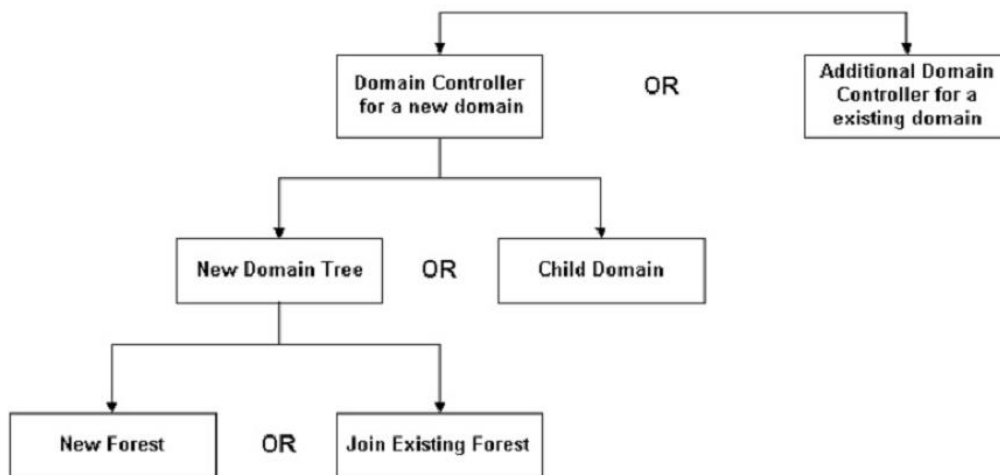


Oefening 3: ACTIVE DIRECTORY installatie

1. Installatie van Active Directory

- De bedoeling is om van dc1 een Domain Controller te maken in een nieuw domein. Selecteer hiervoor [jevoornaam].local. Al de computers zijn ingesteld op deze domeinnaam, zoals o.a. in hun dns suffix.



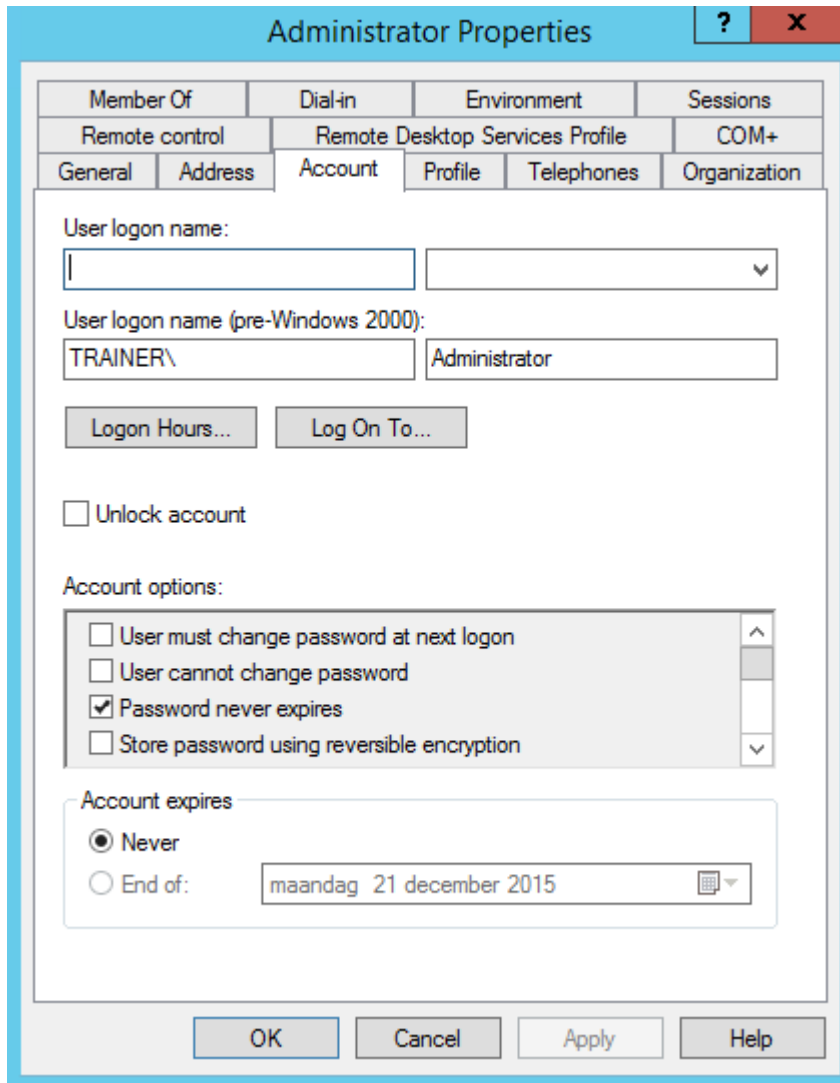
1. Log aan als administrator
2. Open de Server Manager
3. Voeg de Active Directory Domain Services role toe.
4. We installeren een Domain Controller voor een nieuw domein voornaam.local in een nieuwe forest.
5. **BELANGRIJK!** Omdat dc1 van een recentere windows server generatie is dan dc2, en omdat we later dc2 ook een domain controller willen maken van dit domein, kiezen voor een domain- en forest functional level van de editie van dc2. Indien je hier toch kiest voor het domain- en forest functional level van dc1, zal je naar alle waarschijnlijk moeten opnieuw beginnen, dus zorg dat je deze stap correct uitvoert!
6. Onze eerste dc is verplicht DNS server en Global Catalog.
7. Voor deze testopstelling mag je de locatie van de database, logfiles en SYSVOL folder ongewijzigd laten. In een productieopstelling moeten deze zaken op snelle schijven staan, bij voorkeur in RAID.
8. Gebruik hetzelfde paswoord als hetgene voor je domain admin account als paswoord voor de Directory Services Restore Mode.
9. Na de installatie van Active Directory moet je de server herstarten. Je kan nu inloggen met dezelfde credentials als voordien. Je administrator is nu echter Domain Administrator geworden en je lokale users, zelfs de hele SAM-database, zijn verdwenen.
10. Probeer de Active Directory Users en Computers console te openen, alsook de DNS console.

Zoek je meer info of is iets niet duidelijk? Zoek eens op “*Windows Server install Active Directory*”

2. Aanpassen paswoorden admin accounts

Om toekomstige toegang tot het domein te garanderen gaan we een 2^{de} domain admin account aanmaken.

1. Ga onder 'tools' naar 'Active Directory Users and Computers' (ADUC)
2. Ga naar de container 'Users'
3. Open de properties van de 'Administrator' account, kies het tabblad 'account' en vink 'Password never expires' aan.



Administrator Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
Telephones		Organization	

User logon name:
[] [v]

User logon name (pre-Windows 2000):
[TRAINER\] [Administrator]

[Logon Hours...] [Log On To...]

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Store password using reversible encryption

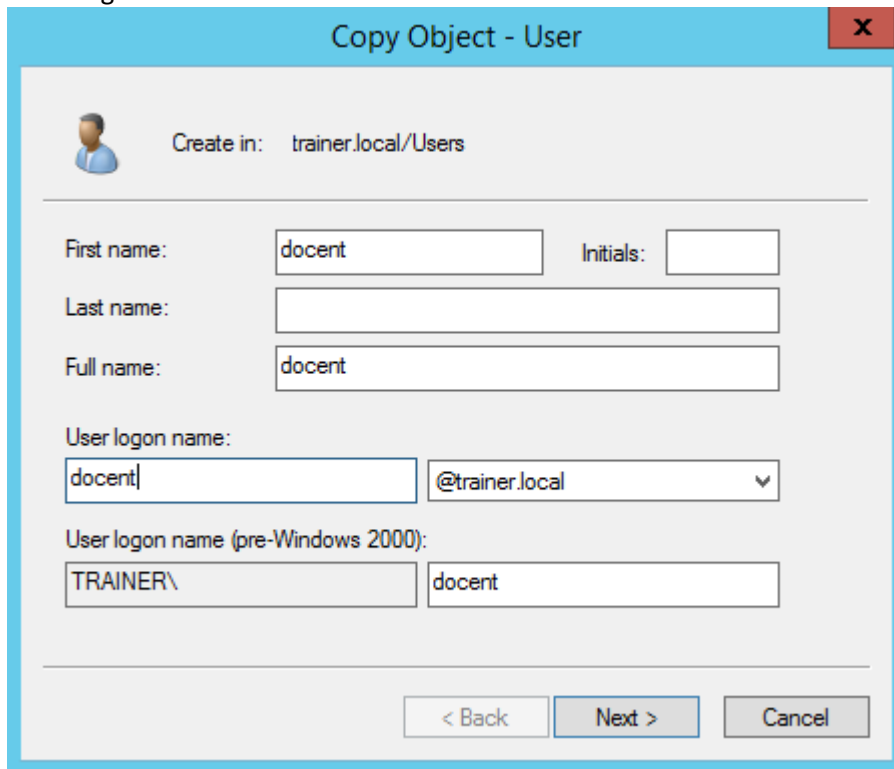
Account expires:

☒ Never

☐ End of: maandag 21 december 2015 [calendar icon]

[OK] [Cancel] [Apply] [Help]

4. Kopieer de Administrator account naar een nieuwe 'docent'-account met onderstaande instellingen



The 'Copy Object - User' dialog box shows the configuration for creating a new user. The 'Create in' field is set to 'trainer.local/Users'. The 'First name' is 'docent', 'Initials' is empty, and 'Last name' is empty. The 'Full name' is 'docent'. The 'User logon name' is 'docent' and the domain is '@trainer.local'. The 'User logon name (pre-Windows 2000)' is 'TRAINER\' and the name is 'docent'. The 'Next >' button is highlighted.

Create in: trainer.local/Users

First name: docent Initials:

Last name:

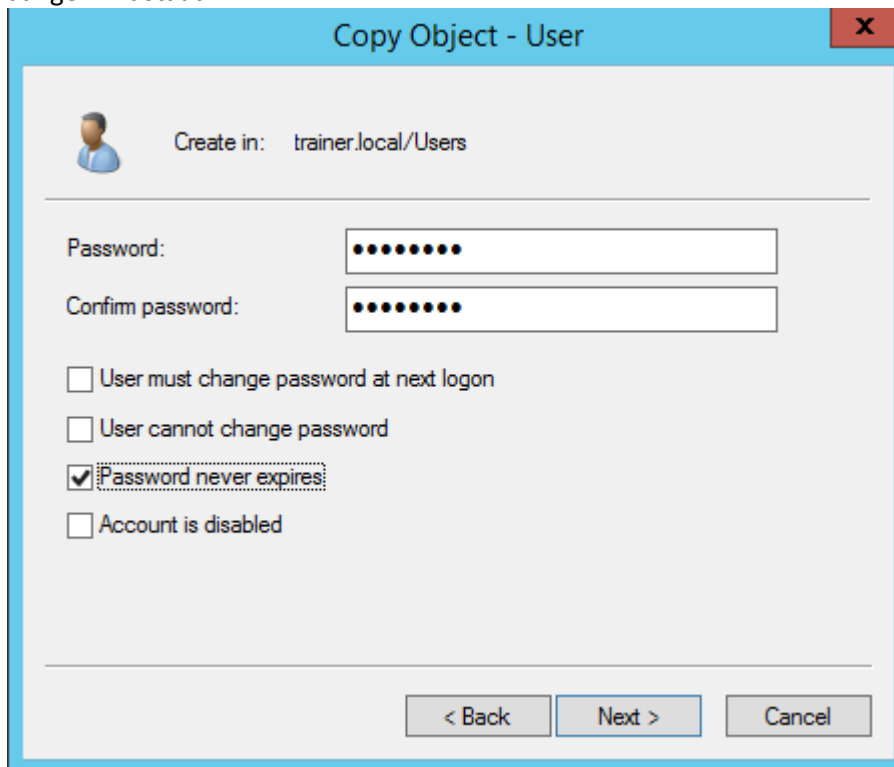
Full name: docent

User logon name: docent @trainer.local

User logon name (pre-Windows 2000): TRAINER\ docent

< Back Next > Cancel

5. Gebruik als paswoord ook hier 'Student1'. Zorg ervoor dat je 'Password never expires' aangevinkt staat.



The 'Copy Object - User' dialog box shows the password configuration. The 'Password' and 'Confirm password' fields are filled with dots. The 'User must change password at next logon' checkbox is unchecked. The 'User cannot change password' checkbox is unchecked. The 'Password never expires' checkbox is checked. The 'Account is disabled' checkbox is unchecked. The 'Next >' button is highlighted.

Create in: trainer.local/Users

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

3. Windows client en dc2 lid maken van domein

We gaan onze Windows client toevoegen aan of lid maken van het domein. Vergelijk het met de PC's in de klaslokalen waarop je met je persoonlijke account kan inloggen en bepaalde settings toegekend krijgt.

1. Log in op je Windows client machine met je lokale account.
2. Ga naar System in het Control Panel of klik rechts op Computer in het startmenu en kies voor
 1. properties.
 2. Klik op Change Settings naast Computer Name.
3. Vul onder Domain je gekozen domeinnaam in. Na enige tijd krijg je de vraag om je credentials op te geven. Dit zijn de credentials van een account in je domein met rechten om computers toe te voegen aan dit domein, zoals bijvoorbeeld de Domain Administrator. De gebruikersnaam wordt voorafgegaan door je domein. Bijvoorbeeld EHB\administrator.

Werkt dit niet? Hoe probeert je client te connecteren met de Domain Controller? Kan je client de dc van je domein wel vinden? Houd er rekening mee dat hiervoor DNS gebruikt wordt!

Doe dit ook voor dc2. Hierdoor gaat deze van stand-alone server naar member server. Straks zal deze de tweede Domain Controller worden.

Zowel de Windows client als dc2 zijn nu lid van AD domein.

4. Remote Server Management via Windows client

Ook een client operating system kan aan serverbeheer doen via de optionele Remote Server Administration Tools voor Windows (versie van windows client). Deze tools zijn gratis te downloaden van op de website van Microsoft, maar sinds de 2018 versie van Windows 10 ook beschikbaar optionele feature in het Windows client OS zelf. Zoek de "Manage Optional Features" via het start menu en voeg de belangrijkste rsat-tools toe (RSAT: Active Directory Domain Services and Lightweight Directory Services Tools, RSAT: DNS Server Tools, RSAT: DHCP Server Tools, RSAT: File Services Tools, RSAT: Group Policy Management Tools, RSAT: Server Manager)

Let wel, zoals steeds om bepaalde taken uit te voeren op een server, zal je hiervoor de juiste rechten nodig hebben. Dit wil zeggen dat als je in je Windows client bent aangemeld met een gewone useraccount, je ook enkel de taken zal kunnen uitvoeren die deze account mag uitvoeren. Vandaar dat het aan te raden is een shortcut te maken voor de mmc.exe met al je snapins in, en dan deze op te starten met een andere useraccount, zoals de domain admin door rechts te klikken op de shortcut met de shifttoets ingedrukt en "login as a different user" te kiezen.

5. Installatie van Active Directory op dc2

Probeer analoog aan de installatie van Active Directory op dc1, ook dc2 Domain Controller te maken voor je bestaande domain. Het wordt dus een nieuwe Domain Controller voor een bestaand domain. Let op dat je bij de installatieprocedure 'global catalog' uitvinkt. We gaan dit later manueel instellen.

Na installatie zal je moeten herstarten. Zoek uit hoe je vanaf eender welke server met de nodige geïnstalleerde tools verschillende servers kan beheren (bijvoorbeeld voor Active Directory). Dit kan ook vanaf een client (zie 3).

6. Multi-master replicatie

Active Directory maakt gebruik van multi-master replicatie. Dit wil zeggen dat elke domain controller een RW-kopie heeft van de database. We zullen dan ook als eerste test na de installatie 2 gebruikers aanmaken om te zien of de replicatie al werkt:

1. Maak in Administrative Tools – ADUC (Active Directory Users and Computers) op je eerste domain controller een nieuwe gebruiker aan met als naam en logon-name naar keuze. Plaats deze in de *users* container.
2. Ga nu naar Administrative Tools – ADUC op je tweede dc en bekijk of de gebruiker ook naar deze domain controller werd gerepliceerd. Eventueel eens refreshen doet soms wonderen als je niet meteen resultaat ziet.
3. Maak nu op je tweede domain controller een nieuwe gebruiker met als naam en logon-name een naam naar keuze.
4. Bekijk vervolgens of deze gebruiker wordt gerepliceerd naar de eerste dc.

Wanneer bepaalde zaken niet meteen gerepliceerd worden, kan je altijd manuele replicatie forceren via Active Directory Sites and Services. Klik hier door naar het NTDS object van een server binnen een bepaalde site. Aan de rechterkant van je MMC zie je nu een automatisch gegenereerde connectie staan waarop je de optie “Replicate Now” kan uitvoeren. Wanneer deze geforceerde replicatie foutmeldingen geeft en je hebt nog maar net een Domain Controller toegevoegd (zoals wij in deze cursus), is het geen slecht idee om eerst eventjes te wachten tot de replicatietopologie volledig is opgezet en er geen foutmeldingen meer zouden mogen zijn.

7. Logische structuur van Active Directory

1. Open Active Directory Users and Computers.
2. Merk op dat er een verschil is tussen de icoontjes van de virtuele folders in ons domein, bv. voor *Users* en voor *Domain Controllers*. Beiden zijn Active Directory containers, alleen containers zoals *users* zijn speciaal want ze zijn geen echte OU's, met als gevolg dat we er geen GPO's aan kunnen koppelen, dus qua functionaliteit blijft zo een container heel beperkt. Van zodra je een domein hebt geïnstalleerd wordt aangeraden om geen users in deze container te zetten (zoals we in de oefening hierboven nog wel hebben gedaan).
3. Maak onder de domeinnaam een Organizational Unit '*sales*' aan. Dit kan door rechts te klikken op je domeinnaam en daar te kiezen voor New -> Organizational Unit. In een latere oefening zullen we een grotere OU-structuur opzetten, gebaseerd op enkele best practices.
4. Verplaats de twee aangemaakte gebruikers van daarnet naar deze *sales* OU.

8. Global Catalog

Een Global Catalog is een Domain Controller die van de hele forest een samenvatting bevat. Om bv. forest-wide queries te versnellen wordt deze GC gebruikt, alsook voor enkele andere belangrijke functionaliteiten. Zo zal de Global Catalog onder andere alle Universal groepen van het gehele forest bevatten. Bij de logon van een gebruiker moet bepaald worden van welke groepen deze gebruiker lid is (om zijn rechten te bepalen), daarom is bij elke logon van een gebruiker sowieso een Global Catalog nodig.

In een single domain omgeving mag eigenlijk elke dc een GC zijn. Aangezien er maar 1 domein is, zal dit geen extra belasting betekenen. Er moeten immers geen andere objecten uit andere domeinen worden opgeslagen.

Sowieso is het in een single-domain of multi-domain omgeving het beste om minstens een aantal GC's te hebben, en zeker 1 op elke site (zie later), zo kan de load verdeeld worden over deze verschillende GC's.

Maak van dc2 ook een GC:

1. Open Active Directory Sites and Services.
2. Kies de site waarin je een dc tot GC wil maken (bij ons is dit *Default-First-Site-Name*).
3. Ga naar *Servers* folder.
4. Rechtsklik op de NTDS settings van een server en kies properties.
5. Op het General tabblad kan je nu "Global Catalog" aanvinken.

Kijk na of beide domain controllers in je domain ook Global Catalog zijn en zo niet, en pas aan.

9. Operations masters

Enkele taken in Active Directory kunnen niet door elke Domain Controller worden uitgevoerd. Het multi-master replicatie-model geldt dus maar tot op bepaalde hoogte. Er zijn 5 taken die niet door elke Domain Controller mogen worden uitgevoerd. 3 van deze rollen worden telkens (en individueel) toegekend aan een bepaalde Domain Controller in een domein, 2 van deze rollen zijn zelfs uniek op forest-niveau en worden (individueel per rol) toegekend aan een domain controller ergens in het forest (meestal in het bovenste domain, het root domain).

Let op: het is enkel de bedoeling te gaan kijken naar de plaats waar dit kan aangepast worden, niet om deze effectief aan te passen.

Je kan via de grafische interface op zoek gaan naar de instellingen (zie verder).

Je kan deze FSMO-rollen verplaatsen, vandaar de F van Flexible. SMO staat voor Single Master Operation en geeft aan dat er maar 1 domain controller deze functionaliteit kan bevatten. Verplaatsen van SMO-rollen gebeurt op verschillende plaatsen, naargelang de FSMO-rol.

Probeer het verplaatsen van een FSMO-rol zelf te vinden in de verschillende MMC's:

- Domain Naming Master: Active Directory Domains and Trusts
- Relative Identifier Master: Active Directory Users and Computers
- Pdc emulator: Active Directory Users and Computers
- Infrastructure Master: Active Directory Users and Computers
- Schema Master
 - Start -> Run

- Mmc.exe
- Add/remove snap-in
- Active Directory Schema
 - Als je deze snap-in nog niet zien staan, moet je eerst het volgende commando uitvoeren in Start->Run: regsvr32 schmmgmt.dll