiervoor eerst op *Show basic permissons* rechts in de kader) : “Clear all” en vink enkel “List folder / read data” aan.



Druk 2 keer op OK, 1 keer op Close om het eigenschappen venster af te sluiten.

Meld je nu aan op je client toestel.

Ga via de verkenner naar de gedeelde map op de server. Je moet de melding krijgen dat je geen toegang hebt ertoe. Voor de groep Users (waarvan de group Domain Users lid is) hebben we immers toegang verwijderd.

Controleer nu op de server in de Event Viewer dat er audit lijnen zijn toegevoegd in de Security log.

7 METEN MET DE SYSTEEM MONITOR

7.1 Real time metingen

7.1.1 De systeem monitor opstarten

- Start / Run / Perfmon

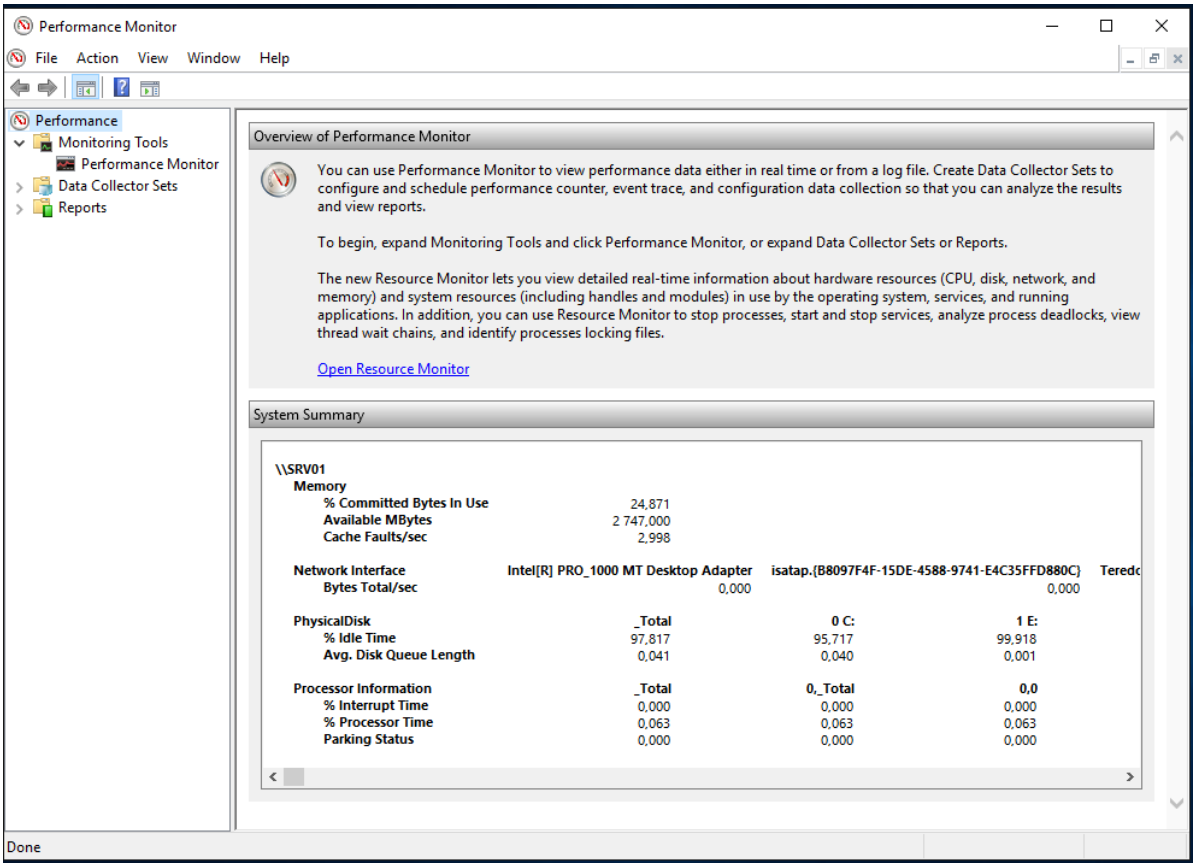
Of

- Server Manager > Tools > Performance Monitor

De MMC biedt een knooppunt **Performance** aan met daaronder drie knooppunten: **Monitoring tools**, **Data Collector Sets** en **Report Generation**.

7.1.2 Een overzicht

Door in het navigatiepaneel op het knooppunt Performance te klikken verschijnt in het middelste paneel een overzicht. Het toont het CPU gebruik, het gebruik van de harde schijf, de drukte op de netwerkinterface en het gebruik van het geheugen, zoals die op dat moment gemeten worden, dit alles in cijfers uitgedrukt.



7.1.3 De systeem monitor configureren

De Performance monitor werkt met objecten, instances en counters.

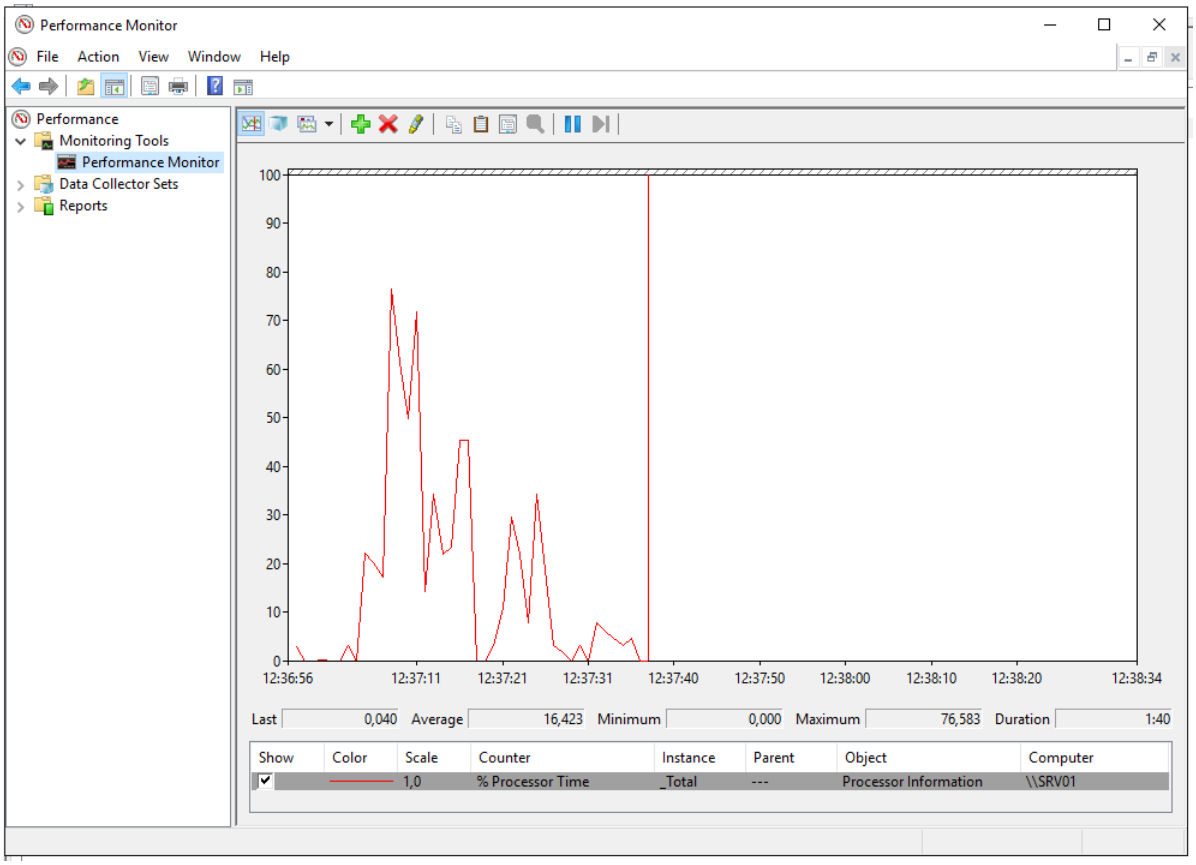
Een object is een type component van het systeem met een aantal meetbare eigenschappen. Dit kan een fysiek onderdeel zijn, zoals het geheugen of de

processor, een logisch onderdeel zoals een volume of een software onderdeel zoals een proces of een thread.

Als een server beschikt over meer dan één object van hetzelfde type dan is elk object een instance van dat type object. Zo is elke processor van een server met meerdere processoren een instance van een processor.

Een counter is dan een meetbare karakteristieke eigenschap van dat object.

De performance counter geeft standaard al een grafische voorstelling van de counter **%processor time**. Die meet het totale gebruik van de processor door alle lopende processen. In een toestel met meerdere processoren is dit een gemiddelde genomen over alle processoren.



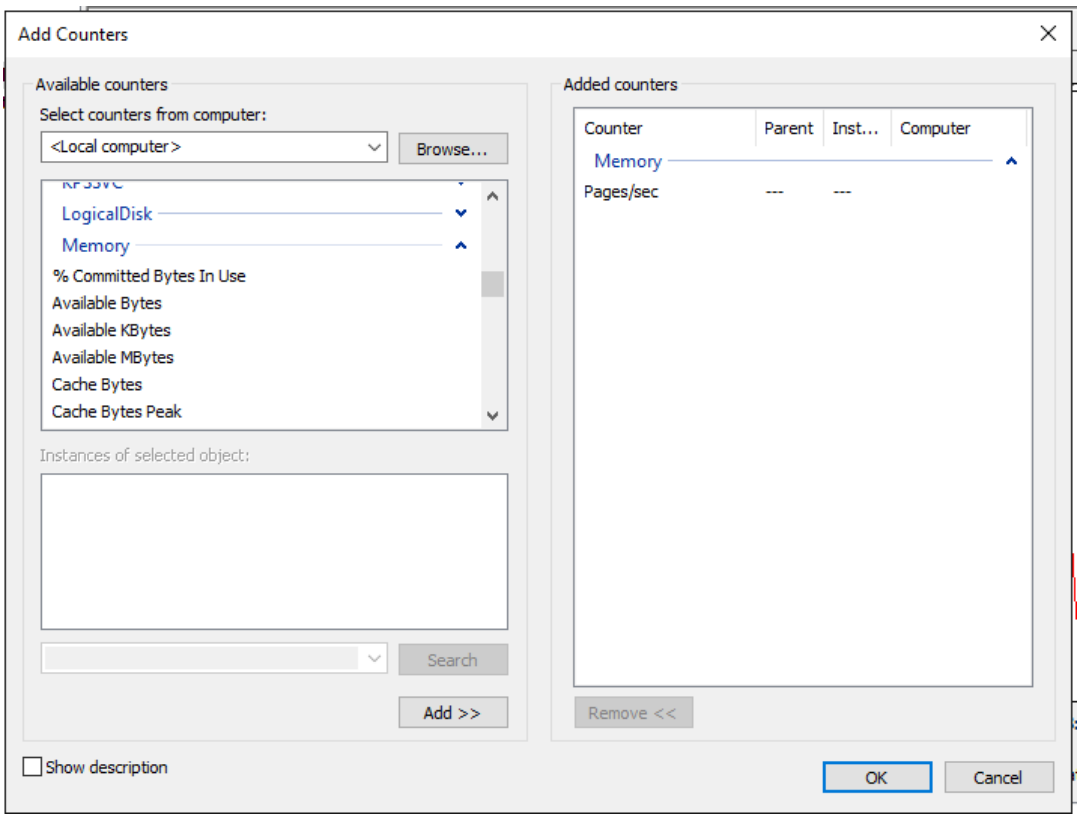
Een counter toevoegen

- Klik met de rechtermuisknop in de grafiek en kies **Add counters** in het snelmenu

Of

- Klik op de knop **Add counters** in de werkbalk 

Het dialoogvenster **Add counters** verschijnt.



Via de knop **Browse** kan je selecteren op welke computer je de metingen wenst uit te voeren. Standaard is dit de locale computer.

Opmerking
Door metingen uit te voeren op een ander toestel dan datgene waarop de performance monitor draait, beïnvloedt de werking van de performance monitor de gemeten waarden niet.

Onder de computer vind je een lijst met objecten.

- Klik op het **plusteken** naast het object om de counters die bij het object horen open te vouwen.

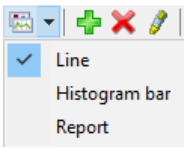
Eén van de objecten is **Memory** en een counter die daarbij hoort **Pages/sec**.

- Selecteer de counter Pages/sec vanhet object Memory.
- Plaats een vinkje bij **Show Description** om te weten te komen wat die counter juist meet. Pages / sec blijkt een teller te zijn die registreert aan welk tempo pages (4 KB) van de harde schijf naar intern geheugen gelezen worden of van RAM naar de harde schijf geschreven.
- Klik op **Add** en de meetresultaten voor de gekozen counter worden toegevoegd aan de grafiek.
- Klik op **OK** om terug te keren naar de grafiek.

Een andere weergave van een grafiek

Standaard worden de resultaten van de metingen als een lijngrafiek gepresenteerd. Dit grafiek type is geschikt om de evolutie van de gemeten waarde in de loopt van de tijd te volgen.

Via de knop **Change Graph Type** (de derde knop) in de werkbalk kan je ook vragen om de meetresultaten in de vorm van een histogram of van een rapport te tonen.



Een histogram verduidelijkt eerder de wijzigingen in de gemeten waarden.

Een rapport toont de gemeten waarde als getallen.

Een grafiek opslaan

Klik met de rechtermuisknop om het resultaat van de metingen op te slaan en kies **Save Settings as**.

Het resultaat van de systeem monitor kan in twee formaten opgeslagen worden:

HTML	het bestand kan achteraf terug geopend worden in een browser. Zolang systeem monitor opgestart blijft, wordt naargelang de stand van de knop Freeze display in de werkbalk, ook de grafiek in de browser aangepast.
.tsv	het bestand kan achteraf geopend worden met een tekst editor. Het resultaat van de metingen op het moment van het opslaan wordt geregistreerd in de vorm van getallen. De verschillende resultaten zijn van elkaar gescheiden met een tab.

Eigenschappen van systeem monitor

Klik ergens in de grafiek met de rechtermuisknop en kies **Properties**. Het dialoogvenster met de eigenschappen van de systeem monitor verschijnt.

Het tabblad **General** bepaalt welke elementen wel en welke niet op de grafiek getoond worden. In het deel **Report and histogram data** kan je ook kiezen om i.p.v. de huidige waarde het minimum, het maximum of het gemiddelde van de gemeten waarden weer te geven. Ten slotte kan je ook meegeven hoe frequent de metingen moeten gebeuren.

Je kunt met performance monitor niet alleen op dit moment gemeten waarden grafisch voorstellen. Je kunt ook kiezen om de waarden opgeslagen in een bestand of in een database te tonen.

Op het het tabblad **Source** kan je bepalen uit welk bronbestand de gegevens moeten getoond worden.

Het tabblad **Data** weerspiegelt welke counters momenteel opgenomen zijn en in welke kleur ze voorgesteld worden. Via de knop **Add** kan je nog andere counters toevoegen.

Eigenschappen van de grafiek kan je bepalen via het tabblad **Graph**. Hoe moet de grafiek eruit zien? Welke schaalverdeling wordt er gebruikt? ...

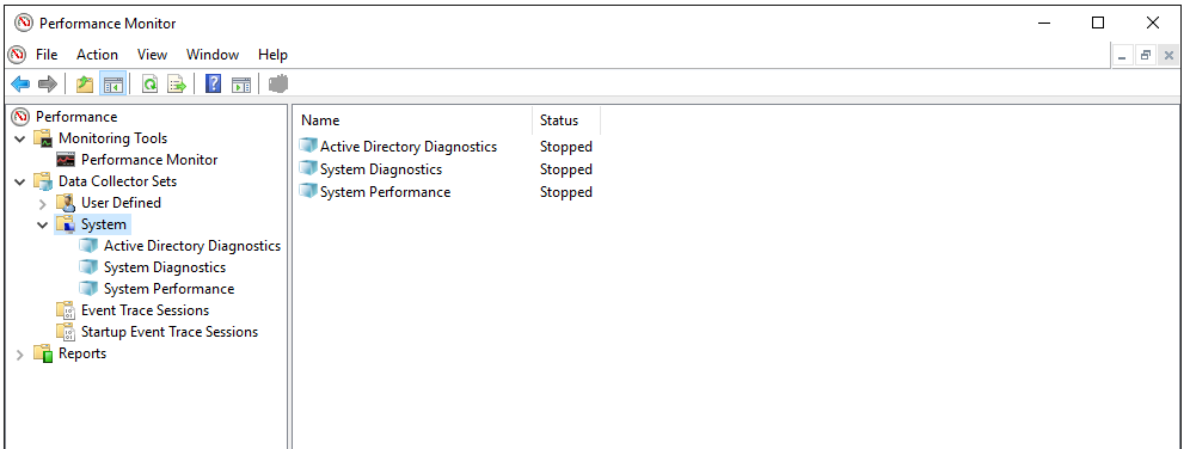
Via het tabblad **Appearance** kan je de opmaak van de verschillende onderdelen van de grafiek instellen

7.2 Metingen laten registreren in een logboek

Om de werking van de server op te volgen, zijn niet alleen de metingen van de huidige situatie relevant, maar kan het ook nuttig zijn om gegevens over een langere periode met elkaar te kunnen vergelijken.

Windows 2008 Server introduceerde daartoe Data Collector Sets en Rapporten.

Een data collector set is een verzameling objecten en counters die je wenst op te volgen en is in dat opzicht een meer geavanceerde uitgave van een counter log in eerdere versies van Windows.



Onder het knooppunt Data Collector sets vind je een verdere onderverdeling terug in sets gemaakt door gebruikers en sets gemaakt door het systeem.

- Open **Performance monitor** om een data collector set te maken
- Klik onder het knooppunt **Data Collector sets** met de rechtermuisknop op het knooppunt **User Defined**.
- Kies **New** en vervolgens **Data Collector Set**.
- Geef een naam op voor de data collector set, b.v. Memory Monitor en kies **Create Manually**.
- Klik op **Next**.

Bij **What type of data do you want to include?** kan je opgeven welk type Data Collector Set dit moet worden.

Performance counter	dezelfde informatie die je via performance monitor kunt verzamelen, maar dan geregistreerd in een data collector set i.p.v. een real time weergave.
Event trace data	vooral voor programma- en database ontwikkelaars interessante informatie zoals hoe dikwijls een bepaald event zich voordoet en welke thread het event veroorzaakt heeft. Deze informatie werd in eerdere versies verzameld via een trace log.
System Configuration data	informatie die te maken heeft met wijzigingen in de registry.

- Kies Performance counter
- In het venster **Which Performance Counters Would You Like To Log** klik je op **Add** en voeg je de performance counters toe die je wenst op te volgen.
- Voeg alle counters die met memory te maken hebben toe.

Hier kan je ook opgeven om de hoeveel tijd er een meting moet gebeuren.

- Behoud de standaardwaarde van 15 seconden.

Kies de plaats waar het bestand mag opgeslagen worden in het volgende venster en klik op **Next**.

Op de volgende pagina kan je kiezen met welke rechten het loggen moet uitgevoerd worden. Default komt overeen met de default system account.

- Behoud default.

De drie opties onderaan hebben te maken met wat er vervolgens moet gebeuren.

- Om nog verder instellingen mee te geven voor de data collector set kies je **Open properties for this data collector set**.
- Klik op **Finish**.

De eigenschappen van een data collector set kunnen ook opgeroepen worden door met de rechtermuisknop op de set te klikken en vervolgens **Properties** te kiezen.

Hier vind je op de verschillende tabbladen de via de wizard gevraagde instellingen terug.

Standaard dient het loggen manueel gestart te worden. Indien je het loggen wenst te starten volgens een vastgelegde planning kan je dat instellen via het tabblad **Schedule**. Het tabblad **Stop Condition** geeft de mogelijheid om te bepalen wanneer het loggen moet stoppen.

7.3 Data collector rapporten

Om problemen op te lossen zal je niet alleen data willen verzamelen over een bepaalde periode, maar zal je ook de data achteraf willen bekijken om ze te analyseren.

Bij elke data collector set, vind je dan ook data collector rapport. En net zoals de data collector sets zelf zijn ook de rapporten onderverdeeld in twee categorieën: user defined en system.

- Start de systeem monitor en klik met de rechtermuiknop op het knooppunt Performance Monitor. Kies vervolgens Properties.
- Activeer het tabblad Source.
- Kies daar in de rubriek Data Source voor **Log files** en klik op Add om een logbestand te openen.
- Selecteer het logbestand dat je wilt analyseren en klik op **Open**.
- Duid ook een tijdspanne aan. Sleep de linkse rand naar rechts om het starttijdstip en de rechtse rand naar links om het stoptijdstip te bepalen.
- Activeer nu het tabblad Data. Via Add kan je de counters selecteren die je wilt bekijken.
- Klik op **OK**

7.4 Performance Counter Alerts

Alerts kunnen een beheerder melden wanneer bepaalde gebeurtenissen zich voordoen of wanneer een bepaalde drempel bereikt wordt.

De waarschuwing kan in de vorm van een netwerk bericht afgeleverd worden of kan geregistreerd worden in het Application logboek.

Het aanmaken van een performance counter alert gebeurt op analoge manier als het aanmaken van een andere data collector set.

- Selecteer in het navigatiepaneel onder het knooppunt **Data Collector Sets** het knooppunt **User defined** en klik met de rechtermuisknop op het knooppunt
- Kies **New > Data collector set**.
- Geef een naam aan de nieuwe data collector set, b.v. Full Disk en kies de optie Create Manually (Advanced).
- Selecteer bij **What type of data do you want to include** de optie **Performance counter alert**.
- Voeg bij **Which performance counters would you like to monitor** de gewenste counters toe. Kies b.v. het object **Logical Disk** en daaronder de counter **%Free Space**.

- Klik op OK. Je belandt terug in het venster Which performance counters would you like to monitor.

- Selecteer een counter en vul onderaan bij **Alert When** een grenswaarde in die een waarschuwing moet veroorzaken en hoe er met de grenswaarde moet vergeleken worden.

Voer de wizard verder uit. De stappen komen overeen met die beschreven om een data collector set te maken.

7.5 Problemen opsporen met performance monitor

7.5.1 Hoe druk heeft de server het?

Hieronder een overzicht van een aantal belangrijke objecten die informatie geven over het gebruik van de processor.

Object	Counter	Wat wordt gemeten
Processor	Total\%processor time Opmerking: In de taskmanager komt deze waarde overeen met CPU Usage	Het totale gebruik van de processor door alle lopende processen. In een toestel met meerdere processors wordt een gemiddelde over alle processors genomen.
Process(instance) Processor(inetinfo) Processor(store)	%processor Time	Om per proces na te gaan hoeveel het van de processortijd in beslag neemt. IIS Exchange

Een hoge waarde op bepaalde momenten, b.v. als een backup loopt is normaal. Een gemiddelde rond 70 à 80 % is OK. 20 à 30% betekent dat de machine niet optimaal gebruikt wordt.

Object	Counter	Wat wordt gemeten?
Processor(_Total)	% Privileged Time	Tijd gebruikt door kernel processen, te hoog betekent waarschijnlijk dat de processor maar juist de opdrachten van het OS aankan.
Processor(_Total)	% User time	Tijd gebruikt door user processen. Te hoog betekent dat het toestel te veel rollen, te veel extra programma's aanbiedt.

System	Processor queue length	Lang betekent dat er veel threads staan te wachten op uitvoering en dat kan erop wijzen dat er te veel werk is voor de processor. Meer dan 5 met een gebruik van de CPU van 100% is zeker een indicatie.

7.5.2 Werkt de hardware naar behoren?

Object	Counter	Wat wordt gemeten?
System	Context Switches / sec	Hoe dikwijls moet de processor overschakelen van kernel naar user mode om een request van een thread die in user mode loopt af te handelen? Deze waarde zou altijd nogal ongeveer hetzelfde moeten blijven. Een plotse wijziging kan wijzen op een hardware device dat niet naar behoren functioneert.
Processor(_Total)	Interrupts / sec	Te gebruiken samen met de vorige Een plotse stijging kan ook op een slecht functionerend hardware device wijzen Indien deze waarde niet mee stijgt, wijst het erop dat een lopende applicatie te veel resources vraagt.
Laat de Context switches counter eerst gedurende een periode meten om een normale waarde vast te leggen.		
Processor(_Total) Processor(instance)	%Privileged time	Een plotselinge verhoging samen met Context switches kan wijzen op een driver van een apparaat die problemen schept. Geeft een mogelijkheid om de schuldige op te sporen.

7.5.3 Is er voldoende intern geheugen ter beschikking?

Object	Counter	Wat wordt gemeten?
Memory	Pages / sec	Een groot aantal paging operaties, kan er op wijzen dat er te weinig RAM ter beschikking is. Vanaf 20 kan dit op problemen wijzen.
Memory	Available bytes	>10% van het totale RAM geheugen wijst erop dat er zeker voldoende is.
Deze waarde kan best via een performance log opgevolgd worden, om te zien of er zich geen neerwaartse trend manifesteert. Laat een trigger genereren als de waarde onder 2% gaat.		
Process(instance)	Working set	Dit is een indicatie van het aantal gealloceerde pagina's dat het proces kan aanspreken zonder een page fault te genereren. In te stellen per proces om na te gaan welke processen veel RAM vragen.
Memory	Cache bytes	Meet de working set van het systeem. Hoeveel pagina's kan een kernelproces zonder problemen alloceren.
Memory	Transition faults / sec	Hoe dikwijls worden pagina's op de standby lijst terug opgeroepen. Een stijging kan er ook op wijzen dat er een te kort aan RAM is.

7.5.4 Zijn de schijven snel genoeg?

Object	Counter	Wat wordt gemeten?
Physical disk(instance)	Disk transfers/sec	Hoeveel lees- en schrijfbewerkingen worden afgewerkt per seconde. > 25 per schijf kan erop wijzen dat de schijf een bottleneck is.
Physical disk(instance)	% idle time	Hoeveel percent van de tijd is de schijf idle tijdens de meting.

		<20% wijst erop dat er waarschijnlijk een wachtrij gevuld wordt met requests voor de schijf.

7.5.5 Zijn er problemen met het netwerk?

Object	Counter	Wat wordt gemeten?
Server	Bytes Total / sec	Geeft een beeld van het tempo waaraan de server netwerk dat verzendt en ontvangt.
Server	Files open	Hoeveel bestanden zijn momenteel open. De teller weerspiegelt hoe zwaar het netwerkverkeer doorweegt.
Server	Server sessions	Hoeveel connecties zijn er momenteel gemaakt met de server? Hiermee kan je o.a. ontdekken of een server ook bezig als er helemaal geen netwerkverkeer zou mogen zijn.
Network interface	Bytes Total /sec	Het tempo waaraan de netwerkkaart data verzendt en ontvangt. Als deze waarde te laag is kan dat wijzen op problemen met de netwerkkaart.

8 COLOFON

Sectorverantwoordelijke:	
Cursusverantwoordelijke:	Bjorn Smeets
Didactiek:	
Lay-out:	
Medewerkers:	Vakgroep systeembeheer
Versie:	Oktober 2021
Nummer dotatielijst:	