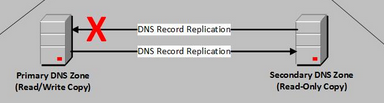
## Vraag 1: Wat is het nut van secondary Dns zone + vb

High availability, backup, redundancy  
Fault tolerant  
Balance the load  
Server 1 heeft een DNS zone, Server 2 heeft een secondary DNS zone die een copy is van de DNS zone van server 1. Als beide servers werken dan wordt de workload verdeeld over de 2 servers. Als de eerste server uitvalt dan zal de 2de nog steeds werken en geraken we nog steeds aan de DNS zone.

Een secondary DNS zone maakt een kopie van een DNS zone die al bestaat op een andere server. Dit zorgt ervoor dat de workload gebalanceerd wordt en geeft fout tolerantie. De secondary DNS zone is read only en kan dus geen nieuwe records aanmaken of records wijzigen.  
Moest de eerste dns server plat liggen dan kan de tweede dns server als backup gebruikt worden.  
Vb.: De eerste server heeft een DNS zone google.be, op een tweede server wordt een secondary DNS zone gemaakt.

Secondary zone  
When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.  
The secondary DNS zone is the read-only copy of the DNS records. This means that the DNS records cannot be added directly to the secondary DNS zone. The secondary DNS zone can receive the updated records only from the primary DNS zone of the DNS server.  


Purpose  
The purpose of a secondary zone is to simply host the same zone on a secondary DNS server so that you can provide a highly avaiable, fault tolerant DNS solution.  
Updates to the zone are made on the primary zone. These updates are then transferred over to the DNS server(s) hosting the secondary zone. More than one DNS server can host a secondary zone. In a simple example, if you clients are configured to use more than one DNS server, if one server fails, the client can simply query the other DNS server which is also hosting a copy of the same zone. therefore, name resolution will continue even though one DNS server is offline.

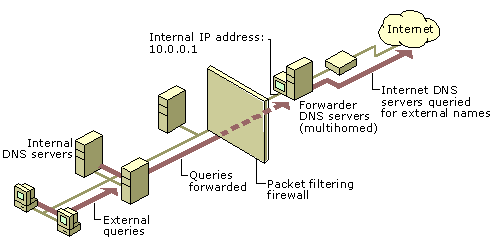
The major point in having a secondary DNS server is as backup in the event the primary DNS server handling your domain goes down. In this case, your server would be still up, and so without having a backup, nobody could get to your server possibly costing you lots of lost customers (i.e. REAL MONEY).  
A secondary DNS server is always up, and ready to serve. It can help balance the load on the network as there are now more than one authoritative place to get your information. Updates are generally performed automatically from the master DNS. Thus it is an exact clone of the master.  
Generally a DNS server contains more information than just a single server, it might contain mail routing information, information for many many hosts, mail spam keys, etc. So resilancy and redundancy are of DEFINITE benefit to domain holders.

## Vraag 2: Wat is het verschil tussen dns bij ip settings en dns bij dns forwarding

When the DNS server receives a query, it attempts to resolve this query by using the zones that it hosts and by using its cache.  
If the query cannot be resolved using local data, the DNS server forwards the query to the DNS server that is designated as a forwarder.  
If forwarders are unavailable, the DNS server attempts to use its root hints to resolve the query. (root hints work slower than forwarders)  
When a DNS server forwards a query to a forwarder, it sends a recursive query to the forwarder. This is different than the iterative query that a DNS server sends to another DNS server during standard name resolution (name resolution that does not involve a forwarder).

Bij DNS bij IP settings wordt er een request gestuurd naar de DNS server en dan wordt er van de DNS server een reply teruggestuurd.  
BV: Client 🡪 DNS server (zonder forwarders) 🡪 Client  
  
Bij DNS forwarding wordt er een request naar de DNS server gestuurd (Met forwarder). Deze wordt dan doorgestuurd naar andere servers tot de FQDN (fully qualified domain name) gevonden is of er geen forwarders meer zijn. Daarna wordt hij over hetzelfde pad teruggestuurd.

Client 🡪 DNS Server 1 (Met forwarder) 🡪 DNS Server 2 (met Forwarder) 🡪 DNS Server 3 (bv 8.8.8.8 aka google) 🡪 DNS Server 2 🡪 DNS server 1 🡪 client

DNS forwarding  
You designate a DNS server on a network as a forwarder by configuring the other DNS servers in the network to forward the queries that they cannot resolve locally to that DNS server. By using a forwarder, you can manage name resolution for names outside your network, such as names on the Internet, and improve the efficiency of name resolution for the computers in your network.  
  
When you designate a DNS server as a forwarder, you make that forwarder responsible for handling external traffic, which limits DNS server exposure to the Internet. A forwarder builds up a large cache of external DNS information because all the external DNS queries in the network are resolved through it. In a small amount of time, a forwarder resolves a large number of external DNS queries using this cached data. This decreases the Internet traffic over the network and the response time for DNS clients.  
A DNS server that is configured to use a forwarder behaves differently than a DNS server that is not configured to use a forwarder. A DNS server that is configured to use a forwarder behaves as follows:  
When the DNS server receives a query, it attempts to resolve this query by using the zones that it hosts and by using its cache.  
If the query cannot be resolved using local data, the DNS server forwards the query to the DNS server that is designated as a forwarder.  
If forwarders are unavailable, the DNS server attempts to use its root hints to resolve the query..  
When a DNS server forwards a query to a forwarder, it sends a recursive query to the forwarder. This is different than the iterative query that a DNS server sends to another DNS server during standard name resolution (name resolution that does not involve a forwarder).

DNS forwarding is the process by which particular sets of DNS queries are handled by a designated server, rather than being handled by the initial server contacted by the client. Usually, all DNS servers that handle address resolution within the network are configured to forward requests for addresses that are outside the network to a dedicated forwarder.  
The terminology around DNS forwarding can be a bit confusing because the forwarder has DNS queries forwarded to it by DNS servers that aren’t forwarders — try saying that five times quickly! The DNS forwarder should be thought of as the designated server to which a particular subset of queries (either for external addresses or specific internal addresses) are forwarded by other DNS servers within the network. It then sends (forwards) those requests for resolution to other DNS servers.

## Vraag 3: wat is folder redirection, toepassing en security rechten

Folder Redirection lets administrators redirect the path of a folder to a new location. The location can be a folder on the local computer or a directory on a network file share. Users can work with documents on a server as if the documents were based on a local drive. The documents in the folder are available to the user from any computer on the network.

Zo kunnen users vanop elke computer op het netwerk aan hun bestanden. Het wordt vaak gebruikt samen met roaming profiles.  
If you use Roaming User Profiles, you can use Folder Redirection to reduce the total size of your Roaming Profile and make the user logon and logoff process more efficient for the end-user. When you deploy Folder Redirection with Roaming User Profiles, the data synchronized with Folder Redirection is not part of the roaming profile and is synchronized in the background by using Offline Files after the user has logged on. Therefore, the user does not have to wait for this data to be synchronized when they log on or log off as is the case with Roaming User Profiles.  
Het wordt ook gebruikt om je bestanden netjes te schijden van je besturingssysteem door naar een andere schijf te redirecten. Zo kan je zonder gegevens te verliezen je besturingssysteem herinstaleren.

Create a security group for users who have redirected folders on a particular share and limit access only to those users  
Create a hidden share by putting a dollar sign ($) after the share name. The share is not visible in the network neighborhood.  
Grant users the minimum permissions that are required to access the data.

Folder redirection zorgt ervoor dat het pad van een map veranderd/verwezen (ge-redirect) wordt naar een andere locatie . De locatie kan een map zijn die lokaal op de PC staat of op een netwerk share.

Dit wordt gebruikt zodat users kunnen werken op verschillende computers op het netwerk en toch nog hun bestanden kunnen behouden alsof ze op een lokale schijf werken.

security rechten: De users kunnen in hun mappen maar de admin niet.

folder redirection  
User settings and user files are typically stored in the local user profile, under the Users folder. The files in local user profiles can be accessed only from the current computer, which makes it difficult for users who use more than one computer to work with their data and synchronize settings between multiple computers. Two technologies exist to address this problem: Roaming Profiles and Folder Redirection. Both technologies have their advantages, and they can be used separately or together to create a seamless user experience from one computer to another. They also provide additional options for administrators managing user data.  
Folder Redirection lets administrators redirect the path of a folder to a new location. The location can be a folder on the local computer or a directory on a network file share. Users can work with documents on a server as if the documents were based on a local drive. The documents in the folder are available to the user from any computer on the network.

Advantages

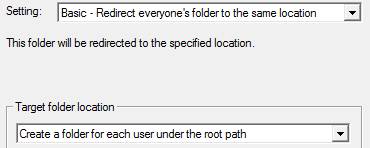
* Even if users log on to different computers on the network, their data is always available.
* Offline File technology (which is turned on by default) gives users access to the folder even when they are not connected to the network. This is especially useful for people who use portable computers.
* Data that is stored in a network folder can be backed up as part of routine system administration. This is safer because it requires no action by the user.
* If you use Roaming User Profiles, you can use Folder Redirection to reduce the total size of your Roaming Profile and make the user logon and logoff process more efficient for the end-user. When you deploy Folder Redirection with Roaming User Profiles, the data synchronized with Folder Redirection is not part of the roaming profile and is synchronized in the background by using Offline Files after the user has logged on. Therefore, the user does not have to wait for this data to be synchronized when they log on or log off as is the case with Roaming User Profiles.
* Data that is specific to a user can be redirected to a different hard disk on the user's local computer from the hard disk that holds the operating system files. This makes the user's data safer in case the operating system has to be reinstalled.
* As an administrator, you can use Group Policy to set disk quotas, limiting how much space is taken up by user profile folders.

Security

* Create a security group for users who have redirected folders on a particular share and limit access only to those users
* Create a hidden share by putting a dollar sign ($) after the share name. The share is not visible in the network neighborhood.
* Grant users the minimum permissions that are required to access the data.
* Create a security group for users who have redirected folders on a particular share and limit access only to those users  
  Create a hidden share by putting a dollar sign ($) after the share name. The share is not visible in the network neighborhood.  
  Grant users the minimum permissions that are required to access the data.

## Vraag 4: nieuwe user, logon hour restrictions en folder redirection op documents

1. Tools 🡪 Active Directory Users And Computers 🡪 In de domein map , in de user map , in de afdelings map 🡪 Nieuwe user aanmaken en toevoegen aan de Global group van die afdeling.
2. Aangemaakte User rechts op klikken 🡪 Properties 🡪 Account 🡪 Logon Hours…
3. Tools 🡪 Group Policy Management 🡪 Create new GPO in folder van gewenste afdeling 🡪 benoem deze Documents Redirection 🡪 rechts klikken , Edit GPO 🡪 User configuration 🡪 Windows Settings 🡪 Folder Redirection 🡪 op Documents rechts klikken , Properties 🡪 stel pad in



## Vraag 5: Hoe maak je een Domain controller?

Server 2008: in Run typ dcpromo , volg de stappen  
Server 2012: Add Roles 🡪 ADDC 🡪 promote to Domain controller 🡪 volg stappen

## Vraag 6: Wat is (en het verschil) forward lookup zone en backward lookup zone? Wat is Cname?

In most Domain Name System (DNS) lookups, clients typically perform a forward lookup, which is a search that is based on the DNS name of another computer as it is stored in a host (A) resource record. This type of query expects an IP address as the resource data for the answered response.  
DNS also provides a reverse lookup process, in which clients use a known IP address and look up a computer name based on its address. A reverse lookup takes the form of a question, such as "Can you tell me the DNS name of the computer that uses the IP address 192.168.1.20?"

Cname-records:

Vaak zal een toestel verschillende taken hebben bv een ftp- en een http- server, deze wil je dan onderscheiden met verschillende namen bv ftp.vdab.be en www.vdab.be. Beide verwijzen wel naar hetzelfde adres 193.53.101.103. Hiervoor maken we dan een alias of een Cname-record.

Een Forward lookup zone gaat de hostnames omzetten naar ip adressen , een Backward Lookup zone gaat het IP adress omzetten naar een hostname

In most Domain Name System (DNS) lookups, clients typically perform a forward lookup, which is a search that is based on the DNS name of another computer as it is stored in a host (A) resource record. This type of query expects an IP address as the resource data for the answered response.  
DNS also provides a reverse lookup process, in which clients use a known IP address and look up a computer name based on its address. A reverse lookup takes the form of a question, such as "Can you tell me the DNS name of the computer that uses the IP address 192.168.1.20?"

As you divide your Domain Name System (DNS) namespace into domains, you also divide your DNS namespace into one or more zones, each of which stores name information about one or more DNS domains. A zone is the authoritative source for information about each DNS domain name that is included in the zone. A forward lookup zone is the most common type of zone. DNS clients can use this zone to obtain such information as IP addresses that correspond to DNS domain names or services that is stored in the zone. Another type of zone, a reverse lookup zone, provides mapping from IP addresses back to DNS domain names.  
DNS also provides a reverse lookup process, in which clients use a known IP address during a name query and look up a computer name based on its address. A reverse lookup takes the form of a question, such as "Can you tell me the DNS name of the computer that uses the IP address 192.168.1.20?"

## Vraag 7: Wat is het verschil tussen een local, roaming en mandatory profile?

|  |  |
| --- | --- |
|  | Beschrijving |
| Local | Een profiel dat wordt opgeslagen op 1 PC. Gebruikers kunnen niet aan hun profiel vanop een andere PC, ookal is deze PC aangesloten op het netwerk. |
|  |  |
| Roaming | Een profiel dat wordt opgeslagen op het netwerk zodat op moment dat je inlogt op eender welke PC die geconnecteerd is met het netwerk, je profiel geladen wordt. |
|  |  |
| Mandatory | Een profiel dat niet kan opgeslagen worden van 1 sesie naar de andere. Een gebruiker kan de PC gebruiken die geconnecteerd is aan het netwerk maar op moment dat de gebruiker uitlogt, worden alle veranderingen aan het profiel gewist. |

### In welke gevallen zou je met een roaming werken?

In een organisatie waar mensen geen vaste computers/laptops hebben is het handig om met roaming profiles te werken. Zo kan iedereen inloggen op hun account vanaf elke computer/laptop.

### In welke gevallen met een mandatory?

In bijvoorbeeld een bibliotheek of ergens waar computergebruik verhuurd wordt. Op deze manier kan iedereen de computers tijdelijk gebruiken en als ze uitloggen wordt alles gereset zodat de volgende gebruiker ook een clean computer heeft.

### Wat zou je aanraden in een studentenomgeving?

Mandatory profiles waarbij studenten alleen dingen kunnen opslaan in hun eigen netwerk map.

## Vraag 8: Zet een vaste achtergrond op een nieuwe user .

Tools 🡪 Group Policy Management 🡪 User Configuration 🡪 Policies 🡪 Desktop 🡪 Desktop 🡪 Desktop Wallpaper

Een shared folder waar de afbeelding in staat en zorgen dat die niet verwijderd kan worden en dat alle gebruikers aan de afbeelding kunnen.

## Vraag 9: Hoe zorg je ervoor dat een webserver bereikbaar is via de url www .domeinnaam.be?

Tools 🡪 DNS 🡪 Forward Lookup Zone 🡪 New Primary Zone 🡪 noem deze domeinnaam.be 🡪 maak hierin een nieuwe CNAME aan en noem deze www 🡪 laat deze verwijzen naar de originele DNS , wat normaal domeinnaam.local is en daar de server kiezen.

### Wat is hier allemaal voor nodig en hoe gebeurt dit dan bijvoorbeeld vanaf een client PC?

* Je zorgt dat de web server + dns server geïnstalleerd zijn.
* Daarna maak de een nieuwe website aan met de naam: [www.domeinnaam.be](http://www.domeinnaam.be)
* Je maakt de html pagina’s enz aan, in de map van je website.
* Daarna ga je naar je DNS Server.
* Je maakt een nieuw domain: “domeinnaam.be” (zonder “”).
* In die nieuwe domain, in de map Forward Lookup Zone maak je een nieuwe host aan met de naam: “www” en dit verwijs je naar het ip address van je server.

## Vraag 10: Leg het principe AGDLP uit. Waarom is dit een goede werkwijze in een domein? Wat is het verschil tussen gl en dl?

AGDLP: account, global, domain local, permission

Global security groups

Domain security groups with global scope represent business roles or job functions within the domain. These groups may contain accounts and other global groups from the same domain, and they can be used by resources in any domain in the forest. They can be changed frequently without causing global catalog replication.

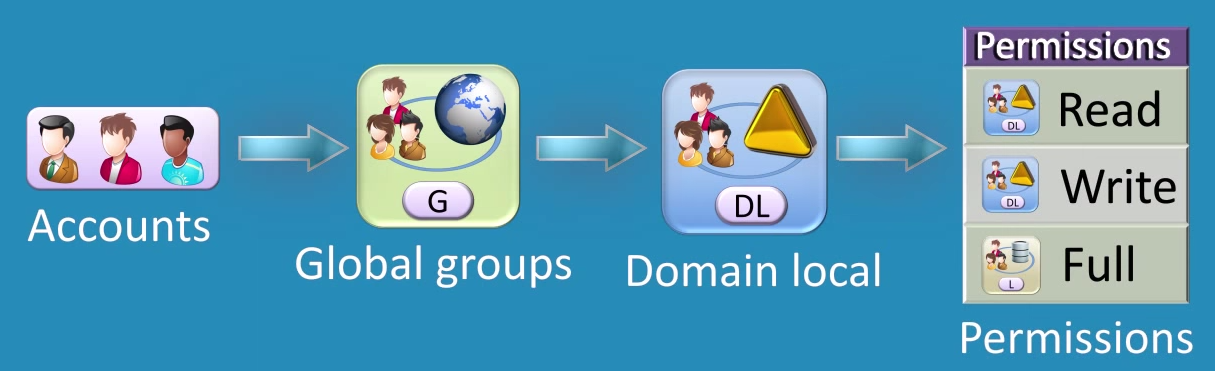
Domain local security groups

Domain security groups with domain local scope describe the low-level permissions or user rights to which they are assigned. These groups can only be used by systems in the same domain. Domain local groups may contain accounts, global groups, and universal groups from any domain, as well as domain local groups from the same domain.

Global groups that represent business roles should contain only user or computer accounts. Likewise, domain local groups that describe resource permissions or user rights should contain only global groups that represent business roles. Accounts or business roles should never be granted permissions or rights directly, as this complicates subsequent rights analysis.

Dit wordt gebruikt om permissies te geven aan je netwerk en dit gebruikt groepen op zo een manier dat om deze permissies en groepen te onderhouden enorm simpel is en zo geconfigureerd dat het andere domeinen hier toegang tot kan geven.

Permisies worden gegeven op basis van welke rol/ rollen een user heeft in je organisatie.  
Users hun permisies kunnen dus heel makkelijk veranderd worden als hun rol verandert  
je kan ook heel makkelijk zijn wie waarop toegang heeft.  
elke group heeft een andere scope, availability en member requirements.



DL group ColorPrintingAllowed provides access to the printer. De group kan niet gebruikt worden in een ander domein.  
Gl groups SalesUsers en Marketing users worden in DL gezet.

Doordat alleen dingen in hetzelfde domein toegang hebben kan je met zekerheid zeggen wie waartoe toegang heeft.

Een global group van een ander domein kan toegevoegd worden aan de domain local group

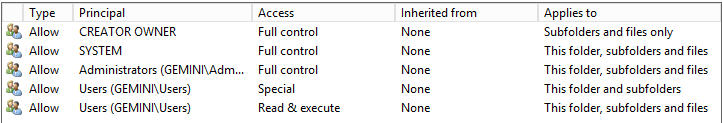


AGDLP (an abbreviation of "account, global, domain local, permission")

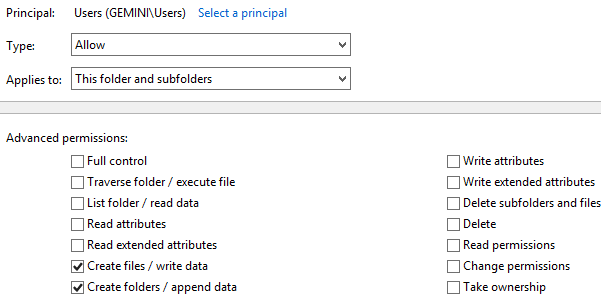
## Vraag 11: Maak een cashed roaming profile voor een nieuwe gebruiker "examen".

Zet het profiel in de share \\server\profiles$ met de correcte security- en share- instellingen.

Op de C schijf gaan: Nieuwe map aanmaken 🡪 profiles noemen 🡪 properties 🡪 sharing 🡪 advanced sharing 🡪 naam = profiles$ 🡪 sharing permissions in dit zelfde scherm Everyone FC 🡪 Security ziet er als volgt uit:



Special permission



Dit wordt gedaan zodat de gebruikers mappen niet kunnen deleten van andere mensen. En de map profiles op zich niet.

## Vraag 12: Wat is het verschil tussen share permissions en NTFS permissions?

Share Permissions

Share permissions are generally used when dealing with folders shared over a network or across multiple user accounts. By changing a folder's share permissions, you can grant or prevent access to it on a user-by-user, group-by-group or all-encompassing basis. The available share permission settings are "Full Control," "Change" and "Read." The Read setting only allows users to view the folder's contents. The Change setting allows users to change but not delete the folder's contents. The Full Control setting encompasses both of the other settings and also allows deleting.

NTFS Permissions

NTFS permissions are used to control permissions over networks and on local computers. When you change a folder's NTFS permissions, you can select individual users, groups or specific user account types -- administrators, for example. NTFS permissions are more in-depth than shared permissions as they are more oriented towards system control rather than sharing control. The available NTFS permission settings are "Full Control," "Modify," "Read & Execute," "List Folder Contents," "Read" and "Write." The Modify setting allows users to change files inside the folder, Read & Execute allows users to view and run files, List Folder Contents allows viewing its files and Write allows adding new files. Full Control and Read are the same as their setting counterparts in the share permissions.

Share permissions zijn permissions die bij het sharen van een folder ingesteld worden. Deze bepalen welke toegang anderen op het netwerk hebben op deze gesharede map. Er zijn drie soorten share permissions: Full Control, Change, and Read.

NTFS permissions bepalen dan weer wat users kunnen doen met een folder of file over het network en local. Anders dan Share permissions geven NTFS permissions verschillende mogelijkheden qua permissions naast Full Control, Change, and Read die individueel of voor groepen kunnen ingestelf worden. Als er een conflict in persmissies onstaat heeft de strengste de voorrang.

OF

Het verschil is dat NTFS permissions lokaal toegepast worden en Share permissions over het netwerk.

|  |  |  |  |
| --- | --- | --- | --- |
| **sharing** | **security** | **lokaal recht** | **netwerk recht** |
| Full Control | FC | FC | FC |
| FC | Read | R | R |
| R | FC | FC | R |
| FC | RW | RW | FC |

Access to a folder on a file server can be determined through two sets of permission entries: the share permissions set on a folder and the NTFS permissions set on the folder (which can also be set on files). Share permissions are often used for managing computers with FAT32 file systems, or other computers that do not use the NTFS file system.  
Share permissions and NTFS permissions are independent in the sense that neither changes the other. The final access permissions on a shared folder are determined by taking into consideration both the share permission and the NTFS permission entries. The more restrictive permissions are then applied.

Share and NTFS are the two types of file permissions used on Windows computers. They function completely separate from each other but serve the same purpose: preventing unauthorized access. Before you change one type of permission or the other, it is important for you understand the differences between the two permission types.

Share Permissions

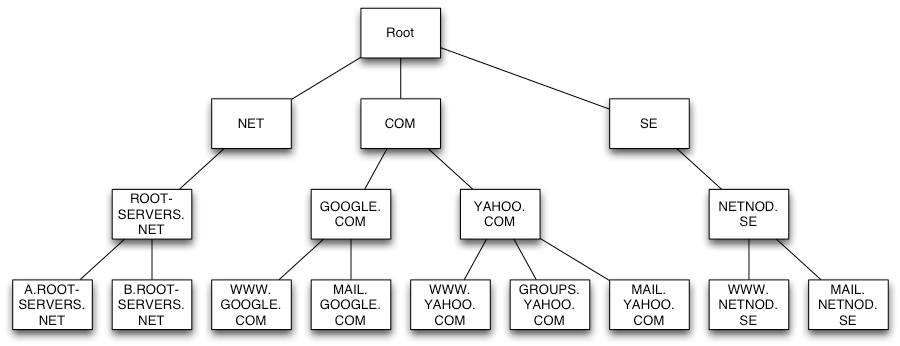
Share permissions are generally used when dealing with folders shared over a network or across multiple user accounts. By changing a folder's share permissions, you can grant or prevent access to it on a user-by-user, group-by-group or all-encompassing basis. The available share permission settings are "Full Control," "Change" and "Read." The Read setting only allows users to view the folder's contents. The Change setting allows users to change but not delete the folder's contents. The Full Control setting encompasses both of the other settings and also allows deleting.

NTFS Permissions

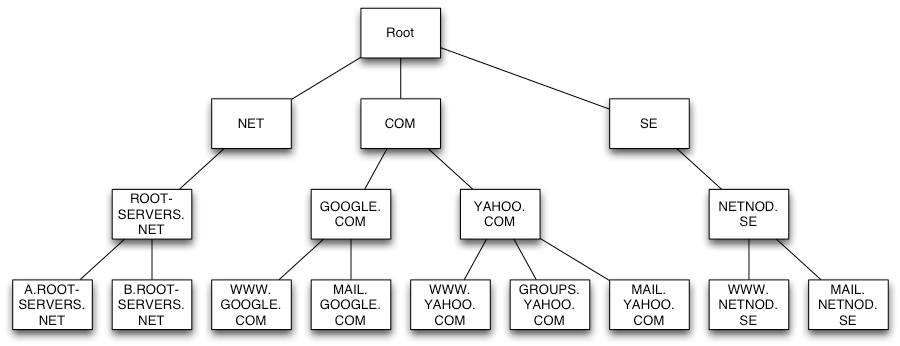
NTFS permissions are used to control permissions over networks and on local computers. When you change a folder's NTFS permissions, you can select individual users, groups or specific user account types -- administrators, for example. NTFS permissions are more in-depth than shared permissions as they are more oriented towards system control rather than sharing control. The available NTFS permission settings are "Full Control," "Modify," "Read & Execute," "List Folder Contents," "Read" and "Write." The Modify setting allows users to change files inside the folder, Read & Execute allows users to view and run files, List Folder Contents allows viewing its files and Write allows adding new files. Full Control and Read are the same as their setting counterparts in the share permissions.

## Vraag 13: Leg uit hoe een DNS opzoeking tewerk gaat met de de root DNS server enz.

hosts-bestand?  
nameserver ISP?  
root name server (kijkt naar .com <= TLD nameserver)  
TLD nameserver (domeinnaam <= authoritaire nameserver van het domein)  
authoritaire nameserver van het domein (<= IP adres)



First, your Internet Provider has to contact one of 13 root name servers to find out the IP address of a name server for the top level domain. Top level domains are .COM/.NET/.BIZ/.CA/etc.  
Next, your Internet Provider will contact the top level domain name server (.COM in the example above) and ask it for the authoritative name server's IP address. Now that your Internet provider has found the authoritative name server, it is able to get the IP address for the domain. The Internet Provider's DNS server will update its local cache so it knows the IP address the next time it receives a query. The website IP address is returned to your computer and this enables you to load the website in your browser



OF

Wanneer je in een browser het adres van een website ingeeft, dan gebeurt er een complexe opzoeking in de wereldwijde nameserver infrastructuur. Die is hierarchisch opgebouwd.

Als voorbeeld nemen we www.google.be

* Het adres “www.google.be” wordt eerst opgezocht in het hosts-bestand.
* Wordt het daar niet gevonden, dan wordt er een opzoeking gedaan in de nameserver van de ISP (bijv. Telenet). Die fungeert als caching nameserver (“recursor”) en slaat enkel informatie op van vorige opzoekingen.
* Als er geen resultaat is in de nameserver van de ISP, dan wordt er een opzoeking gedaan in de root nameserver.
* De root nameserver zal enkel kijken naar de extensie (“TLD”), dus “.be”. Op basis van de extensie zal er worden doorverwezen worden naar de correcte TLD nameserver. In dit geval zal er verwezen worden naar de nameservers van DNS.be. Dit resultaat wordt teruggestuurd naar de nameserver van de ISP.
* De nameserver van de ISP zal daarna een opvraging doen bij de TLD nameserver, in ons voorbeeld dus de nameservers van DNS.be. De TLD nameserver zal enkel kijken naar de domeinnaam “google.be” en verwijzen naar de authoritaire nameserver van het domein. Dit resultaat wordt teruggestuurd naar de nameserver van de ISP.
* De nameserver van de ISP zal daarna een opvraging doen bij de authoritaire nameserver van het domein. Die bevat de informatie over alle hostnames van “google.be”. De authoritaire nameserver van het domein zal het correcte IP-adres terugsturen naar de nameserver van de ISP.
* De nameserver van de ISP stuurt het correcte IP-adres terug naar de browser. De browser kan nu een verbinding opzetten met de correcte webserver.
* De nameserver van de ISP zal het correcte IP-adres opslaan gedurende de Time-to-live periode. Alle volgende aanvragen voor de hostnaam zullen nu vanuit de cache gebeuren.
* Na het verstrijken van de TTL-periode wordt de informatie van de hostnaam terug uit de cache van de nameserver van de ISP gewist.

Caching in de nameservers van de ISP gebeurd om het aantal aanvragen bij de nameservers te beperken en zo de snelheid te verhogen.

De TTL periode, de periode dat er caching gebeurd, ligt meestal tussen 900 seconden (15 minuten) en 86400 seconden (24 uur). De TTL kan ingesteld worden per domeinnaam op de authoritaire nameservers van het domein in het SOA record.

Compared to many other services on the Internet this service is rather unspectacular. The function and content of the root zone file are what make it special and cause it to be at the focus of increased attention. The root zone file is at the apex of a hierarchical distributed database called the Domain Name System (DNS). This database is used by almost all Internet applications to translate worldwide unique names like www.isoc.org into other identifiers; the web, e-mail and many other services make use of the DNS.

They are part of the Domain Name System (DNS), a worldwide distributed database that is used to translate worldwide unique domain names such as www.isoc.org to other identifiers. The DNS is an important part of the Internet because it is used by almost all Internet applications.  
The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located; in other words: which server one has to ask for names ending in one of 267 (September 2007) TLDs, such as ORG, NET, NL or AU. Read the detailed description of how the DNS works and the role of the root name servers.

DNS was made, just because we humans are not capable enough to remember numbers, or i must say we can remember names better than numbers. But computer's and network addresses are always numbers. So there must be some technology in between that will sit and translate names to number's. But as i just said, computers are named only in number's, and even if there is a computer that will sit and translate you or give you the number associated with a name, you first need to know the number of that particular computer that will help you translate names to numbers.

And there is no solution other than at least remembering the number of that particular computer who will do the job of translation for you. That initial number that every DNS software needs to know are referred to as DNS root servers. In fact these root servers never does the complete job of translation, but its only a starting point of the entire translation procedure.  
www. example.com.  
Although we humans will read it like www dot example dot com. The computer(your local DNS server) that will initiate the job of translation will start reading it from right to left rather than left to right. It will be something like dot com example www(yeah i understand that's gibrish but that's how it works). If you are a system administrator, then the below articles about DNS might prove helpful to you.  
So the translating computer will begin its job from right to left, with dot com example www. The first dot, indicates root servers. DNS server computer/software must know the number(numerical IP address) of them, because they are the starting point, as i told before in the job of the entire translation procedure. There are 13 IP addresses/number of these DOT server's that every DNS software's already know by default.

## Vraag 14: Leg uit: Forest, tree, child domain.

**Forest**

Een AD DS hoort bij 1 forest en omgekeerd.  
Een reden voor meerdere forest is als test netwerk of voor het isoleren van erg gevoelige data.  
In elk forest vindt je minstens 1 domein.

**Trees**

Een tree is een hierarchisch gestructureerde verzameling domeinen in eenzelfde namespace.

De reden voor een 2de tree op te zetten is om een tweede namespace te maken binnen eenzelfde forest.

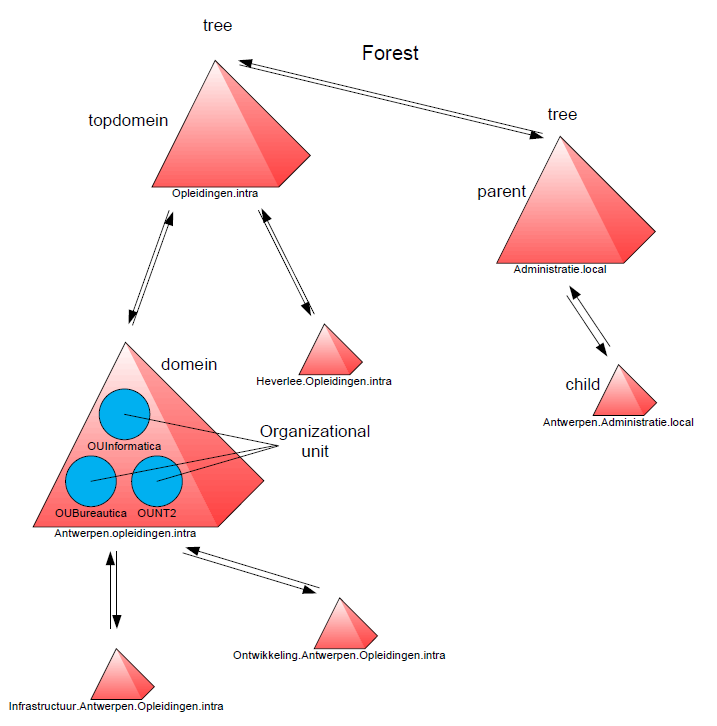
**Domein**

Elk domein beschikt over een eigen database met gebruikers, computers, enz. Een server waarop deze database bestaat en beheerd wordt, is een domeincontroller.  
Een domein is dus een verzameling resources en gebruikers die centraal kunnen beheerd worden aan de hand van 1 enkele database.  
Elk domein beschikt over minstens 1 domeincontroller en elke domeincontroller hoort maar bij 1 domein.

Het is beter om meerdere domeincontrollers op eenzelfde domein te maken voor fouttolerantie of om de werkdruk te spreiden.  
Een reden voor meerdere domeinen is 2 verschillende personenen die elk een domein beheren, beperking van het replicatieverkeer, beperking verkeer over een trage verbinding, beperking van de grootte van de AD Database.

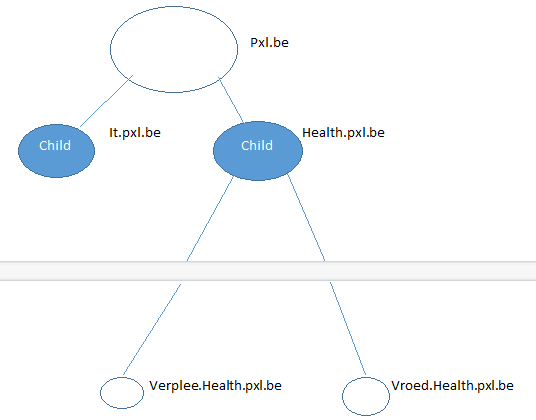
**Parent vs Child**

Een domein kan uit meerdere children domeinen bestaan. Het parent domein is dan de leider over zijn children maar elk child beheerd zichzelf ook.



Bij Active Directories werken we met forests, trees en child domains. Een forest is een complete Active Directory instance. Een forest is opgesteld uit tree domains, tree domains zijn collecties van domains die gegroepeerd zijn. De gegroepeerde domains noemen we child domains.

OF

Een Tree is eigenlijk een subddomein van u hoofddomein bv : IT = IT.PXL.local, Health = Health.PXL.local  
Een child is een domein dat onder een tree domein volgt of een ander child domein   
bv : verpleegkunde = Verpleegkunde.Health.PXL.local  
Een forrest is hetgene dat deze domeinen samenhoudt ook het hoofdomein. Zodat deze tree domeinen met elkaar kunnen communiceren. Bv : PXL = PXL.local 

## Vraag 15: Zorg dat intranet.uwdomein.be bereikbaar is. (Dan moet je een CNAME voorzien in uw DNS forwarding zones).

## Vraag 17: Je wilt op een website [www.kstv.be](http://www.kstv.be) maar die staat ook op de domein bec.local, wat heb je hiervoor nodig?

nieuwe lookup zone genaamd kstv.be  
daarin alias CNAME www

## Vraag 18: Wat is ADGLP? Hoe stel je dit op? Op welke groepen zet je de permissies? En waarom niet op de andere groep?

"AGDLP = account, global, domain local, permission"  
Accounts gaan in Global groups. Global groups gaan in Domain Local groups. Domain Local groups worden toegepast aan permissions.  
Global groups kunnen rechten en permissions krijgen. Een global group kan enkel accounts bevatten die van zijn eigen domain zijn.  
Domain local groups kunnen 'security group rights' en permissions geven worden over resources die ter beschikking zijn in de domain local group. De Domain local group kan andere domain -, global - en universal groups bevatten.

OF

AGDLP: account, global, domain local, permission

Tools 🡪 Active Directory Users And Computers 🡪 OU map aanmaken domein 🡪OU user map aanmaken 🡪 OU map maken van alle gewenste afdelingen 🡪 Nieuwe users aanmaken in gewenste afdelingen 🡪 Global en Domain Local groups aanmaken in afdelingen🡪 toevoegen users aan de Global group van die afdeling 🡪 Global group toevoegen aan Domain Local Group van de afdelingen

Je zet op de Domain Local u policies omdat een Domain Local group is voor alles Users die op dat domein zitten ingelogd of op het parent domein. Global is enkel binnen hun eigen domein. Vind de vraag wat wazig dus weet niet wat het antwoord effectief is, dus daarom maar een samenvatting hieronder.

|  |  |
| --- | --- |
|  | Beschrijving |
| Domain Local group | Is een security of een distribution group dat Universal groups, global groups, andere domain local groups kan bevatten van zijn eigen domein en account van welk ander domein in de forrest. |
|  |  |
| Global group | Is een group dat kan gebruikt worden in zijn eigen domein, in andere servers, in workstations van het domein en in trusting domains. In al deze locaties, kunt ge een global groep rechten en permissies geven. De global groep kan lid worden van local groups, maar een global group kan enkel users bevatten van zijn eigen domein. |
|  |  |
| Universal group | Is een sucirty of een distribution groep dat users, groepen en compukan een universal groep rechten en permissies geven op eender welk bestand in eender welk domein in de forrest. |

# Extra

## Vraag 19: VPN en Remote desktop uitleggen (overeenkomsten, verschillen en welke wanneer gebruiken)

RDP is een protocol om een desktop te repliceren over een netwerk connectie  
VPN laat je toe om connectie te maken met een netwerk dat normaal private is. Er wordt een point-to-point network geëmuleert waarbij de data die verstuurd wordt geëncrypteerd en ingecapsuleert wordt met een header (voor het beschermen van vertrouwbare informatie).

beide connecteren een desktop met de server, maar RDP repliceert een account op de desktop terwijl VPN een connectie simuleert met het netwerk.

VPN  
A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.[1] A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.

Remote desktop  
In computing, the term remote desktop refers to a software or operating system feature that allows a personal computer's desktop environment to be run remotely on one system (usually a PC, but the concept applies equally to a server), while being displayed on a separate client device. Remote desktop applications have varying features. Some allow attaching to an existing user's session (i.e., a running desktop) and "remote controlling", either displaying the remote control session or blanking the screen. Taking over a desktop remotely is a form of remote administration.

VPN  
Virtual Private Networks (VPNs) have been around for many years in the form of frame relay based networks before eventually becoming synonymous with IP-based data networking. With VPN, users have the ability to make a secure connection to a private network over unsecured networks such as public networks or the Internet. Two types of VPNs exist; remote access VPNs and site-to-site VPNs. Remote access VPNs are typically for individual users who are not at one fixed location, such as business travelers, while site-to-site VPNs usually consist of multiple users in fixed locations such as regional offices.

Remote desktop  
Remote Desktop Protocol (RDP) was developed by Microsoft. Starting with Windows XP, every version of Windows has had RDP technology included. RDP allows a user to remotely connect to another computer with the ability to view the remote desktop and control the keyboard and mouse as if it were physically connected to the remote machine.

Major Differences

While VPN and RDP may seem to be two separate technologies that accomplish the same goal, there are actually substantial differences between the two.

A Virtual Private Network (VPN) is just that, a private network. VPN runs on top of a larger network, such as any corporate network you'd find in an office building. Conversely, RDP is typically remote control of an individual computer, which may or may not reside on a network.

Furthermore, RDP allows access and control to a specific computer and the resources available on that computer. For example, any hard disk drives (both internal and external) that are connected to that computer, in addition to open networked resources would be available. Conversely, VPN allows access to shared network resources, which may not include the physical hard drives of individual machines, unless those drives are specifically shared on the network. Additionally, using RDP to connect to a machine on a network will not always mean that you'll have access to all of the networked connections that computer has.

Advantages/Disadvantages

There are different advantages and disadvantages to VPN and RDP connections:  
VPN is typically the easiest to troubleshoot as problems have a higher probability of being isolated.  
RDP is typically easier to use with higher bandwidth connections, but problems are usually harder to diagnose.  
VPN offers and additional level of security, as data traveling to the private network is encrypted before it hits the Internet, and decrypted once it reaches the private network. This additional level of security may be a plus for most, but this type of connection suffers from slower speeds than a non-encrypted method.

Remote Desktop Management  
Remote desktop programs (RDP) enable you to access the desktop of another computer over the Internet. RDP can be used to access files on your desktop at home while on vacation with your laptop. The program recreates the desktop, enabling you to explore the files and access the programs on it. This tool can also be useful for tech support tasks, as you can quickly access important information and try different troubleshooting techniques without waiting on the computer's owner or dealing with user error.

Virtual Private Networks  
Virtual Private Networks (VPN) are used to securely connect to and access materials on another network. VPNs use encryption to create a secure connection over a generally insecure connection like the Internet, enabling the transmission of potentially sensitive materials. VPNs are often used to connect to business networks from the home, enabling you to access the documents and data on your work computer without being in the building. VPNs also don't require you to connect to an online computer or workstation; all information is stored on the network itself.

Benefits and Drawbacks  
Both technologies have good and bad points. VPNs are secure and enable you to access networked materials while on the move or at home, which is useful for increasing productivity. VPNs sometimes suffer from lag issues, and the computer you're using to access them needs to have compatible programs installed to view every file type on the network. Without compatible software, some files will be unusable from your home computer. RDP solves this problem by using the resources of the computer to which you're connected, but may not be as secure. If someone else gains access to your RDP protocol, they can also hijack the computer and rob it of information. RDP also requires that the computer to which you're connecting is powered on and online.

Synergy Between the Two Technologies  
These two technologies aren't mutually exclusive. By using the two in tandem, you can actually create a more secure RDP experience. By connecting to the other computer via a VPN and controlling it using RDP, you can access your desktop remotely with greater security. Generally, using the two together is actually a better idea if you plan to use RDP, because of the increased security VPN offers.

## Vraag 20: Wat is dcpromo en hoe configureer je een active directory

dcpromo = promoveer tot domain controller. Met het programma dcpromo kan je de server upgraden naar een domain controller.

servermanager -> tools -> ad ds

## Vraag 21: Wat is DFS

- DFS staat voor Distributed File System en wordt gebruikt voor een file server, om mappen te beheren en te delen.

- Ook is het mogelijk (indien meerdere servers) om bestanden op alle servers te synchroniseren, en ervoor te zorgen dat elke server de bestanden ontvangen.

- Dit is mogelijk met de (Replication mode)

Distributed File System (DFS) is a set of client and server services that allow an organization using Microsoft Windows servers to organize many distributed SMB file shares into a distributed file system. DFS provides location transparency and redundancy to improve data availability in the face of failure or heavy load by allowing shares in multiple different locations to be logically grouped under one folder, or DFS root.

DFS namespaces  
Traditional file shares, associated with a single server, have SMB paths of the form \\<SERVER>\<path>\<subpath>. Domain-based DFS file share paths are distinguished by using the domain name in place of the server name, in the form \\<DOMAIN.NAME>\<dfsroot>\<path>. When a user accesses such a share, either directly or by mapping a drive, their computer will access one of the available servers associated with that share, following rules which can be configured by the network administrator. For example, the default behaviour is that users will access the closest server to them; but this can be overridden to prefer a particular server.  
If a server fails, the client can select a different server transparently to the user. One major caveat regarding this flexibility is that currently-open files will potentially become unusable, as open files cannot be failed-over.

DFS replication  
Early versions of DFS used Microsoft's File Replication Service (FRS) which provides basic file replication capability between servers. FRS identifies changed or new files, and copies the latest version of the entire file to all servers.  
Windows Server 2003 R2 introduced "DFS Replication" (DFSR) which improves on FRS by only copying those parts of files which have changed (remote differential compression), by using data compression to reduce network traffic, and by allowing administrators flexible configuration options for limiting network traffic with a customizable schedule.

Distributed File System (DFS) allows administrators to group shared folders located on different servers by transparently connecting them to one or more DFS namespaces. A DFS namespace is a virtual view of shared folders in an organization. Using the DFS tools, an administrator selects which shared folders to present in the namespace, designs the hierarchy in which those folders appear, and determines the names that the shared folders show in the namespace. When a user views the namespace, the folders appear to reside on a single, high-capacity hard disk. Users can navigate the namespace without needing to know the server names or shared folders hosting the data. DFS also provides many other benefits, including fault tolerance and load-sharing capabilities, making it ideal for all types of organizations.

**DFS**  
One of the goals of most information technology (IT) groups is to manage file server resources efficiently while keeping them available and secure for users. As networks expand to include more users and servers—whether they are located in one site or in geographically distributed sites—administrators find it increasingly difficult to keep users connected to the files they need. On one hand, distributing resources across a network makes them more available to more people and promotes cross-organizational efforts. On the other hand, storing files on different file servers located throughout an organization makes it difficult for users to know where to look for information. Administrators also find it difficult to keep track of all the servers and all of the people who use those servers. The task of swapping out an old server becomes a major communication chore when users across an organization must be notified to update links and file paths.

To help administrators address these problems, Windows Server 2003 includes Distributed File System (DFS). DFS allows administrators to group shared folders located on different servers by transparently connecting them to one or more DFS namespaces. A DFS namespace is a virtual view of shared folders in an organization. Using the DFS tools, an administrator selects which shared folders to present in the namespace, designs the hierarchy in which those folders appear, and determines the names that the shared folders show in the namespace. When a user views the namespace, the folders appear to reside on a single, high-capacity hard disk. Users can navigate the namespace without needing to know the server names or shared folders hosting the data. DFS also provides other benefits, including the following:

Simplified data migration

DFS simplifies the process of moving data from one file server to another. Because users do not need to know the name of each physical server or shared folder that contains the data, administrators can physically move data to another server without needing to reconfigure applications and shortcuts and without needing to reeducate users about where they can find their data. This minimizes the impact of server consolidation on users. It also allows administrators to deploy additional file servers and present the folders on those new servers as new folders within an existing namespace.

Increased availability of file server data

In the event of a server failure, DFS refers client computers to the next available server, so users can always access shared folders without interruption.

Load sharing

DFS provides a degree of load sharing by mapping a given logical name to shared folders on multiple file servers. For example, suppose that \\Company\StockInfo is a heavily used shared folder. Administrators can use DFS to associate this location with multiple shared folders on different servers, even if the servers are located in different sites.

Security integration

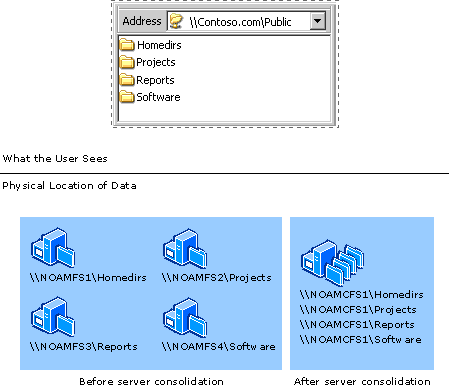
Administrators do not need to configure additional security for DFS namespaces because file and folder security is enforced by existing the NTFS file system and shared folder permissions on each target. For example, a user navigating a DFS namespace is permitted to access only the files or folders for which he or she has appropriate NTFS or shared folder permissions.

Common DFS Scenarios

DFS is commonly used in the following scenarios:

Server Consolidation

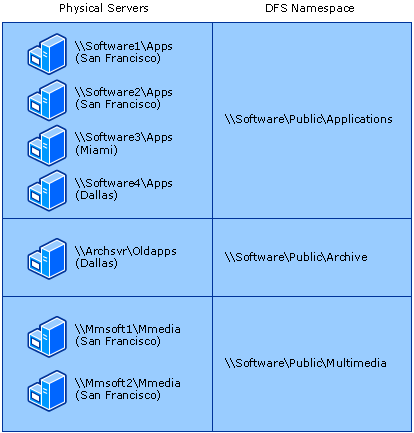
Many organizations today are consolidating older file servers throughout the organization into fewer, larger, more powerful file servers. Consolidation reduces the cost of managing multiple file servers and increases the efficiency of storage allocation and backup tasks. Organizations that have implemented DFS can perform server consolidations without impacting the way users’ access data. The following figure illustrates this benefit.   
**How DFS Eliminates the Impact of Server Consolidation on Users**



Publishing Applications

DFS is commonly used to publish applications to users throughout the organization. Using DFS in this scenario provides a number of benefits, such as the ability to use multiple servers to host application data and distribute the load across servers. A feature in DFS known as “least expensive target selection” ensures that users are connected to the closest server. The following figure illustrates a DFS namespace used to publish applications in an organization based in San Francisco with offices in Miami and Dallas.

Using DFS to Publish Applications



This organization has three types of software:

* Business-critical software and operating systems that must be available at all times.
* Previous versions of software that are still in use in the Dallas branch office.
* Multimedia software used primarily in San Francisco.

The organization uses four servers to host the business-critical software and operating systems, including two servers in the San Francisco site. Using two servers to host the applications ensures that a failure on one server does not cause the data to become unavailable. All users can access this software at \\Software\Public\Applications, and users are automatically directed to the server in their site (San Francisco, Dallas, or Miami).

Because the archived software is used only in the Dallas office and the data is not business-critical, only a single server hosts that data. The multimedia software is not business-critical, but the organization uses two servers for this software to improve server response times because the client portion of the multimedia software accesses files from the server.

Increasing Data Availability

As described in the scenario for publishing applications, administrators can use DFS to increase the availability of data by storing the data on multiple servers. DFS makes this process transparent by presenting to users what appears to be a single folder in the namespace. Administrators can use File Replication service (FRS) or some other replication method, such as the Windows Resource Kit Tool Robocopy, to keep the data synchronized on the servers. If one of the servers hosting data is unavailable, clients are referred to another server that hosts the data.

## Vraag 22: Wat zijn de twee soorten backups en waneer gebruik je deze?

- Full backup: is een volledige backup. (voor nieuwe systemen, volledige back-up is het eerste dat je doet!)

- Incremental backup: is een volledige backup waarvan enkel aangepaste files en folders worden ge backt-upt. Dus er wordt geen volledig backup gemaakt, enkel van de aangepaste bestanden. (als je al een volledige back-up hebt, en enkel de bijkomende bestanden, mappen wilt back-uppen die zijn bijgekomen)

## Vraag 23: waarom zou je meerdere DC aanmaken in 1 domein?

Om een backup systeem te creeren

Het is beter om meerdere domeincontrollers op eenzelfde domein te maken voor fouttolerantie of om de werkdruk te spreiden.

(adc = additional domain controller)

Extra domain controllers kunnen ervoor zorgen dat er fouten tolerantie is. Ze kunnen ook helpen met het laden van bestaande domain controllers en ze brengen een extra infrastructuur voor sites.

You would have redundant DCs in a corporate environment so that if one DC goes down the secondary can take over the primary DC's responsibilities. Both DCs would contain replicated copies of AD and would have the same services running. The DCs may be deployed as a failover cluster, with total downtime in the event of a failure being less than 2 minutes.

## Vraag 24: Leg uit: DNS-replication

- Hier worden de DNS instellingen van server 1 volledig over gekopiërd naar server 2 als voorbeeld.

## Vraag 26: Wat is een Single Point Of Failure?

Een SPOF is een deel van het systeem dat, als het faalt, het hele systeem doet stoppen met werken.

## Vraag 27: Wat is IIS?

Internet Information Services 7.0 biedt:

• Een krachtig webplatform voor toepassingen en diensten

• Vereenvoudigd webbeheer

• Een verbeterde en taakgebaseerde beheerinterface

• Cross-site control

• Veiligheidsverbetering

• Delegeren van site- en toepassingsbeheer

ISS is een verzameling van serverdiensten voor het internet bedoeld voor Windows-machines.

IIS (Internet Information Server) is a group of Internet servers (including a Web or Hypertext Transfer Protocol server and a File Transfer Protocol server) with additional capabilities for Microsoft's Windows NT and Windows 2000 Server operating systems. IIS is Microsoft's entry to compete in the Internet server market that is also addressed by Apache, Sun Microsystems, O'Reilly, and others. With IIS, Microsoft includes a set of programs for building and administering Web sites, a search engine, and support for writing Web-based applications that access databases. Microsoft points out that IIS is tightly integrated with the Windows NT and 2000 Servers in a number of ways, resulting in faster Web page serving.

A typical company that buys IIS can create pages for Web sites using Microsoft's Front Page product (with its WYSIWYG user interface). Web developers can use Microsoft's Active Server Page (ASP)technology, which means that applications - including ActiveX controls - can be imbedded in Web pages that modify the content sent back to users. Developers can also write programs that filter requests and get the correct Web pages for different users by using Microsoft's Internet Server Application Program Interface (ISAPI) interface. ASPs and ISAPI programs run more efficiently than common gateway interface (CGI) and server-side include (SSI) programs, two current technologies. (However, there are comparable interfaces on other platforms.)

Microsoft includes special capabilities for server administrators designed to appeal to Internet service providers (ISPs). It includes a single window (or "console") from which all services and users can be administered. It's designed to be easy to add components as snap-ins that you didn't initially install. The administrative windows can be customized for access by individual customers.

## Vraag 28: Wat is WSUS

WSUS = Windows Server Update Services  
De WSUS server zorgt voor het downloaden van updates en het verspreiden ervan binnen het netwerk.