VDAB
TRAINING & OPLEIDING

Samen sterk voor werk

Windows Server Administration

Objecten in Active Directory

Inhoud

1 OBJECTEN IN AD

Wat komt er aan bod in deze module?

- Gebruikers en computers creëren en beheren in AD
- Groepen en Organizational units (OU's) creëren en beheren in AD
- Service authentication en account policies configureren

AD is één centrale opslagplaats van objecten, zoals gebruikers, computers, resources enz., op het netwerk. Meer dan 2 miljard objecten kunnen opgeslagen worden in een AD.

1.1 Security principals

Het systeem wijst bij creatie aan sommige types objecten een Security Identifier (SID) toe, d.i. een unieke waarde om het object te identificeren binnen het domein.

SID en object zijn onlosmakelijk met elkaar verbonden.

- bij verwijdering van het object wordt de bijbehorende SID niet opnieuw in gebruik genomen voor een ander object
- bij wijziging van het object, zelfs bij verandering van de naam blijft de SID behouden.

AD objecten waaraan een SID (Security Identifier) toegewezen is, worden security principals genoemd: gebruikeraccounts, groepen, computeraccounts.

Aan Security principals kunnen rechten toegekend worden.

Die rechten kunnen te maken hebben met het

- al dan niet toegang krijgen tot bepaalde resources op het netwerk
- al dan niet bepaalde handelingen mogen uitvoeren (userrights).

Andere AD objecten zoals contacten, distributiegroepen, printers, OU's ... behoren tot de non-security principals.

Objecten die geen SID hebben kunnen ook geen rechten krijgen.

Bij het opzetten van een domein worden al een aantal standaard security principals aangemaakt. Op elk domein wordt een SID volgens dezelfde regels samengesteld.

Enkele voorbeelden

- Administrator S-1-5-{domeinid}-500
- Domain admins S-1-5-{domeinid}-512
- Domain users S-1-5-{domeinid}-513
- Domain computers S-1-5-{domeinid}-515

1.2 Organizational units

Een organizational unit is een container waarin AD objecten kunnen aangemaakt worden, m.a.w. een OU is een logische groep objecten in AD. Een OU krijgt **geen** SID en bijgevolg kunnen er ook geen rechten aan een OU toegekend worden.

Objecten die je in een OU kunt maken:

- Gebruikers
- Groepen
- Computers
- Shared folder objecten
- Contacten
- Printers
- InetOrgPerson objecten
- Microsoft Message Queuing Queue aliases
- Andere OU's

Factoren die het plannen van een OU structuur zullen beïnvloeden:

- Het delegeren van beheertaken
- Het koppelen van grouppolicies
- Structuur brengen in de AD objecten

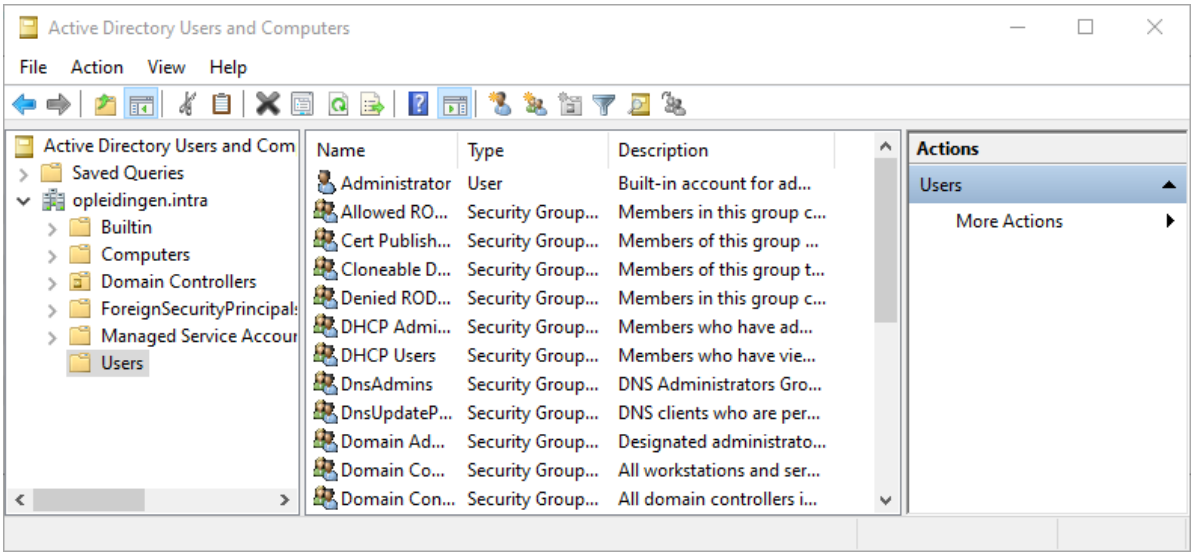
De volgende hoofdstukken bespreken enkele tools om objecten in AD aan te maken.

2 ACTIVE DIRECTORY USERS AND COMPUTERS (ADUC)

Er zijn meerdere tools ter beschikking om objecten in de AD DS te beheren.

In de Server Manager vind je ADUC onder Tools > Active Directory Users and Computers.

2.1 De interface van ADUC



Het venster van ADUC bestaat uit drie panelen. Welke al dan niet getoond worden kan je aanpassen via **View > Customize** of met de knoppen **Show / Hide Console tree** en **Show / Hide Action Pane** in de werkbalk.

Het linkse paneel (Console tree), toont de structuur met de verschillende containers die het besturingssysteem al zelf heeft aangemaakt tijdens de installatie.

Builtin	Bevat een aantal domein lokale groepen.
Computers	Hier komen standaard de accounts van alle client computers en memberservers die lid zijn van het domein. Hier zou je dus de account van je client computer moeten terugvinden.
Domain Controllers	Alle domein controllers van het domein. Hier zou je de account van je domain controller moeten terugvinden.
Foreign Security Principals	Security principals van vertrouwde domeinen.
Managed Service Accounts	Accounts die gebruikt worden door toepassingen zoals IIS, SQL Server…

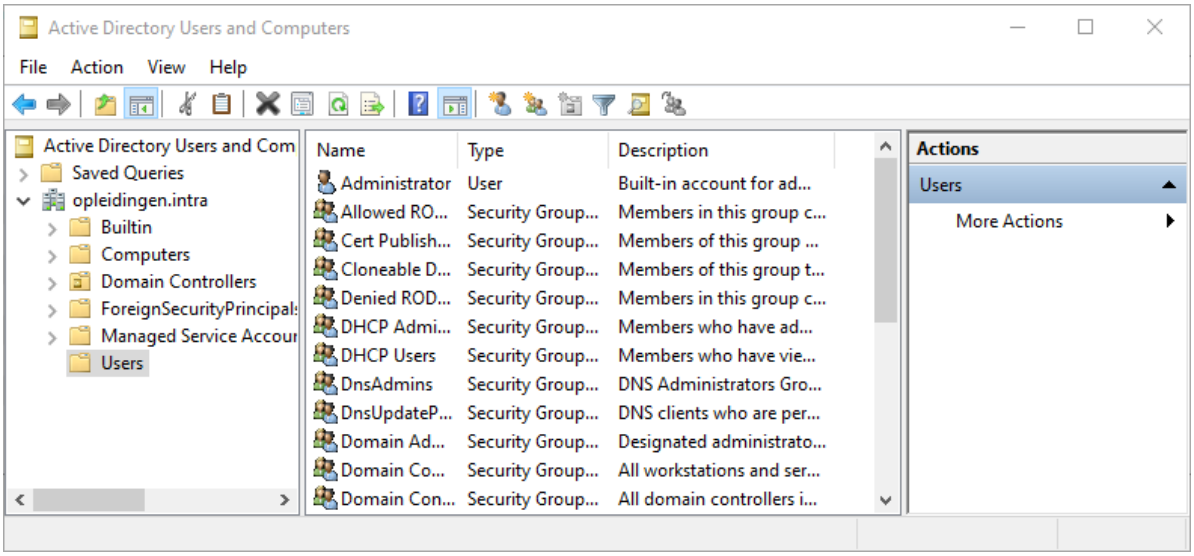
Users	De administrator en de guest account en een aantal door het besturingssysteem aangemaakte groepen.

Selecteer je in het linkse paneel een container, dan verschijnt, zoals gebruikelijk in een Windows omgeving, in het middelste de inhoud van de container. Het rechtse paneel (Action Pane) biedt een lijst opdrachten aan die relevant zijn voor de huidige selectie.

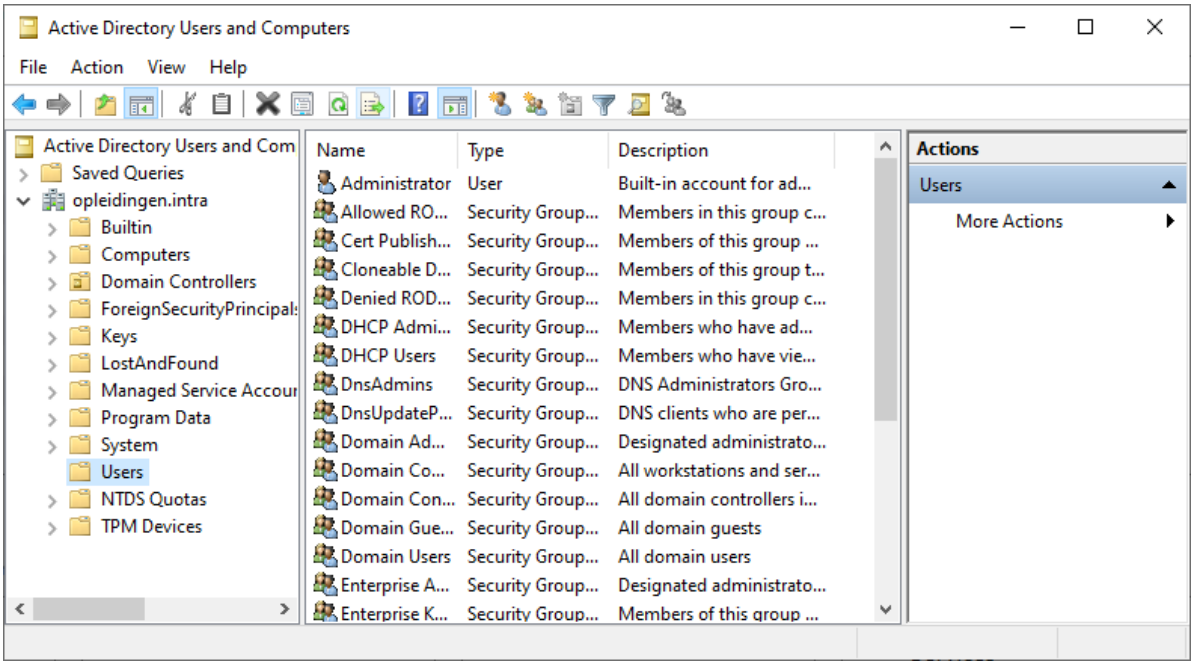
2.1.1 Advanced mode

Deze mode activeer je via **View > Advanced features**. Ze toont meer informatie over de objecten in de ADUC.

ADUC in normale weergave



en ADUC als **Advanced features** geactiveerd is

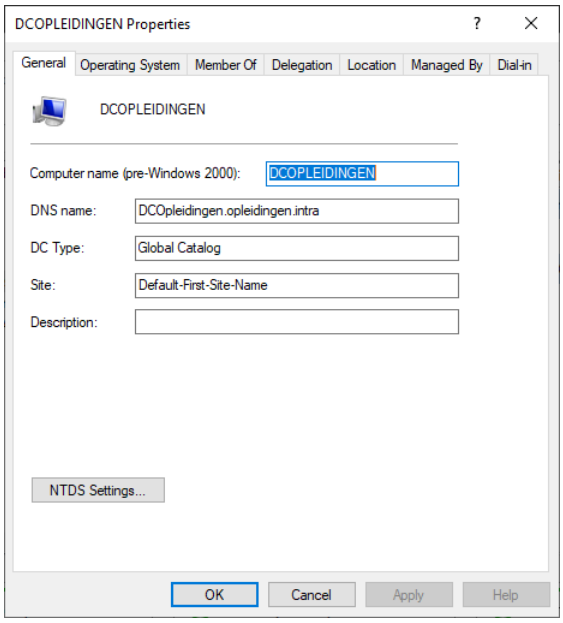
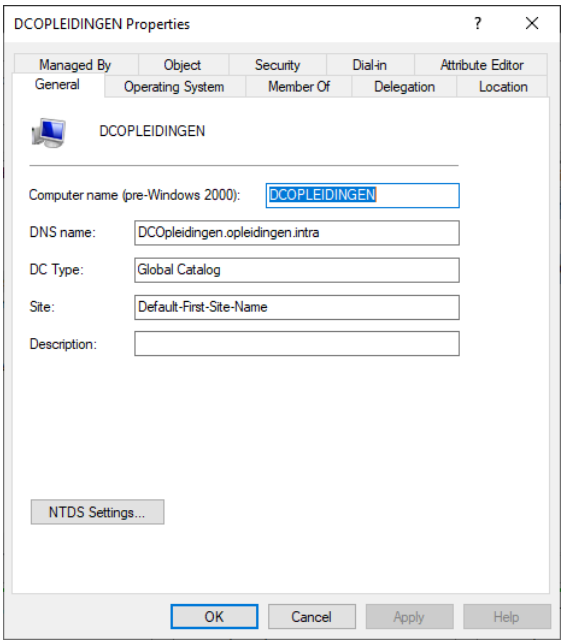


Er zijn duidelijk een aantal containers bijgekomen.

In Advanced weergave worden ook meer eigenschappen van de objecten getoond.

- Klik met de rechtermuisknop op de server DCOpleidingen in de OU Domain controllers en kies Properties.

Opmerking:
Meervoudige selecties in het middelste paneel zijn mogelijk volgens de geijkte Windows technieken: de Shift toets gebruiken om een lijst aaneensluitende objecten te selecteren en de Ctrl toets om willekeurige objecten uit een lijst te selecteren.

Normale weergave	Advanced weergave
	

2.1.2 Kolommen toevoegen

Het middelste paneel toont standaard de inhoud van de velden Naam, Type en Description. De waarde van andere velden kan je hier ook te zien krijgen door kolommen toe te voegen.

Dit kan via **View > Add/remove Columns**

2.1.3 Users, Contacts, Groups and Computers as containers

Deze weergave toont bij een account alle objecten die ermee geassocieerd zijn. Dit kan b.v. nuttig zijn om de printerobjecten te tonen die geassocieerd zijn met een computeraccount.

Inschakelen gebeurt via **View > Users, Contacts, Groups and computers as containers**.

2.2 Remote beheren met RSAT

Servers staan in de praktijk in een beveiligde, gekoelde ruimte. Een administrator zal beheeropdrachten dan ook meestal niet lokaal op een server ingeven, maar vanop een client.

Tijdens de installatie van een server met GUI worden meteen ook beheertools voor een server geïnstalleerd. De installatie van een domeincontroller voegt daar nog de beheertools voor een domein aan toe. Op een client zijn deze tools echter niet automatisch ter beschikking. Het pakket RSAT (Remote Server Administration Tools) bevat de nodige software om ook vanop een client een domein te beheren.

We zullen in deze module het domein beheren vanop een client CL01 die lid is van het domein en waarop de RSAT tools geïnstalleerd werden. Je zorgt ervoor dat je aangemeld bent met je adminstrator account uit het domein, niet met je gebruiker van het werkstation.

2.2.1 RSAT vanaf Windows 10 release 1809

Vanaf de Windows 10 Oktober 2018 Update (release 1809) moet je de software niet meer downloaden, maar is deze beschikbaar via de Settings.

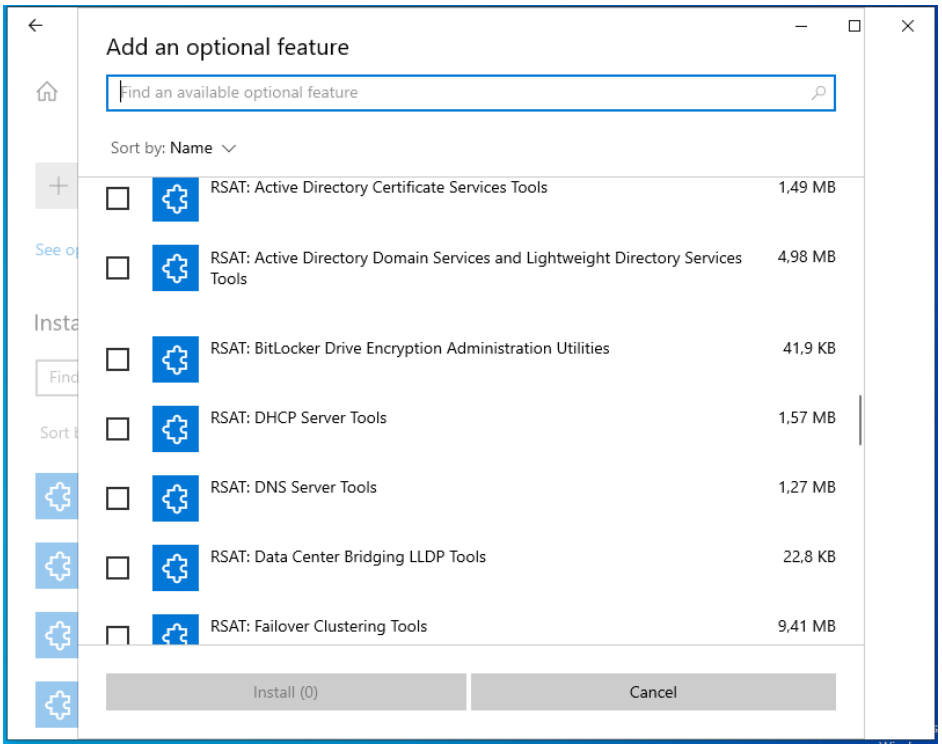
Windows 10:

- 🛠 Settings -> Apps -> optional features -> Add a feature.

Windows 11:

- 🛠 Settings -> System -> optional features -> Add a feature.

Kies daar de juiste tools die je nodig hebt.



~~2.2.2 RSAT ophalen (voor release 1809)~~

~~Tip indien je nog werkt met een release ouder dan 1809:~~

~~Je vindt de download van RSAT via https://www.microsoft.com/en-us/download/details.aspx?id=45520~~

~~De versie van RSAT die je installeert op een toestel, moet exact overeen komen met de versie van het Windows besturingssysteem dat erop geïnstalleerd is.~~

~~Let op dat je zowel de juiste taal als de juiste versie als de juist bit versie kiest. Er wordt een 32-bit en een 64 bit versie aangeboden.~~

~~In de naam van het installatiebestand vind je zowel de build als de bitversie van het besturingssysteem waarvoor dat installatiebestand bedoeld is.~~

~~Zo vind je oa. *WindowsTH-RSAT_WS_**1803**-x**64**.msu* om te installeren op een client. De 1803 verwijst hier naar de build van het Windows 10 besturingssysteem op de client.~~

~~2.2.3 RSAT installeren (voor release 1809)~~

- ~~Klik dubbel op het binnengehaalde bestand.~~
- ~~Aanvaard de licentieovereenkomst.~~

~~De installatie begint.~~

~~Opmerking~~

~~Er kan slechts één versie van RSAT tegelijkertijd op een toestel geïnstalleerd worden. Eerder geïnstalleerde versies moeten eerst verwijderd worden.~~

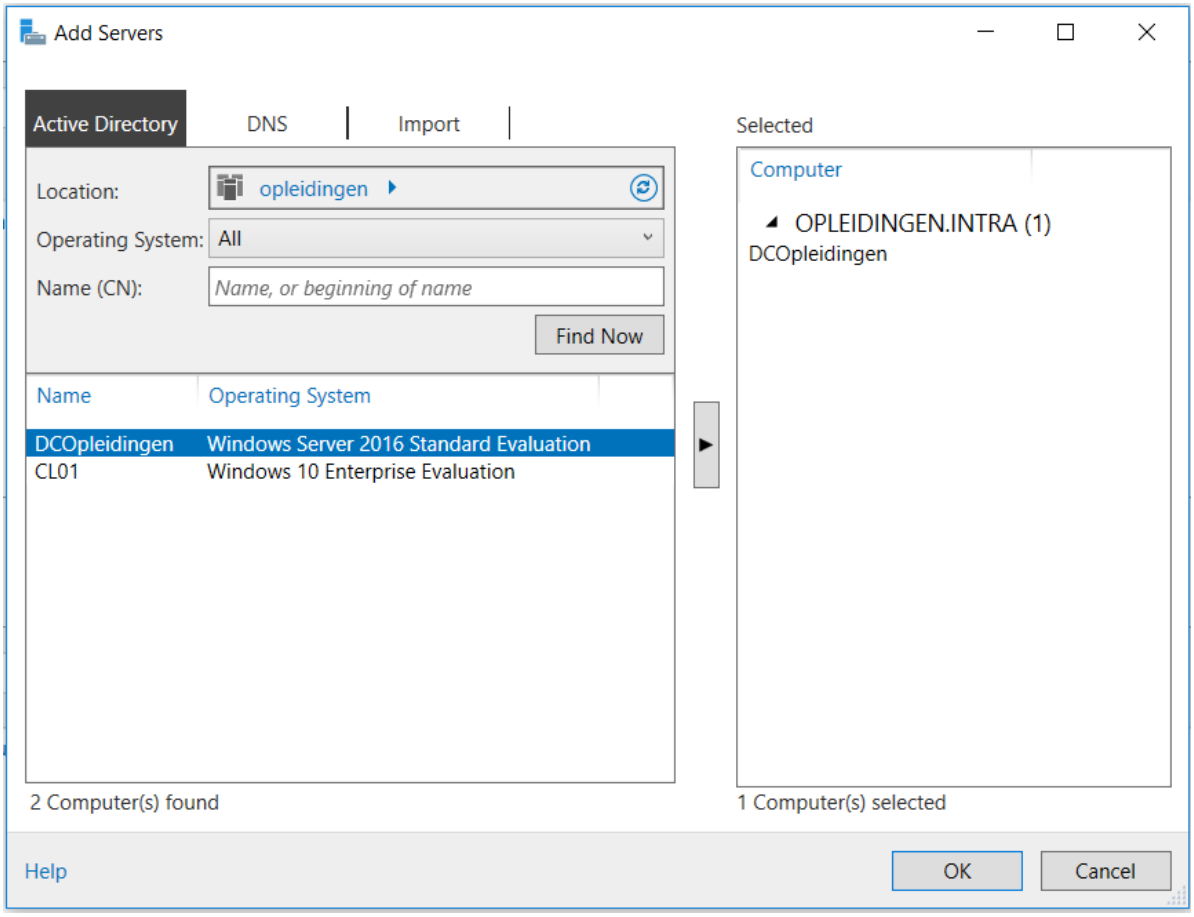
2.2.4 RSAT Gebruiken

Na installatie vind je de tools op meerdere plaatsen:

- In de server manager in het menu Tools
- In het startmenu onder Windows Administrative Tools
- In het Control Panel onder System and Security > Administrative Tools

2.2.5 De praktijk

- Zorg ervoor dat je beschikt over een client CL01 die lid is van het domein Opleidingen.intra en waarop RSAT geïnstalleerd werd.
- Meld aan op de client met een account die lid is van de domein administrators.
- Start Servermanager (via de geïnstalleerde RSAT)
- Manage > Add Servers
- Klik op “Find Now”



- Voeg de domeincontroller, DCOpleidingen toe aan de geselecteerde servers en klik op OK.
- Klik met de rechtermuisknop op de server. Een lijst met beheertools voor het domein komt ter beschikking.
- Kies het programma dat je wenst te gebruiken.

In de rest van de module wordt ervan uitgegaan dat ADUC geopend wordt vanop een client.

3 ORGANIZATIONAL UNIT (OU)

3.1 OU's plannen

Zoals eerder vermeld spelen drie factoren een rol bij het plannen van OU's

3.1.1 Het beheer van een aantal objecten delegeren

Een domeinbeheerder kan beheertaken voor een OU delegeren. Zo kan aan een overigens gewone gebruiker het recht gegeven worden om nieuwe gebruikers aan te maken en wachtwoorden te veranderen, maar enkel binnen een bepaalde OU en niet elders op het domein.

3.1.2 Structuur brengen in de verzameling objecten van het domein

In dat opzicht kunnen OU's vergeleken worden met mappen die structuur brengen in een verzameling van bestanden in de verkenner.

En net zoals elke gebruiker zijn mappen naar eigen voorkeur kan organiseren, zijn er ook geen vaste regels om OU's aan te maken. Je kunt OU's zo aanmaken dat ze de structuur van het bedrijf weerspiegelen, maar je kunt je ook baseren op de geografische ligging of op de verschillende projecten die lopen.

OU's kunnen computers, gebruikers, groepen, security policies, gedeelde printers, gedeelde mappen enz. bevatten, maar alleen van het eigen domein.

OU's kunnen ook genest worden. Zo zou je de OU die correspondeert met de afdeling Inkoop verder kunnen onderverdelen in een OU met de gebruikers en een OU met de computers van de afdeling Inkoop.

3.1.3 Policies die moeten gelden voor bepaalde gebruikers en computers

Ten slotte kunnen aan een OU ook policies gekoppeld worden. Een policy is een verzameling gebruikers- en computerinstellingen. Zo kan een grouppolicy b.v. verhinderen dat bepaalde gebruikers nieuwe programma's kunnen installeren, een configuratie wijzigen of het uitzicht van het bureaublad aanpassen.

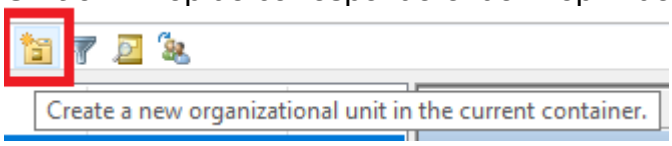
Samengevat, het ontwerp van de structuur van OU's zal enerzijds het antwoord weerspiegelen op de vraag: "Wie beheert wat?" en anderzijds rekening houden met group policies die de gebruikersomgeving moeten controleren en voor de nodige beveiliging moeten zorgen.

3.2 OU's beheren

3.2.1 Een organizational-unit aanmaken

- Selecteer in ADUC de container waarin je de OU wenst te maken, hier opleidingen.intra.

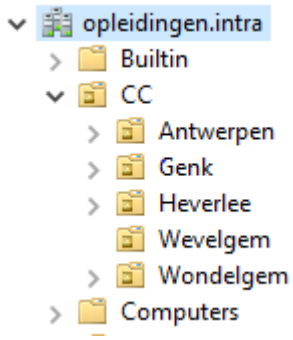
- Klik met de rechtermuisknop op de container en kies **New > Organizational Unit** of klik op de corresponderende knop in de werkbalk.



- Geef de OU een naam, b.v. CC

- Haal al dan niet het vinkje weg bij Protect container from accidental deletion. Als deze optie aangevinkt is, kan je de OU niet verwijderen, tenzij je expliciet de toegangsrechten op de OU aanpast.

- Maak de structuur onder CC verder af volgens onderstaand voorbeeld.



3.3 Accounts verplaatsen naar een OU

Er zijn twee manieren om accounts (users) te verplaatsen naar een andere OU:

- Met drag en drop een object van een container naar een OU verslepen.
- Via de opdracht Move in het snelmenu van een object.

- Maak twee accounts (users) aan in de OU CC, b.v. Jip en Janneke.[1]

- Verplaats Janneke met drag en drop naar Antwerpen.

- Verplaats Jip via de opdracht Move naar Wevelgem.

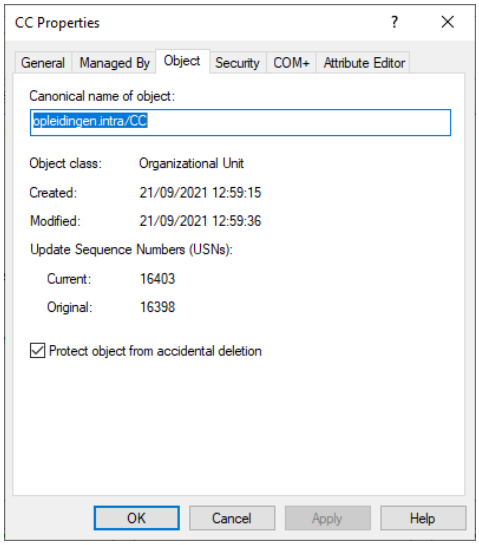
Tip: om meerdere accounts tegelijkertijd te verplaatsen kan je een meervoudige selectie gebruiken.

3.4 Een beveiligde OU verwijderen

Een OU wordt standaard beveiligd tegen per ongeluk verwijderen. Als je een OU toch wilt verwijderen moet je die beveiliging eerst opheffen. De beveiliging komt er

[1] Als je niet weet hoe je een gebruikersaccount aanmaakt vind je uitleg in paragraaf 4.1 Een gebruikersaccount maken.

op neer dat het systeem het recht om het object (de OU) te verwijderen voor iedereen op geweigerd (Deny) heeft gezet.



Je moet lid van de Domain Admins zijn om onderstaande procedure uit te voeren.

- Open ADUC en activeer **Advanced Features**.
- Klik met de rechtermuisknop op de OU die je wenst te verwijderen en kies **Properties**.
- Leg het tabblad **Object** bovenop en haal het vinkje weg bij **Protect object from accidental deletion**.

Opmerking: ook om een OU te verplaatsen zal je de rechten op de OU moeten aanpassen. Verplaatsen betekent immers kopiëren en verwijderen.

- Maak een OU Extra die beveiligd is tegen verwijderen.
- Neem daarna de nodige maatregelen om de OU toch te verwijderen.

3.5 Het beheer van een OU

Delegeren van het beheer is een belangrijke reden om te werken met OU's.

Zo kan je een gewone gebruiker beperkte beheerrechten verlenen uitsluitend op objecten binnen een bepaalde OU.

Bovendien kan je de beheerrechten van die gebruiker niet alleen beperken tot een deel van het domein, maar ook tot bepaalde taken.

Opmerking

Ook door een gebruiker lid te maken van bepaalde groepen kan je die gebruiker beheerrechten geven. Zo krijgt een gebruiker die lid is van de groep 'account operators' het recht nieuwe gebruikers aan te maken. Dit recht geldt dan echter op het volledige domein. Op deze ingebouwde groepen en hun rechten wordt verderop in de cursus teruggekomen.

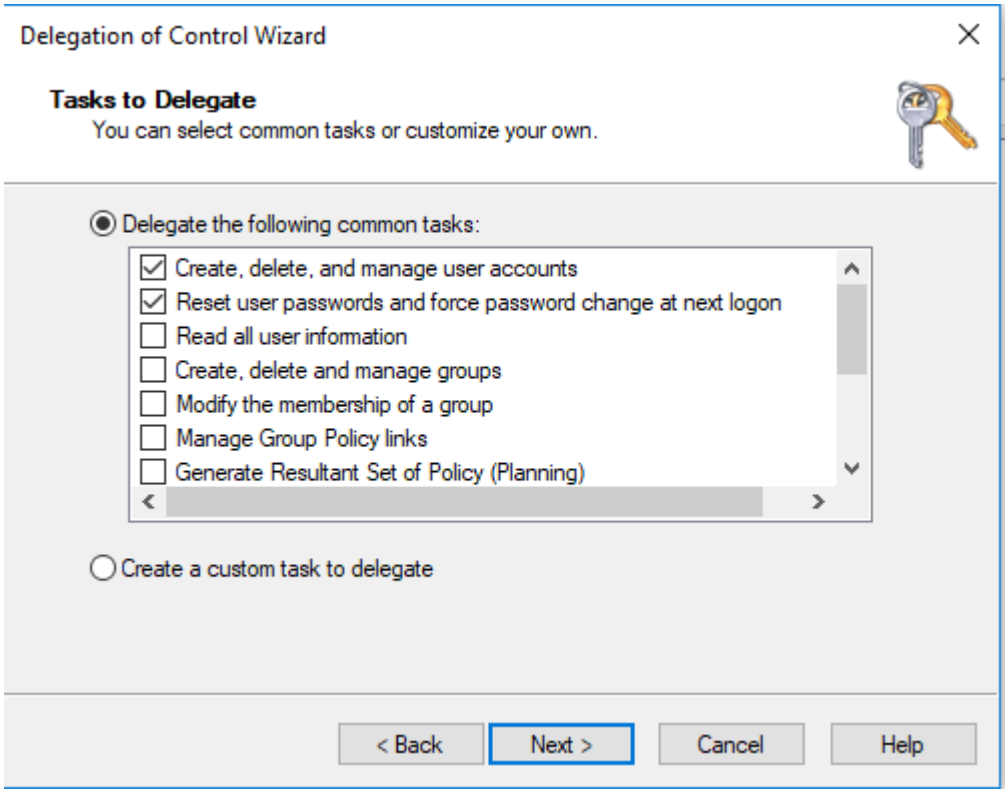
3.5.1 Het beheer van een OU delegeren

- Open ADUC in normale weergave.
- Klik met de rechtermuisknop op de OU waarvan je het beheer wenst te delegeren en kies **Delegate Control** in het snelmenu. De bijbehorende wizard wordt gestart.

In de eerste stap beslis je aan welke gebruikers of groepen je het beheer wenst te delegeren.

- Klik op **Add** en selecteer de gewenste gebruiker(s) en/of groep(en).

In de volgende stap beslis je welke taken je wenst te delegeren. Onder **Delegate the following common tasks** vind je een lijst met een aantal veel voorkomende taken.



Op het laatste scherm van de wizard volgt nog een samenvatting en de opdracht wordt uitgevoerd.

Vind je bij de **Common tasks** je gading niet dan kan je kiezen voor **Create a custom task to delegate**.

In dat laatste geval geef je eerst op voor welke objecten het beheer mag gedelegeerd worden en vervolgens welke rechten mogen gedelegeerd worden.

Voorbeeld:

- Delegeer het beheer van de OU Antwerpen aan Janneke. Zij krijgt het recht accounts te maken in de OU en wachtwoorden aan te passen.

Opmerking:

Dit is een eerste kennismaking met het delegeren van beheertaken. Later komt dit opnieuw aan bod. In de praktijk zal bij het delegeren van taken met groepen gewerkt worden. Voor de eenvoud wordt hier slechts één gebruiker aangeduid.

3.5.2 Controleren welke instellingen de wizard doorgevoerd heeft.

Als je het beheer van een OU delegeert naar een gebruiker, dan komt het er eigenlijk op neer dat je die gebruiker het recht geeft bepaalde handelingen uit te voeren op die OU.

In de volgende stappen ga je na welke rechten de wizard ingesteld heeft om jouw gebruiker het recht te geven accounts in de OU Antwerpen aan te maken en wachtwoorden aan te passen:

- Open ADUC en activeer **Advanced Features**
- Klik met de rechtermuisknop op de OU Antwerpen en kies **Properties**
- Activeer het tabblad **Security** en klik op de knop **Advanced**

Je vindt hier twee vermeldingen voor de gebruiker, één voor het object en al zijn afhankelijke objecten en één alleen voor de afhankelijke objecten van het type user.

- Selecteer één van de twee entries en klik op **Edit** om meer gedetailleerd informatie te krijgen over de rechten die jouw gebruiker gekregen heeft.

4 GEBRUIKERS

4.1 Een gebruikersaccount maken

- Start ADUC
- Klik met de rechtermuisknop op de container waarin je de account wenst te maken.
- Kies **New** en vervolgens **User** via het contextmenu.

In het eerste dialoogvenster komt de naam van de gebruiker

De Full name wordt automatisch opgebouwd op basis van de First name, Initials en Last name. Deze namen komen vooral van pas in zoekopdrachten en zoekresultaten, maar worden overigens niet gebruikt door het besturingssysteem.

Om aan te melden gebruikt een gebruiker zijn **User logon name**, b.v. Jean. Een logon naam is niet hoofdlettergevoelig.

Aan die logon name wordt standaard de naam van het topdomein in het forest toegevoegd om tot de UPN (User Principal Name) te komen, die de vorm heeft van een e-mail adres, b.v. Jean@opleidingen.intra. Afhankelijk van de structuur van het forest kan in de lijst gekozen worden voor de domeinnaam van het topdomein, van het huidige domein of alternatieve UPN suffixen die aangemaakt werden via Active Directory Domains and Trusts. In een structuur met slechts één domein in één forest is er slechts één keuze mogelijk.

De **Pre-Windows 2000 logon naam** moet compatibiliteit met oudere systemen die nog met NetBIOSnamen werken, garanderen.

De afhandeling van de aanmelding gebeurt in beide gevallen op een verschillende manier.
In het eerste geval handelt de domein controller de vraag voor authenticatie af.

In het tweede geval wordt de aanvraag doorgespeeld naar de global catalog. De global catalog lokaliseert het bijbehorende domein op basis van de UPN, verwerkt de aanvraag tot authenticatie en maakt een lijst van de universele groepen waar de gebruiker lid van is.

Na een klik op Next kan je in het tweede dialoogvenster een voorlopig wachtwoord invullen. Wachtwoorden zijn wel hoofdlettergevoelig. Standaard eist Windows Server dat een wachtwoord minimum 7 karakters lang en voldoende ingewikkeld is. Voldoende ingewikkeld betekent concreet dat van de vier karakterverzamelingen (kleine letters, hoofdletters, cijfers en speciale karakters) er minstens drie vertegenwoordigd zijn in het wachtwoord.

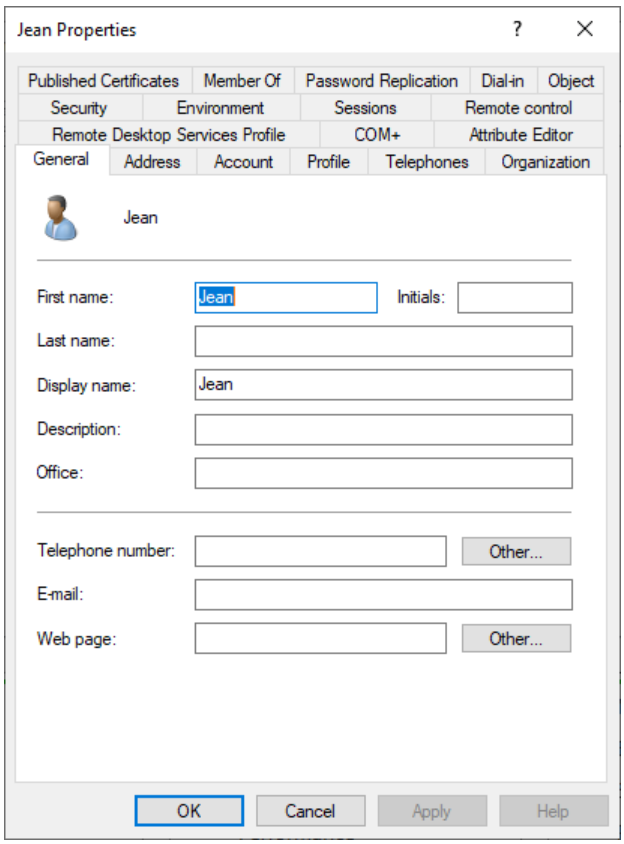
De overige opties in het dialoogvenster zijn:

User must change password at next logon	De gebruiker stelt bij een volgende aanmelding zelf een nieuw wachtwoord in
User cannot change password	Alleen beheerders mogen het wachtwoord wijzigen, deze optie is niet te combineren met de vorige en geldt niet voor administrators.
Password never expires	Standaard blijft een wachtwoord slechts 42 dagen geldig. Als deze termijn verlopen is, wordt een gebruiker verplicht een nieuw wachtwoord te kiezen, tenzij deze optie actief is. Deze optie heeft voorrang op de instellingen bij Password policy. In de praktijk wordt deze optie ingesteld bij accounts waarmee bepaalde services opgestart worden.
Account is disabled	De account kan niet gebruikt worden om aan te melden, maar bestaat nog in de database. Dit kan van pas komen voor model accounts of voor accounts die tijdelijk buiten gebruik moeten gesteld worden.

🛠 Maak een gebruiker Fien in de OU Heverlee.

4.2 De eigenschappen van een gebruikersaccount

De eigenschappen van een gebruiker kunnen opgeroepen worden door met de rechtermuisknop op de gebruiker te klikken en dan in het snelmenu te kiezen voor **Properties**.



Hieronder volgt een kort overzicht van de verschillende tabbladen. Op een aantal van deze tabbladen wordt ook nog in volgende hoofdstukken teruggekomen.

Sommige tabbladen zijn louter informatief. Deze velden al dan niet invullen heeft geen invloed op wat de gebruiker al dan niet kan op het domein. Op basis van de inhoud van deze velden kan een gebruiker wel teruggevonden worden in de AD DS, b.v. via een query.

General	Algemene gegevens i.v.m de gebruiker zoals voornaam, achternaam, beschrijving, telefoonnummers, email adres enz.
Address	Adresgegevens van de gebruiker
Telephones	Allerlei telefoonnummers.
Organization	De functie van de gebruiker, het departement waarvoor hij werkt, de manager waarvoor hij werkt enz.

De andere tabbladen bevatten velden waarvan de inhoud wel de toegang tot bepaalde objecten op het domein kan beïnvloeden.

Account	Hier staan o.a. de gegevens die bij het aanmaken van de account meegegeven werden. **User Logon Name**: de naam waarmee de gebruiker zich aanmeldt, die kan hier ook gewijzigd worden. **Pre-Windows2000**: Om aan te melden op domeinen in Windows 2000 mixed mode.

	Logon Hours: Standaard kan een gebruiker zich 24 uur op 24, 7 dagen op 7 aanmelden. Klik op de knop Logon Hours om dit te veranderen. Selecteer een blok tijd en klik op Logon Permitted of Logon Denied. Gebruikers worden standaard niet uit het systeem gegooid als ze zich al hebben aangemeld en de Logon-Denied-tijd is aangebroken. Als ze zich afmelden, kunnen ze zich echter niet opnieuw aanmelden totdat de Logon Permitted-tijd aanbreekt. **Logon To:** Standaard mag een gebruiker zich op eender welke niet server op het netwerk aanmelden. Via de knop Logon To kan een beheerder machinenamen in het dialoogvenster invoeren. Hierdoor kunnen de gebruikers zich alleen via de opgegeven machines aanmelden. Opmerking: Deze instelling beïnvloedt alleen het aanmelden met een domeinaccount en niet het aanmelden met een lokale account. **Unlock account**: indien een account teveel keer een verkeerd paswoord heeft ingegeven, kan het zijn dat deze gelocked staat en met deze optie kan de vergrendeling opgeheven worden. **Account Options**: Sommige van de opties bestonden ook al in Windows NT 4.0 en zijn vanzelfsprekend, andere opties zijn erg geavanceerd. **Account Expires**: Om accounts zo in te stellen dat ze automatisch worden geblokkeerd als de ingestelde datum bereikt wordt. Deze instelling is uitermate handig voor seizoenskrachten of tijdelijke werknemers.
Profile	Waar worden het profiel en de homedirectory van een gebruiker opgeslagen en welk logonscript wordt uitgevoerd als de gebruiker zich aanmeldt. Hierop wordt verderop teruggekomen.
Member Of	Toont tot welke groepen de gebruiker behoort. De gebruiker kan via dit tabblad ook aan groepen toegevoegd worden.
Dial-In	Mag de gebruiker inbellen op een Network Policy Server?

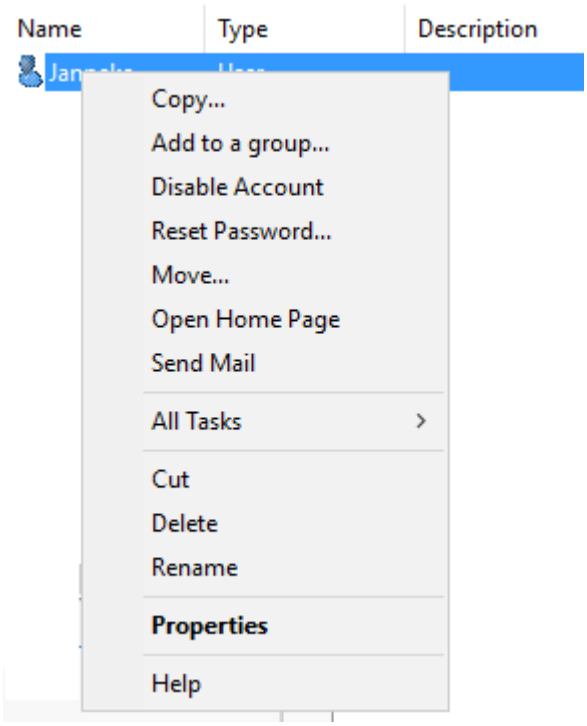
Nog andere tabbladen hebben te maken met terminal services en remote desktop verbindingen

Environment	Configureert de omgeving bij het gebruik van terminal services: welk programma moet opgestart worden, moet de printer toegankelijk zijn tijdens de sessie, …
Sessions	Bepaalt de timeout en reconnection instellingen van terminal services
Remote control	Configureert terminal services en remote control instellingen.

Remote desktop services profile	Configureert het profiel voor de gebruiker uitsluitend bij gebruik van terminal services

4.3 Gebruikersaccounts beheren

Als je met de rechtermuisknop op een account klikt vind je in het snelmenu de beheeropdrachten.



4.3.1 Een account kopiëren

De opdracht **Copy** maakt een kopie van een account. De gekopieerde account neemt een aantal eigenschappen van de oorspronkelijke account over zoals lidmaatschap van groepen, logon hours, profielinstellingen, logonscripts, …

Adresgegevens, telefoonnummers, wachtwoord, e.d. worden uiteraard niet gekopieerd. Vanaf Windows 2003 werken ook de typische Windows drag and drop technieken om te kopiëren.

Voorbeeld:

- Vul bij de eigenschappen van Janneke op de tabbladen General, Address en Organization een aantal eigenschappen in.
- Kopieer de account van Janneke, geef de nieuwe account een naam en wachtwoord en ga na welke eigenschappen van Janneke overgenomen werden in de kopie en welke niet.

4.3.2 Een account toevoegen aan een groep

Add to a group: maakt de account lid van een groep. (zie ook 6.1.2 Gebruikers lid maken van een groep)

4.3.3 Een account tijdelijk uitschakelen

Disable account: dient om bij langdurige afwezigheid van een gebruiker een account tijdelijk buiten gebruik te stellen of om te vermijden dat een modelaccount misbruikt wordt om aan te melden.
De optie kan ook van pas komen als een medewerker het bedrijf verlaat en je zijn account nog niet onmiddellijk wenst te verwijderen.
De optie in het menu verandert in **enable account** na het buiten werking stellen van de account. In ADUC wordt de account gemarkeerd met een witte cirkel met een pijl naar beneden erin.

Voorbeeld

- Schakel de account uit die je zojuist via Copy hebt gemaakt.

4.3.4 Een wachtwoord wijzigen

Met **Reset password**: kan je als beheerder het wachtwoord van een gebruiker veranderen, b.v. als die gebruiker zijn wachtwoord vergeten is. De beheerder kan meteen ook aanvinken dat de gebruiker bij een volgende aanmelding zijn wachtwoord zelf opnieuw moet wijzigen.

Voorbeeld

- Wijzig het wachtwoord van een gebruiker.

4.3.5 Een account verplaatsen

Met de opdracht **Move** kan een account van een container naar een andere container verplaatst worden. Vanaf versie 2003 kan dit ook met de klassieke drag en drop technieken. (zie ook 3.3 Accounts verplaatsen naar een OU)

4.3.6 De naam van een account veranderen

De naam wijzigen van een account kan via de opdracht **Rename**. Dit kan nuttig zijn als je alle eigenschappen van de account zoals gebruikersrechten, toegangsrechten en lidmaatschap van groepen wilt behouden, maar de account wilt toekennen aan een andere gebruiker.

4.4 Standaard gebruikersaccounts

Bij het opzetten van het domein worden al twee gebruikers aangemaakt in de container users: de administrator account en de guest account.

4.4.1 De administrator account

De administrator is een gebruiker met volledige controle over het domein. Het wachtwoord van de administrator wordt opgegeven bij het opzetten van het domein. Vergeten van het wachtwoord betekent opnieuw installeren!
De naam van de administrator kan veranderd worden, maar de account kan niet verwijderd worden. Elke administrator heeft best nog een gewone gebruikersaccount om andere taken dan beheertaken uit te voeren.

Vanuit beveiligings standpunt is de administrator een erg gevaarlijke account, omdat hij zoveel rechten heeft.

Microsoft besturingssystemen ontwikkeld na Windows 2000 Server en Windows XP laten toe met een secundaire aanmelding te werken via de **Runas** opdracht. Bij heel wat tools vind je deze opdracht terug in het snelmenu. Bij sommige verschijnt de Runas opdracht alleen als je tijdens het klikken ook de Shifttoets ingedrukt houdt. Deze optie geeft je de gelegenheid één bepaalde toepassing uit te voeren met een andere account dan de aangemelde gebruiker. Meestal wordt dit gebruikt om een toepassing uit te voeren als administrator, terwijl je aangemeld bent als

gewone gebruiker. Zo kan je het aanmelden met de administratoraccount tot een minimum beperken.

Enkele eenvoudige beveiligingstips i.v.m. de administrator account:

- Hernoem de account. De aanmeldingsnaam is immers al de helft van de informatie nodig om op het netwerk te geraken.
- Geef een account met de naam administrator weinig rechten (=gewone gebruiker van het domein).
- Maak voor de administrator ook een gewone user account aan die geen lid is van de administrators group.
- Meld als beheerder zo weinig mogelijk aan met de administrator account op clients. Meld aan met je gewone account en gebruik Runas om administratieve taken uit te voeren waarvoor je bijzondere rechten nodig hebt. Dikwijls kan je ook remote werken.

4.4.2 De guest account

De guest account is ter beschikking voor gebruikers die geen account hebben en die af en toe toch toegang tot het systeem moeten krijgen.

Gebruikers die aanmelden met de guest account kunnen toegang krijgen tot gegevens en toepassingen, maar kunnen geen software installeren of instellingen van hardware wijzigen. Standaard is deze account uitgeschakeld en zijn de opties **User cannot change password** en **Password never expires** ingeschakeld.

Alhoewel deze account slechts beperkte rechten heeft, kan hij toch misbruikt worden om toegang te krijgen tot het systeem. Het is dan ook nuttig met volgende beveiligingstips rekening te houden

- Laat de account uitgeschakeld als hij niet gebruikt wordt.
- Geef de account een wachtwoord.

4.5 InetOrg accounts

Een Inetorg account is een LDAP account type dat vergelijkbaar is met een gebruikersaccount, maar kan samenwerken met andere X.500 directory services.

Een gebruikersaccount kan te allen tijde omgezet worden naar een InetOrg account en omgekeerd.

4.6 Managed service accounts

Microsoft heeft managed service accounts ingevoerd om te gebruiken bij installatie van bepaalde toepassingen of services.

Het is een account uitsluitend bestemd om een bepaalde service, batch job of beheertaak uit te voeren.

Specifieke kenmerken zijn:

- De account gebruikt een complex, automatisch gegenereerd wachtwoord. Het systeem wijzigt het wachtwoord automatisch wanneer nodig volgens de wachtwoord policy.
- De account kan niet uitgesloten worden of gebruikt worden om interactief aan te melden.
- Met eenzelfde managed service account kan slechts op één enkele computer aangemeld worden.

Meer info vind je op:

https://www.ntweekly.com/2018/02/07/configure-managed-service-accounts-windows-server-2016/

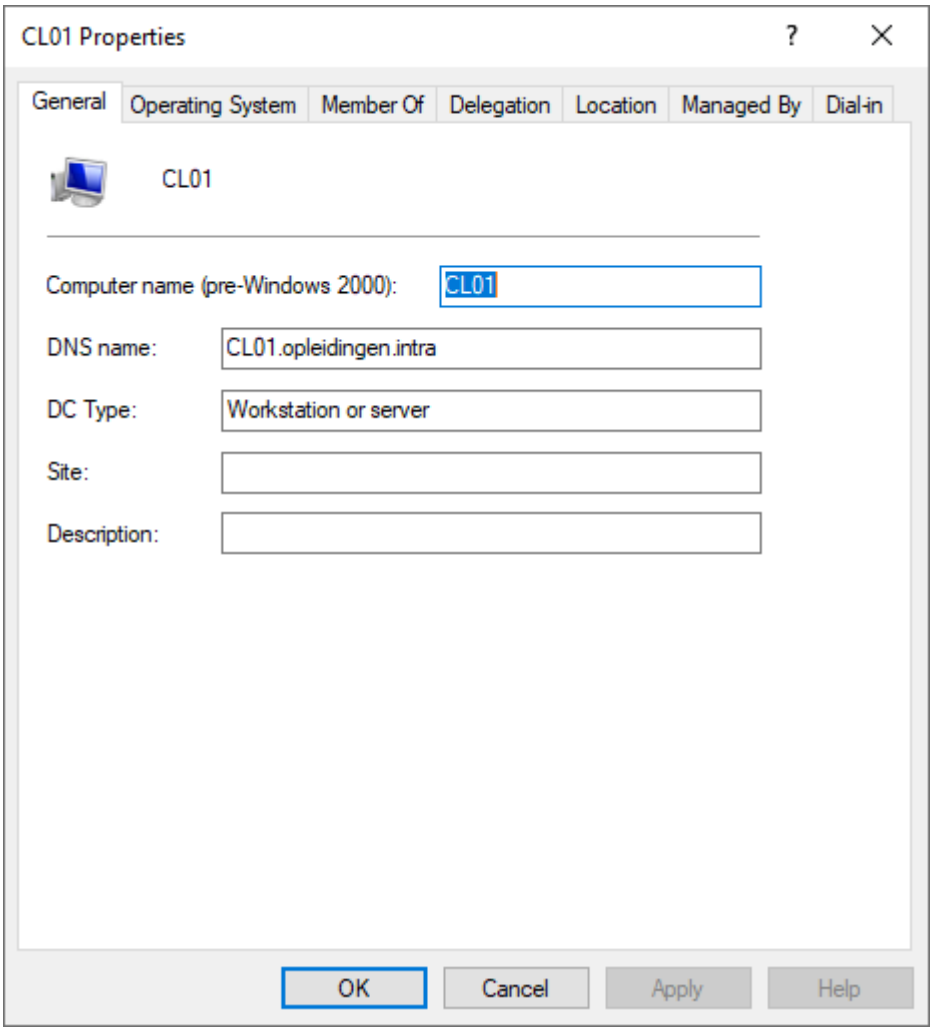
https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

5 COMPUTERACCOUNTS

Elke computer die lid wordt van het domein krijgt een computeraccount. Standaard komt die in ADUC terecht in de container Computers. Op basis van deze account krijgt de computer toegang tot bepaalde objecten op het domein.

5.1 De eigenschappen van een computeraccount

Ook een computeraccount heeft eigenschappen die kunnen opgeroepen worden door met de rechtermuisknop op de account van de computer te klikken en te kiezen voor **Properties.** Er verschijnt een dialoogvenster met een aantal tabbladen**.**



General	Elke computer wordt geïdentificeerd aan de hand van twee namen: de hostnaam of DNSnaam en de NetBIOS of Pre-Windows 2000 naam.
Operating system	Hier vind je het besturingssysteem dat op het toestel geïnstalleerd werd, de versie van dat besturingssysteem en het Service Pack

Member of	Een computeraccount kan ook lid zijn van een aantal groepen. Standaard wordt die bij het lid maken van het domein automatisch ook lid van de groep 'Domain Computers'
Delegation	De standaardinstelling is hier dat de computer niet mag gebruikt worden voor delegatie. Concreet betekent dit dat een computerservice geen toegang kan krijgen tot een netwerkobject in naam van de aangemelde gebruiker.
Location	Waar bevindt de computer zich, b.v. in welke afdeling, op welke verdieping.
Managed by	Wie is verantwoordelijk voor het beheer van de computer? De info is zuiver administratief.
Dail-in	Instellingen ivm Network Access Permission en Callback.

5.2 Het snelmenu van een computeraccount

In het snelmenu van een computeraccount vind je naast de gebruikelijke opdrachten als Add to a group, Disable Account, Move, Delete, ... ook nog de opdrachten **Manage** en **Reset** account.

5.2.1 Manage

Mits de nodige firewall poorten open staan op de computer kom je via de opdracht **Manage** terecht in de toepassing computermanagement van de computer.

5.2.2 Reset Account

Bij het aanmelden zet een computer een aparte communicatie verbinding op met de domein controller. De domein controller slaat een willekeurig wachtwoord op voor authenticatie over die verbinding. Dat wachtwoord wordt elke 30 dagen gewijzigd.

Soms ontstaat er een verschil tussen het wachtwoord van de computer en dat opgeslagen op de domein controller en dan faalt de communicatie tussen beide computers en verschijnt een melding die verwijst naar een verbreking van de trust tussen beide computers. Bij een cllient kan je die dan gewoon uit het domein halen en opnieuw lid maken van het domein om het probleem op te lossen. Voor memberservers die een bepaalde functie vervullen en configuratie informatie opslaan in Active directory kan dit echter problemen veroorzaken.

5.3 Een computeraccount aanmaken

Zodra een computer lid wordt van een domein krijgt die automatisch een account in dat domein. Standaard komt die account terecht in de container computers.

In de meeste omgevingen is het echter wenselijk dat de computeraccounts geplaatst worden in een bepaalde OU in functie van het vereiste beveiligingsbeleid. Zeker voor servers zal in veel gevallen een aangepast beveiligingsbeleid van toepassing zijn.

Via ADUC kan je ook vooraf in een bepaalde OU een account aanmaken voor een computer (prestaging). Zodra die computer dan lid gemaakt wordt van het domein komt die automatisch in de juiste OU terecht.

6 GROEPEN

Het mag duidelijk zijn dat beheer van een netwerk op een gebruiker per gebruiker basis niet erg overzichtelijk en efficiënt gebeurt. Gelukkig kunnen groepen van het type security gebruikt worden om accounts te groeperen die eenzelfde toegang moeten krijgen tot een bepaald object. Elke security groep krijgt dan ook een eigen Security ID (SID).

6.1.1 Een groep maken

Alleen gebruikers die lid zijn van de domain administrators kunnen nieuwe groepen aanmaken. Om een groep te maken kan je ADUC gebruiken.

- Klik in het linkse paneel met de rechtermuisknop op de container of OU waarin je de groep wenst te plaatsen, b.v. CC
- Kies New in het snelmenu en vervolgens Group

Net zoals de andere security principals krijgt een groep ook een naam en een NetBIOS of pre-Windows 2000 naam. Geef de groep de naam ExterneLesgevers.

Andere eigenschappen van een groep die bij het maken ingesteld worden:

Group type

Een groep van het type Security heeft een SID, een groep van het type Distribution niet. Op basis van lidmaatschap van een distributiegroep kan een gebruiker dan ook geen toegang krijgen tot bepaalde objecten. De distributiegroepen worden vooral in het kader van Exchange gebruikt.

Het type van een groep kan achteraf te allen tijde veranderd worden. Bij het converteren van een groep van het type security naar een groep van het type distribution verliest de groep wel zijn SID en alle leden verliezen meteen ook de rechten geassocieerd met de SID.

In deze module wordt verder alleen met security groepen gewerkt.

- Kies het type Security voor de ExterneLesgevers

Group scope

De eigenschap group scope bepaalt of een groep alleen op het eigen domein zichtbaar is of ook in andere domeinen binnen hetzelfde forest. De betekenis van de verschillende scopes hangt verder af van het functional level van het domein.

Onderstaande tabel toont de gevolgen van een scope op de regels voor het lidmaatschap van de groep:

Scope van de groep	Waar zichtbaar?	Wie mag erin?
Domain local	Uitsluitend op het eigen domein	Universele groepen; gebruikers en globale groepen van elk domein in het forest; domein

		lokale groepen van hetzelfde domein
Globale groepen	Binnen het forest	Gebruikers en globale groepen van het eigen domein
Universele groepen	Binnen het forest	Universele groepen; gebruikers en globale groepen van elk domein in het forest.

- Maak van de groep ExterneLesgevers een globale groep

6.1.2 Gebruikers lid maken van een groep

Je kunt zowel uitgaan van de gebruiker als van de groep om een gebruiker lid te maken van een groep.

Maak Jip lid van de groep ExterneLesgevers.

- Klik met de rechtermuisknop op de account van Jip en kies in het snelmenu voor **Add to a group**. Het dialoogvenster Select Groups verschijnt.
- Typ de eerste letters van de naam van de groep, ‘Ext’ , en klik op de knop **Check Names**. Als de naam gevonden wordt in AD DS, wordt die onderlijnd.
- Klik op **OK**.

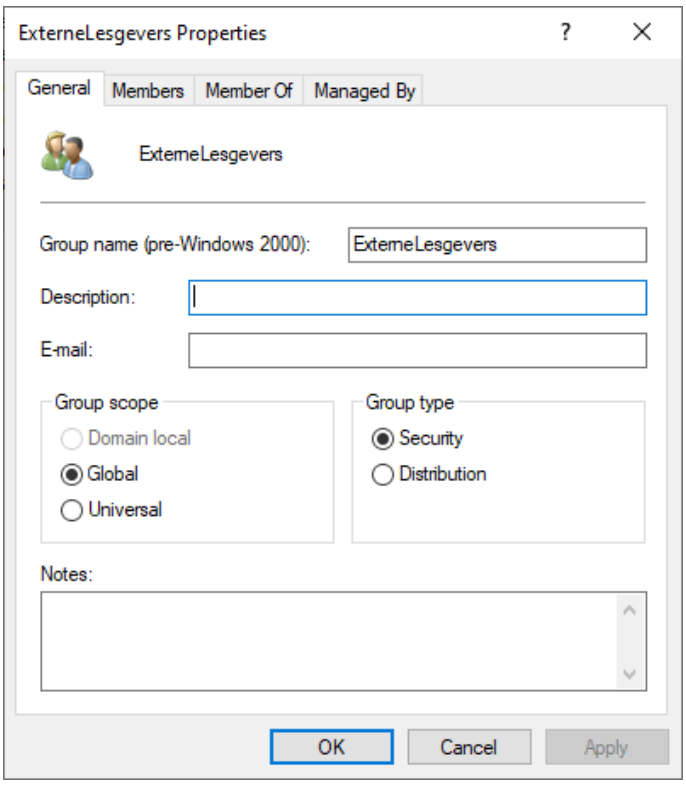
De melding **The Add to Group operation was successfully completed** beëindigt de procedure.

Hoe maak je Janneke lid van ExterneLesgevers, uitgaande van de groep?

- Klik met de rechtermuisknop op de account van de groep en kies **Properties**.
- Activeer het tabblad **Members**
- Klik op **Add**. Het dialoogvenster **Select Users, Contacts, Computers , Service Accounts or Groups** verschijnt.
- Typ de eerste letters van de naam van de account en klik op **Check names**.
- Klik op **OK** totdat alle dialoogvensters gesloten zijn.

6.1.3 Eigenschappen van groepen

De eigenschappen van groepen roep je op dezelfde manier op als de eigenschappen van andere objecten: Klik met de rechtermuisknop op de groep en kies **Properties**.



Op het tabblad **General** vind je de attributen die je bij het aanmaken van de groep hebt meegegeven.

Eventueel kan hier nog een e-mail adres voor de groep ingevuld worden. Mails gestuurd naar dit adres zullen bij alle leden van de groep bezorgd worden.

In het veld **Notes** kan nog wat bijkomend commentaar ter attentie van de beheerders opgenomen worden.

Het tabblad **Members** toont de accounts die lid zijn van de groep en laat toe accounts toe te voegen of te verwijderen.

Als een andere groep lid is van de groep, dan kan je dubbel klikken op die geneste groep en dan worden de leden van de geneste groep getoond.

Member Of toont een lijst groepen waarvan de geselecteerde groep lid is. Je kunt hier groepen toevoegen of verwijderen.

Door telkens dubbel te klikken op een groep in de lijst kan je heel de hiërarchie van geneste groepen terug samenstellen.

Op het tabblad **Managed b**y kan je via de **Change** knop de manager van de groep aanduiden.

De knop **Properties** brengt je naar de eigenschappen van de manager. Enkele van die eigenschappen worden ook automatisch overgenomen op het tabblad.

Clear verwijdert de manager.

Manager can update membership list delegeert het beheer van het lidmaatschap van de groep naar de manager. Voor security groepen is dit vanuit

beveiligingsoverwegingen niet aan te raden. Voor distributiegroepen kan dit wel nuttig zijn.

6.1.4 Het plannen van groepen

Wanneer gebruik je domein lokale, globale of universele groepen?

Als beheerder is het je verantwoordelijkheid ervoor te zorgen dat gebruikers toegang krijgen tot de objecten waarmee ze moeten werken. Die objecten kunnen e-mails, bestanden, printers, software applicaties, enz. zijn. Omgekeerd moet je er ook voor zorgen dat gebruikers geen toegang krijgen tot de objecten die ze niet nodig hebben of waar ze niet bij mogen.

Een beheer gebaseerd op rollen moet dit mogelijk maken op een overzichtelijke en efficiënte manier. Het moet snel antwoord kunnen geven op vragen van het type: “Tot welke objecten heeft Janneke toegang?” en “Wie heeft er toegang tot de map cursusmateriaal?”. Het baseert zich dus op een benadering volgens **wie** mag **wat** en **waar.**

6.1.4.1 Groepen die overeenkomen met een rol.

Een groep die overeenkomt met een rol definieert een verzameling gebruikers of computers die een gemeenschappelijke rol of functie vervullen binnen het netwerk.

In een competentiecentrum kan je b.v. de rollen cursist, instructeur, externe lesgever, manager, administratief personeel, … terugvinden.

Voor groepen die corresponderen met een **rol** worden typisch **globale** security groepen gebruikt. Globale groepen staan voor **wie** ergens iets mag doen.

6.1.4.2 Groepen die overeenkomen met toegangsrechten

We gaan nu uit van een map “cursusmateriaal” waar de cursisten leesrechten op moeten krijgen en lesgevers schrijfrechten. Je kunt het leesrecht rechtstreeks aan de globale groep cursisten geven, maar stel dat er een externe lesgever ook leesrechten moet krijgen.

Er zijn dan verschillende opties mogelijk, maar geen enkele is echt naar wens.

De externe lesgever opnemen in de groep cursisten	Dit strookt niet met de logica van de globale groep cursisten
De externe lesgever opnemen in de groep lesgevers	Dan krijgt de account te veel rechten
De account van de externe lesgever apart leesrechten geven op de map of een globale groep externe lesgevers maken die leesrechten krijgt op de map	Elke uitzondering gaat dan apart leesrechten moeten krijgen of elke groep die leesrechten nodig heeft gaat apart leesrechten moeten krijgen. Op termijn gaat dit onoverzichtelijk worden

Een betere benadering is een groep maken die alle accounts groepeert die leesrechten moeten krijgen op de map “cursusmateriaal”. Deze groep zou dan de naam “Cursusmateriaal_Read” krijgen.

In die groep worden de globale groepen opgenomen die overeenkomen met de rollen cursisten en externe lesgevers.

Voor dergelijke groepen die overeenkomen met een bepaald **recht** op één enkel object worden typisch **domein lokale groepen** gebruikt.

Domein lokale groepen representeren **wat** een account **waar** kan doen.

Opmerking: Naamconventies

Om onmiddellijk duidelijk te maken welke scope bij een groep hoort, kan het nuttig zijn systematisch dezelfde prefix te gebruiker voor groepen met een bepaalde scope.

Een afspraak kan zijn dat globale groepen geen prefix krijgen en dat domein lokale groepen systematisch het prefix ACL krijgen.

6.1.4.3 AGDLP strategie

De hiervoor beschreven benadering om groepen te plannen wordt ook wel de AGDLP strategie genoemd.

A: eerst Accounts maken

G: de accounts volgens hun rol lid maken van globale groepen, alleen gebruikers van het eigen domein kunnen lid worden van een globale groep

DL: per recht dat per object moet gegeven worden een domein lokale groep maken, de globale groepen die dat recht moeten krijgen lid maken van de domein lokale groep; dit kunnen ook globale groepen van een ander domein zijn.

P: Permissies (toegangsrechten) toekennen aan de lokale groep.

AGDLP is eigenlijk de Microsoft implementatie van RBAC, Role Based Access Control.

6.1.4.4 Een uitgewerkt voorbeeld

Een netwerk is als volgt gestructureerd:

- Een topdomein met de naam vdab.be
- Een childdomein van vdab.be met naam Antwerpen.vdab.be
- Een childdomein van vdab.be met de naam Wevelgem.vdab.be

De verkopers van het domein Antwerpen moeten in de map prijzen op het domein Wevelgem kunnen lezen.

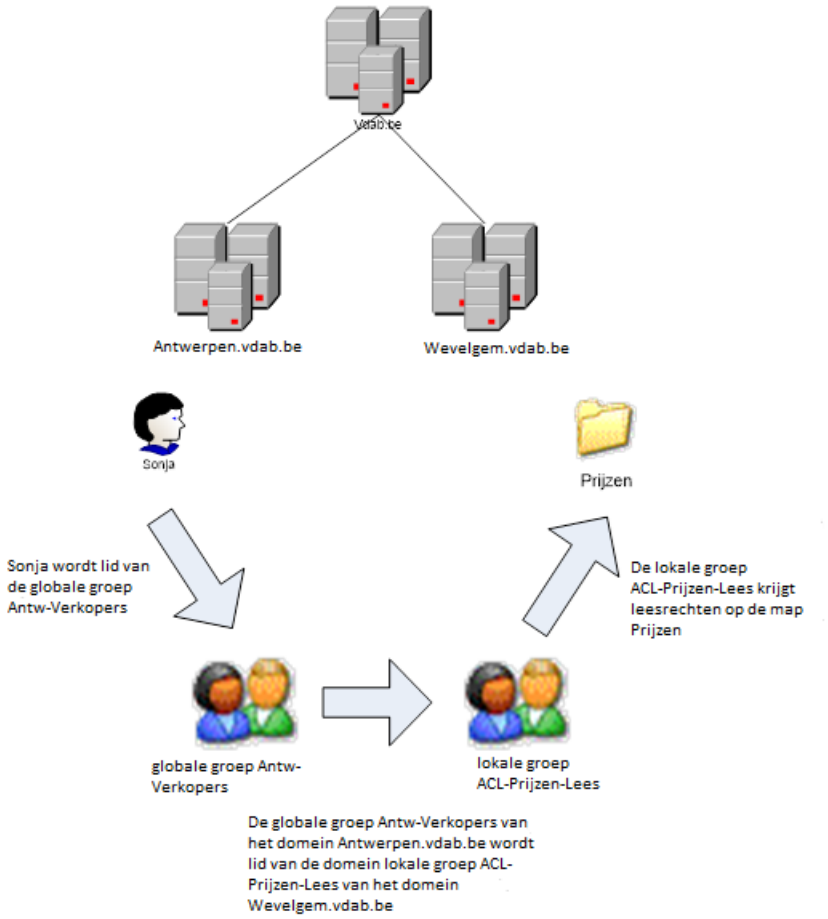
Meer concreet bekijken we hoe dit voor een gebruiker Sonja van de afdeling verkoop gerealiseerd wordt.

Sonja krijgt een account op het domein Antwerpen die net zoals alle andere medewerkers van de afdeling verkoop lid wordt van een globale groep

Antw-Verkopers. We kiezen voor een globale groep omdat het de bedoeling is gelijkaardige gebruikers bij elkaar te zetten.

Op het domein Wevelgem bestaat een domein lokale groep ACL-Prijzen-Lees die leesrecht krijgt op de map prijzen. Dit is een domein lokale groep, niet alleen omdat het de bedoeling is rechten toe te kennen aan de groep, maar ook omdat we gebruikers van een ander domein via deze groep leestoegang willen geven tot de map en globale groepen geen gebruikers van andere domeinen kunnen bevatten.

De globale groep AntwVerkopers wordt lid gemaakt van de domein lokale groep ACLPrijzenLees.



Opmerking
Het nut van de AGDLP strategie blijkt het best als er meerdere domeinen betrokken zijn. Ook op één domein blijft deze strategie nuttig om structuur te brengen in het toekennen van rechten en om toegekende rechten overzichtelijk te houden.

6.1.4.5 Universele groepen

Universele groepen gaan vooral een rol spelen in een omgeving met meerdere domeinen.

Universele groepen kunnen accounts bevatten van gebruikers, globale groepen en universele groepen van eender welk domein in het forest. Ze zijn ook zichtbaar op

alle domeinen in het forest. De leden van een universele groep worden gekopieerd naar de Global Catalog.

Waarom dan niet uitsluitend met universele groepen werken?

Het lidmaatschap van een universele groep wordt opgeslagen in de Global Catalog. Elke wijziging in dat lidmaatschap moet bijgevolg gerepliceerd worden naar alle Global Catalogs. Een wijziging in de samenstelling van de universele groep heeft dus tot gevolg dat alle leden opnieuw moeten gerepliceerd worden naar de Global Catalog. In dat geval beperk je de leden van een universele groep best tot globale groepen. Zo kan je leden toevoegen aan en verwijderen uit de globale groepen zonder dat dit replicatie in gang zet.

6.1.4.6 Groepen versus OU's

Zowel in OU's als in groepen kan je accounts groeperen. Toch spelen OU's en groepen een heel verschillende rol op een domein:

- OU's horen thuis bij de logische bouwstenen en brengen mee structuur in de netwerkobjecten, groepen daarentegen zijn accounts waaraan toegangsrechten kunnen verleend worden.
- Een account kan slechts tot één OU behoren, hij kan dan weer wel lid zijn van meerdere groepen.
- Aan een OU kan je grouppolicies koppelen, aan een groep kan dit niet.
- Aan een groep kan je toegangsrechten geven, aan een OU niet.

6.1.5 Groepen ingebouwd in een Windows Domein

6.1.5.1 Standaard groepen

Bij het opzetten van een domein met Windows server worden al een aantal groepen aangemaakt, sommige in de container **Builtin**, andere in de container **Users**.

Door een gebruiker lid te maken van één van deze groepen krijgt die extra user rights op het domein.

Zo mag een gebruiker die lid is van de groep **Account operators** gebruikers, computer en groep accounts beheren in elke container/OU op het domein behalve in de OU 'Domain Controllers'.

Een gebruiker die lid is van de **Backup operators** mag dan weer backups maken en terugzetten ook van bestanden waar hij geen toegangsrechten toe heeft.

Een meer gedetailleerde beschrijving van deze groepen vind je o.a. op https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups#default-security-groups

Enkele veel gebruikte standaard groepen

Groep	Omschrijving
Account Operators	Account Operators kunnen gebruikers, groepen en computer accounts maken en beheren in alle containers van AD DS met uitzondering van de 'Domain Controllers' OU. Account Operators hebben niet het recht om de Administrators of de Domain Admins groep te veranderen. De groep bevat standaard geen leden.
Administrators	Leden van deze groep hebben onbeperkte toegang tot alle domeincontrollers Standaard is de administrator lid van deze groep.
Guests	De Guests groep heeft slechts beperkte toegang tot de computer. De bedoeling van deze groep is gebruikers toegang verlenen tot bepaalde bronnen zonder dat ze over een volwaardige account op het domein beschikken. De meeste administrators geven geen toegang aan de Guests voor veiligheidsredenen. Standaard is de Guestaccount lid van deze groep.
Print Operators	Print Operators kunnen printers in het domein beheren, aanmaken en delen. Deze groep bevat standaard geen leden.
Remote Desktop Users	Deze speciale groep laat leden toe om vanop afstand aan te loggen op de server. Deze groep bevat standaard geen leden.
Server Operators	Server Operators kunnen de domein servers beheren. Daaronder vallen taken als het maken, beheren en verwijderen van gedeelde bronnen, het starten en stoppen van services, de harde schijf formatteren, een backup maken en het terugplaatsen van het bestandssysteem en het afsluiten van

Groep	Omschrijving
	DC's. Standaard bevat deze groep geen leden.
Users	De Users groep beperkt de toegang van zijn leden. Zij kunnen bestandssysteem en de programma bestanden niet veranderen, evenmin als de systeemtijd. Zij kunnen geen lokale printer toevoegen. Default zijn alle leden die op deze computer gecreëerd werden lid van deze groep, met uitzondering van de Guests,.

6.1.5.2 Speciale groepen

Naast de hiervoor vermelde standaard groepen maakt Windows Server ook een aantal speciale groepen aan. Het lidmaatschap van deze speciale groepen kan niet aangepast worden en zij vertegenwoordigen, afhankelijk van de omstandigheden, andere gebruikers. Gebruikers worden immers automatisch lid van één van deze groepen op het ogenblik dat ze aanmelden of een bepaald object benaderen.

Deze speciale groepen kunnen rechten krijgen, maar een lijst van leden kan niet opgevraagd worden. Group scopes zijn niet van toepassing.

Hieronder volgt een beschrijving van enkele van die bijzondere groepen.

Groep	Omschrijving
Anonymous Logon	Gebruikers en services die niet met een account aangemeld zijn.
Authenticated Users	Alle gebruikers van het lokale domein en van andere domeinen in het forest. De guest account maakt geen deel uit van de authenticated users.
Everyone	Alle gebruikers van het lokale domein, van andere domeinen in het forest en de guests. In oudere versies was ook anonymous logon lid van deze groep, maar vanaf server 2003 is dat niet meer het geval.
Network	Alle gebruikers die objecten op de computer benaderen via het netwerk.
Interactive	Alle gebruikers die lokaal of via terminal services aangemeld zijn op het toestel.

Terminal Server User	Alle gebruikers die aangemeld zijn via Remote desktop.

7 NOG HULPMIDDELEN OM ACCOUNTS TE BEHEREN

In dit hoofdstuk maak je kennis met enkele andere tools dan ADUC om accounts te beheren en leer je accounts zoeken in AD DS.

7.1 Accounts exporteren en importeren met `csvde`

Gebruikers kunnen ook ingevoerd worden in AD DS via een comma-seperated (csv) tekstbestand. Deze methode kan nuttig zijn om gebruikers gedefinieerd in een andere omgeving te importeren in AD DS. Een andere toepassing kan zijn snel een aantal gebruikers aanmaken in een testomgeving.

Het tekstbestand moet strikte regels volgen op het vlak van formaat. Enkele spelregels:

- De eerste regel van het bestand definieert de attributen die geïmporteerd worden voor de nieuwe accounts. Deze attributen worden van elkaar gescheiden door een komma.
- Elke volgende regel komt overeen met de gegevens voor een account.
- De DN (Distinguished Name) van het item dat je probeert te importeren moet zich in de eerste kolom van het CSV-bestand bevinden , anders mislukt het importeren.

Tip

Een export uit AD DS naar een .csv bestand geeft een duidelijk beeld van het juiste formaat.

Om een .csv bestand op een comfortabele manier te bewerken kan je het ook openen in excel.

Gebruik de volgende syntax om het hulpprogramma uit te voeren vanaf de opdrachtprompt:

`csvde –f <bestandsnaam>` om accounts te exporteren.

`csvde –i –f <bestandsnaam.csv>` om accounts te importeren.

- Csvde staat voor Comma Separated Value Data Exchange
- -i staat voor import
- -f staat voor file
- <bestandsnaam.csv> wordt vervangen door het pad en de naam van het tekstbestand.

Een beperking is dat csvde alleen kan gebruikt worden om nieuwe accounts te maken en niet om bestaande accounts aan te passen.

Bij de oefenbestanden vind je ledenbe.txt als voorbeeld van een bestand geschikt om te importeren met csvde. De gegevens moeten aangepast worden aan je eigen omgeving:

Een woordje uitleg bij het bestand:

De eerste regel van het bestand:

```
dn,sAMAccountName,userPrincipalName,telephoneNumber,department,l,title,userAccountControl,objectCl
ass
```

De eerste regel definieert de attributen die voor elke gebruiker geïmporteerd worden.

De tweede regel geeft waarden voor een bepaalde gebruiker.

```
"CN=Dirk Goossens,OU=CC,DC=opleidingen,DC=intra",Dirkg,Dirkg@opleidingen.intra,555-
1239,infra,Antwerpen,instructeur,514,user
```

Het eerste attribuut, dn, staat voor distinguished naam. De distinguished naam staat tussen aanhalingstekens en de structuur komt overeen met de structuur in de active directory.

```
"CN=Dirk Goossens,OU=CC,DC=opleidingen,DC=intra”
```

staat voor de gebruiker met common name **Dirk Goossens** in de OU **CC** van het domein **opleidingen.intra**.

- 🛠 Controleer of deze structuur overeen komt met de structuur op je eigen domein.

Aanpassingen die nodig kunnen zijn:

- Een OU CC aanmaken in je Active Directory als die nog niet bestaat.
- De naam van het domein aanpassen in het bestand leden.txt

- 🛠 Voer de gebruikers van het csv bestand toe in je AD.

De accounts van alle geïmporteerde gebruikers zijn uitgeschakeld, hebben een blanco wachtwoord en moeten bij een eerste aanmelding hun wachtwoord veranderen.

Het script Setpwd.vbs (zie ook bij de oefenbestanden) kan je uitvoeren om de wachtwoorden te veranderen, de accounts te activeren en uit te schakelen dat een gebruiker bij een volgende aanmelding zijn wachtwoord moet veranderen. Dit laatste geeft immers problemen als je via remote desktop probeert aan te melden.

- 🛠 Lees het script Setpwd.vbs aandachtig, probeer te begrijpen wat er gebeurt, pas het aan indien nodig (rechtermuisknop – edit) en voer het uit (dubbelklik). Op einde van uitvoering zal je een popup krijgen met oa. de OU waarin de paswoorden van de gebruikers zijn gewijzigd.

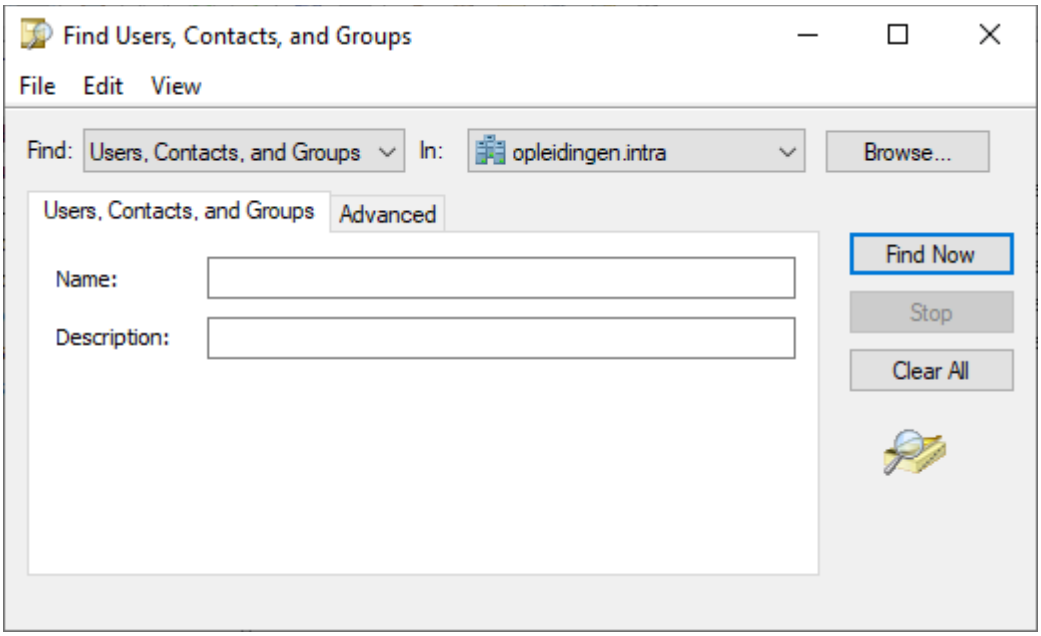
Tip

Een refresh (F5) van het venster van ADUC zal nodig zijn om het resulaat te zien.

7.2 Zoeken in AD DS

- 🛠 Start > Administrative tools > ADUC.
- 🛠 Selecteer het domein.

- Kies in het menu **Action** de opdracht **Find**.



Het dialoogvenster Find Users, contacts and groups verschijnt.

Find	Selecteer het type van het object waarnaar je op zoek bent. Naargelang de keuze die je hier maakt worden de mogelijkheden op het eerste tabblad aangepast.
In	Selecteer (via de knop 'Browse …') de locatie waar je wil zoeken, dit kan de volledige AD zijn, een welbepaald domein of een OU

Objecten worden dikwijls gezocht op basis van hun naam of omschrijving. Vul in dat geval de naam of omschrijving en en klik op **Find Now**.

Op een ander attribuut zoeken kan via het tabblad **Advanced.**

In de lijst **Field** selecteer je op welk attribuut je de zoekopdracht wilt baseren

- Via **Condition** en **Value** geef je de voorwaarde waaraan het attribuut moet voldoen om in de lijst met gevonden objecten te verschijnen.
- Klik op **Add** om het geformuleerde criterium toe te voegen aan de lijst met **Search criteria**
- Klik op **Find Now** om de lijst met gevonden objecten samen te stellen.

Enkele voorbeelden

- Ga eens op zoek naar de cursisten van Wondelgem
- Zoek ook eens de cursisten waarvan de achternaam met een K begint.

7.3 Queries in AD DS met ADUC

Vooral in grotere bedrijven zal de mogelijkheid om accounts te selecteren op basis van de waarde van bepaalde attributen van pas komen. De node **Saved Queries** kan hierbij helpen.

- ADUC > Context menu van Saved Queries > New > Query

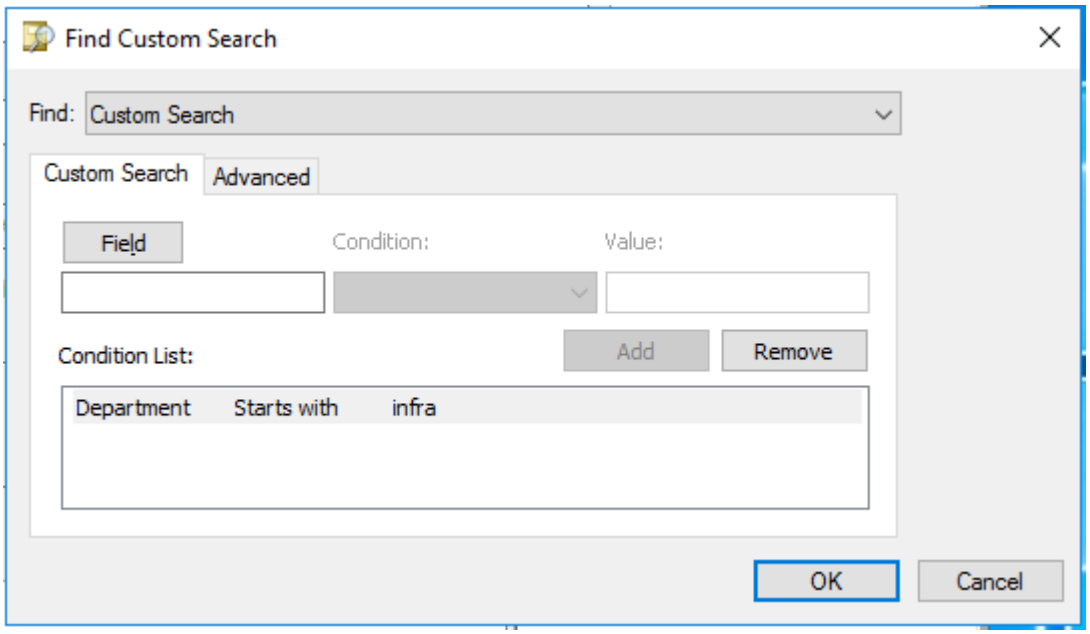
Om b.v. de gebruikers van het departement Infra te selecteren.

- Geef de query een naam in het tekstvak **Name** (Infrastructuur).
- Klik op de knop **Define Query** om de query te definiëren.

Het dialoogvenster **Find Common Queries** verschijnt waar je een aantal veel gebruikte queries kunt definiëren om accounts van gebruikers, computers en groepen terug te vinden op basis van hun naam en omschrijving.

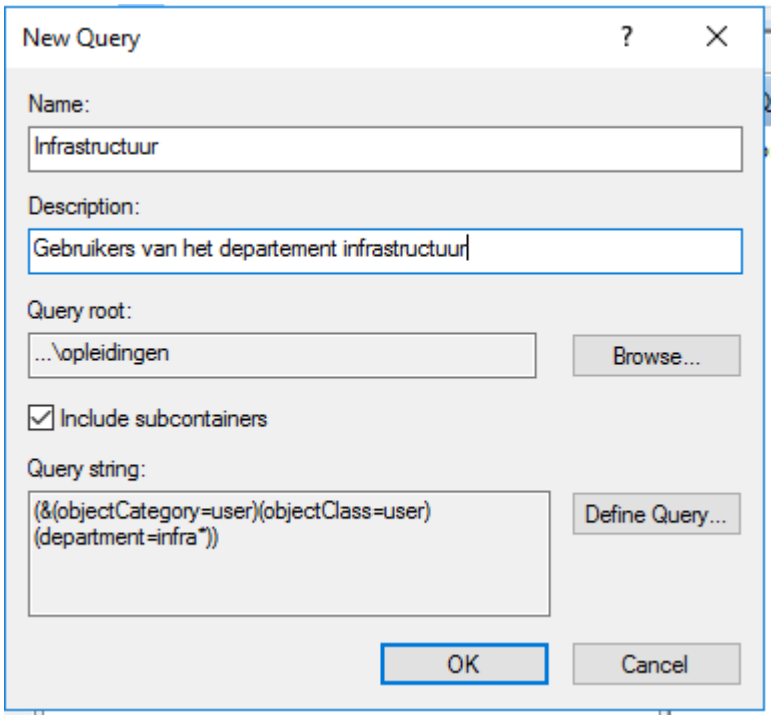
- Selecteer in de lijst bij **Find** de entry **Custom Search**.
- Klik op de knop **Field** en selecteer in de lijst **User**. Een lijst met de attributen van een user wordt opengevouwen. Selecteer hierin **Department**. Het veld **Department** verschijnt onder **Field**.
- Klik in de lijst **Condition** op **Starts with** en typ **Infra** bij **Value**.
- Klik op de knop **Add**.

De voorwaarde verschijnt bij **Condition List**.



- Klik vervolgens op **OK**.

De LDAP formulering voor de Query verschijnt bij Query string.



- Klik op **OK**.

Tip:

Refresh (F5)

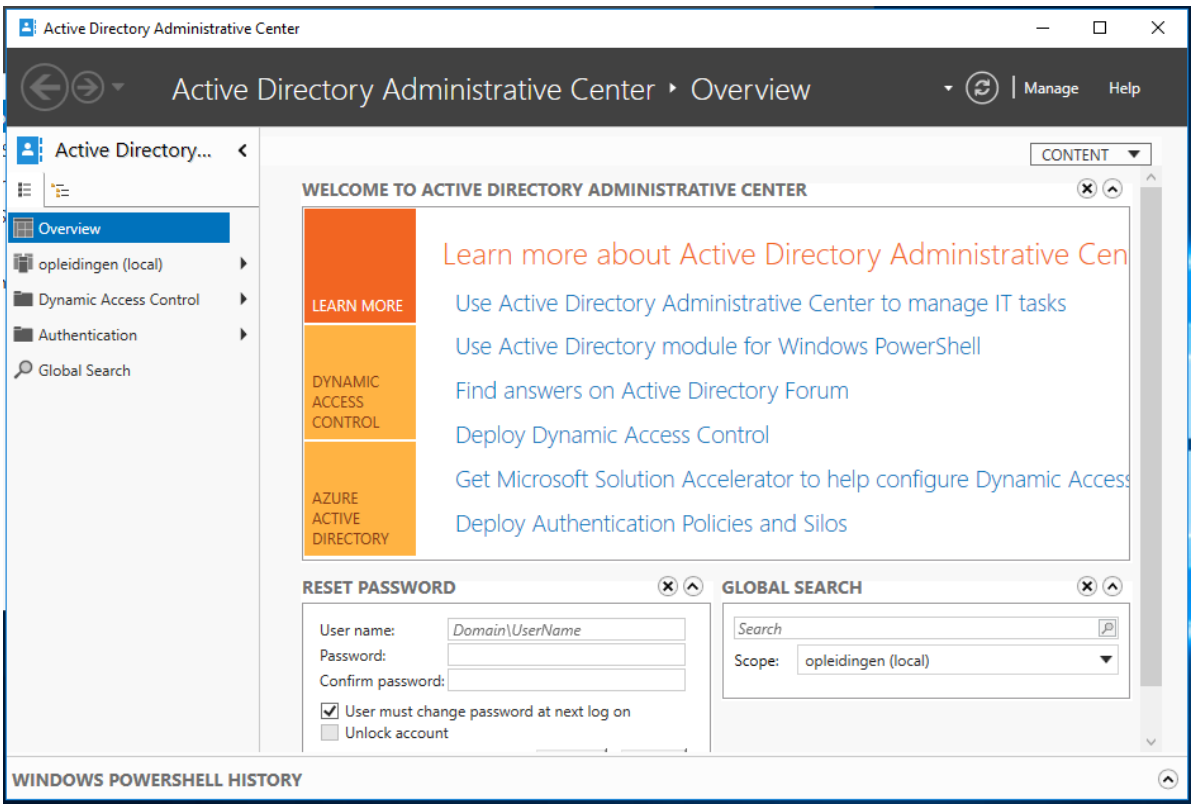
7.4 Active Directory Administrative center (ADAC)

Accountbeheer kan sinds release 2 van server 2008 niet alleen via ADUC, maar ook via ADAC.

Met ADAC kan je accounts en OU's aanmaken en beheren op alle domeinen en domeincontrollers die deel uitmaken van dezelfde instance van ADAC. Je kunt ook data filteren in AD DS via queries.

Het programma wordt meteen mee geïnstalleerd bij het opzetten van een domein.

Je vindt de toepassing o.a. via de **Server Manager** onder **Tools**.



Na het opstarten verschijnt een overzicht (Overview) van het administratief centrum. Standaard staan op dit startscherm drie tegels: Welcome, Reset Password en Global Search. Die tegels kunnen naar eigen voorkeur zichtbaar of onzichtbaar gemaakt worden via de lijst **Content** rechts bovenaan.

Met de **Breadcrumb bar** bovenaan kan je op een efficiënte manier naar eender welk object in de Active Directory navigeren. Het toont ook te allen tijde het momenteel geselecteerde object.

De **navigatiebalk** (navigation pane) links laat toe in Active Directory te bladeren in twee weergaves: list view of tree view.

- Selecteer het domein. Dat verduidelijkt wat je te zien krijgt in de andere delen van het venster.

Centraal vind je de **management lijst** met de inhoud van de momenteel geselecteerd container.

De **preview pane** onderaan toont allerlei informatie van het object dat, of van de container die geselecteerd is, in de management lijst.

Rechts in de taakbalk vind je de taken die je kan toepassen op de geselecteerde objecten.

Zoals vermeld komt het navigatiepaneel (links) met twee weergaves: **Tree View** en **List View**.

List View werkt met een lijst van laatst gebruikte containers. Die verschijnt automatisch onder een navigatie node en bevat de drie containers die laatst

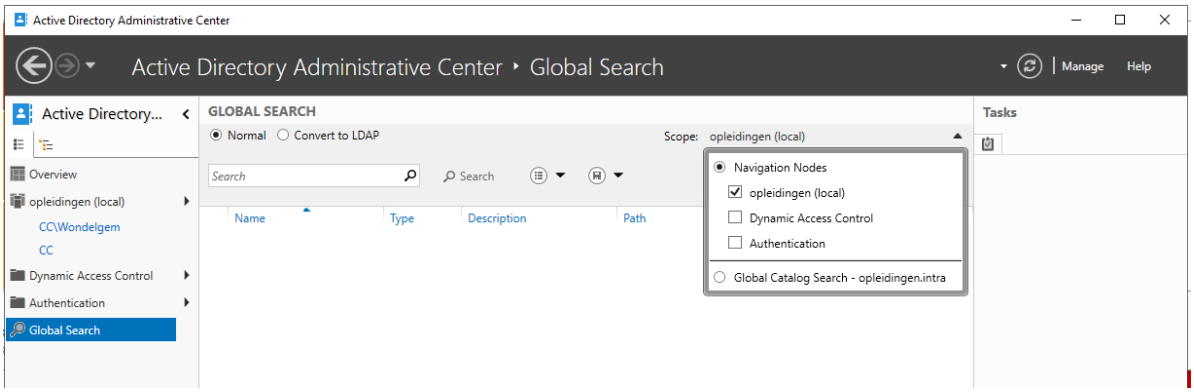
bezocht werden. Elke container die bezocht wordt komt bovenaan in de lijst onder de node. De onderste container verdwijnt dan uit de lijst.

Elke node beschikt ook over een Column Explorer om snel de inhoud van een container te ontdekken.

Tree View sluit meer aan bij de vertrouwde weergave van containers in ADUC.

7.4.1 Zoeken in AD met ADAC

Zowel in List View als in Tree View vind je onderaan in de navigatiebalk de node **Global Search**.

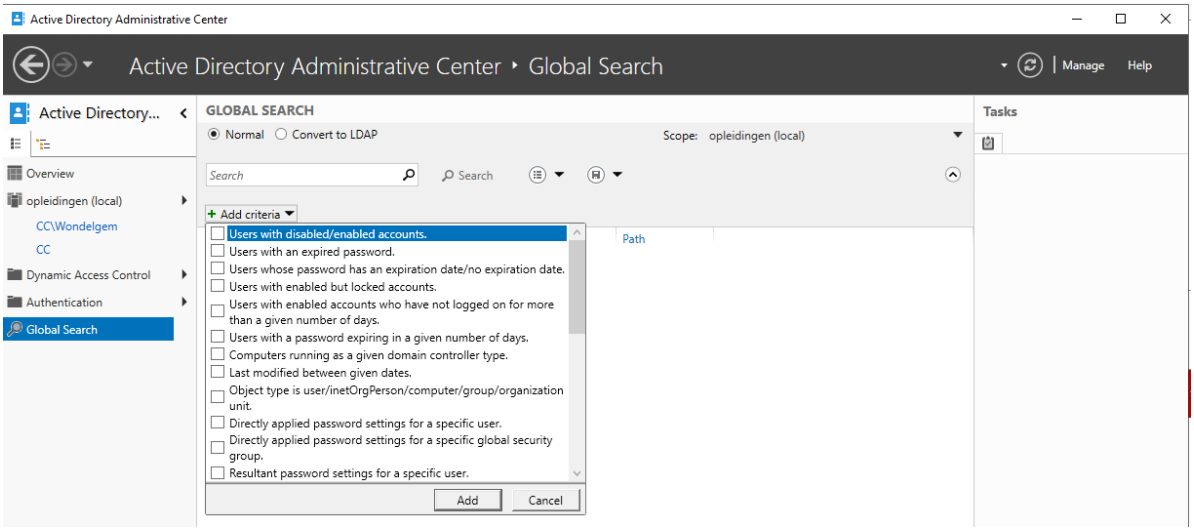


Rechts bovenaan bepaal je de scope waarbinnen je wil zoeken.

Je kunt op naam zoeken door die in het Search vak te typen.

- Zoek Janneke in je AD via Global Search.
- Klik met de rechtermuisknop op het resultaat. Je krijgt een menu met toegang tot de meest gebruikte beheeropdrachten voor een gebruikersaccount.

Andere criteria om op te zoeken komen ter beschikking door eerst de knop **Add criteria** toe te voegen via het dakje rechts in de management lijst.

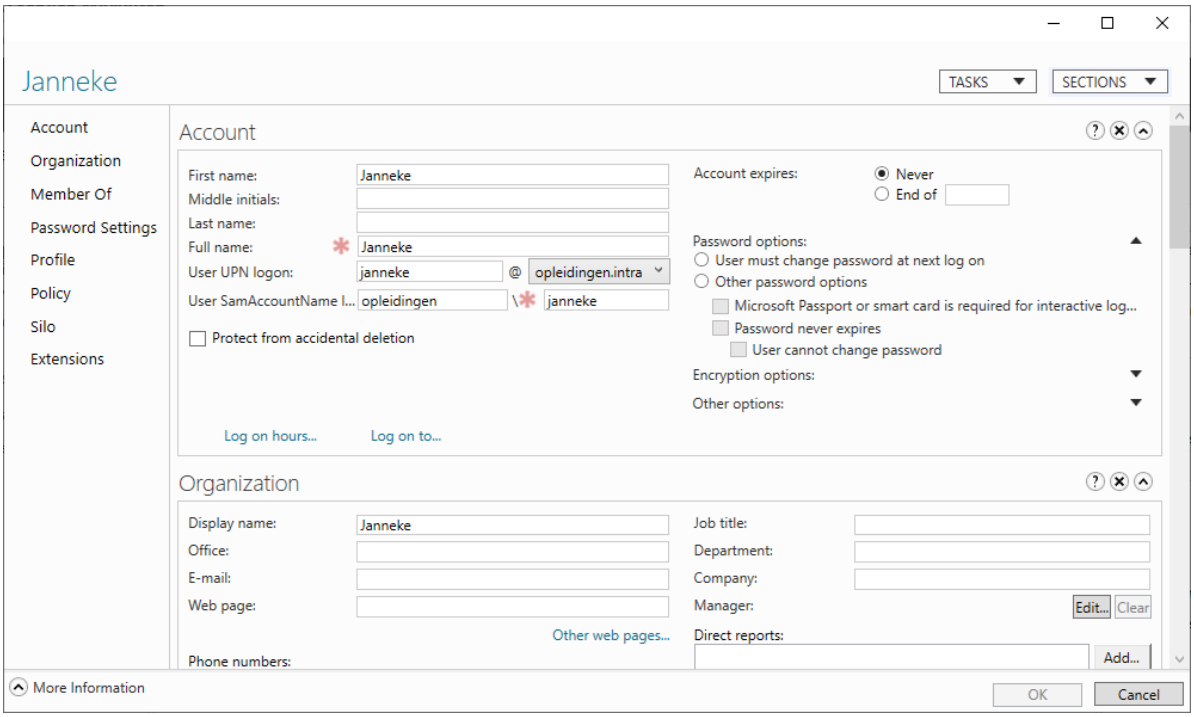


Om met een LDAP query te werken selecteer je bovenaan Convert to LDAP

Queries kunnen ook opgeslagen worden.

7.4.2 Pagina's met eigenschappen van een object

Klik op een object en kies rechts onder **Tasks** de optie **Properties** om de eigenschappen van een object op te roepen.



Elke pagina is opgedeeld in een aantal secties. Via de lijst **Sections** rechts bovenaan bepaal je welke moeten getoond worden en welke niet.
Via de lijst met alle getoonde secties (links) kan je van de ene sectie naar de andere navigeren.

7.4.3 Objecten aanmaken met ADAC

Via het contexmenu van een container kan je nieuwe objecten aanmaken in die container. Dit gebeurt door de eigenschappen van het nieuwe object in te vullen op een pagina. Verplicht in te vullen eigenschappen zijn aangeduid met een rode asterisks.

- 🛠 Maak een nieuwe OU met de naam Infrastructuur in de OU Antwerpen.
- 🛠 Maak een nieuwe gebruiker aan in die OU Infrastructuur.

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/advanced-ad-ds-management-using-active-directory-administrative-center--level-200-

7.4.4 ADAC en de AD Recycle Bin

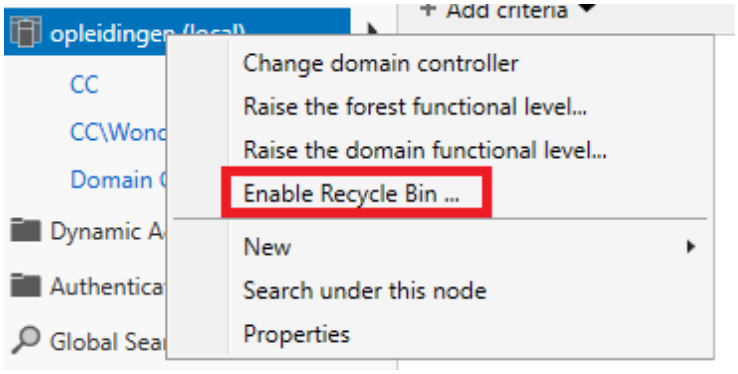
Het kan gebeuren dat een beheerder een object per ongeluk verwijdert uit de AD. Sinds Windows Server 2008 R2 komen uit de AD verwijderde objecten terecht in

een prullenbak. Oorspronkelijk kon die prullenbak alleen benaderd worden via de command-line. Windows Server 2012 introduceert via ADAC een grafische interface tot de AD Prullenbak.

Na installatie is de AD Prullenbak standaard niet ingeschakeld.

De prullenbak inschakelen kan op voorwaarde dat het forest functional level 'Windows Server 2008 R2' of hoger is en alleen met een account die behoort tot de Enterprise Admins of tot de Schema Admins.

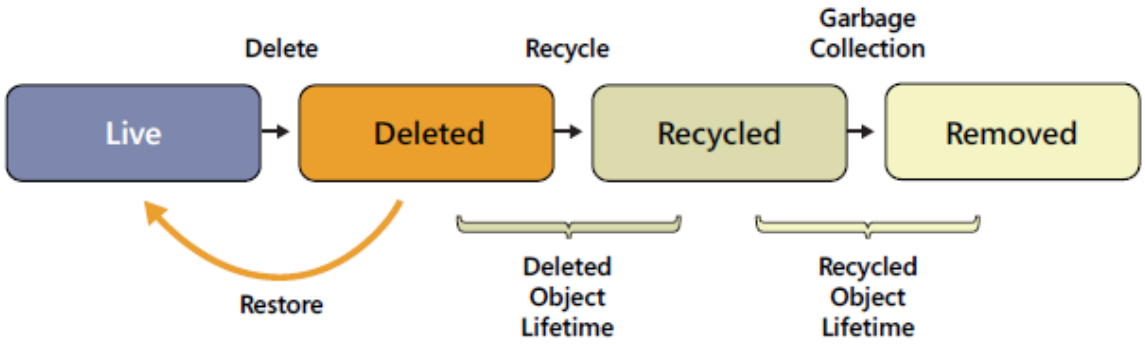
- Start indien nodig ADAC en klik met de rechtermuisknop op het topdomein van het forest.
- Geef de opdracht **Enable Recycle Bin**.



Er verschijnt een waarschuwing dat de AD Prullenbak niet meer kan uitgeschakeld worden.

Microsoft beschouwt het inschakelen van de AD Prullenbak weliswaar als een best practice, maar het forest functional level daarna terugdraaien wordt onmogelijk.

Na het inschakelen van de AD Prullenbak verschijnt een container Deleted Objects in AD en krijgt elk object één van vier mogelijke statussen:



http://techgenix.com/configuring-active-directory-recycle-bin/

Live	het object bestaat binnen AD in de juiste container en functioneert naar behoren.
Deleted	het object is verplaatst naar de container Deleted Objects in AD. Het object functioneert niet meer, maar zijn attributen bestaan nog, zodat

het object nog kan opgevist worden uit de prullenbak. De lifetime van het object is nog niet verlopen. Standaard wordt die ingesteld op 180 dagen zodra het object verwijderd wordt.

Recycled het object bevindt zich nog altijd in de Deleted Object container, maar de attributen zijn verwijderd. Het object kan niet meer gerecupereerd worden uit de prullenbak.

Removed de lifetime van het object is verlopen. Het AD garbage collection proces heeft het object verwijderd uit de directory database.

- Verwijder de gebruiker Janneke en stel vast dat die verschijnt in de container Deleted Objects.

Een verwijderd object uit de prullenbak halen is eenvoudig zolang de liftetime van het object niet verlopen is.

In de container Deleted Objects krijg je in het contextmenu van het object vier opties aangeboden:

Restore	Plaatst het object terug op zijn oorspronkelijke locatie in AD.
Restore To	Plaatst het object terug in een container die kan gekozen worden.
Locate Parent	Toont de container waarin het verwijderde object zich oorspronkelijk bevond
Properties	Toont de eigenschappen van het verwijderde object.

- Selecteer de container Deleted Objects in de navigatiebalk en roep het contextmenu op van het verwijderd object.
- Recupereer de account van Janneke op zijn oorspronkelijk locatie.

7.5 PowerShell

Een grafische interface werkt intuïtief en is geschikt om op kleine schaal objecten te beheren. Op grotere schaal kan het automatiseren van taken belangrijk zijn, zeker als taken op een regelmatige basis moeten uitgevoerd worden.

PowerShell kan daar een belangrijke bijdrage in leveren. PowerShell opdrachten worden gegeven aan een Windows PowerShell prompt.

- Start een Windows PowerShell prompt met administratorrechten op CL01.
- Vraag b.v. een overzicht van de opdrachten die ter beschikking zijn om gebruikers te beheren met Get-Command *ADUser

Er verschijnen vier cmdlets, de naam waarmee PowerShell naar opdrachten verwijst.

New-ADUser	om een nieuwe gebruiker aan te maken
Get-ADUser	selecteert één of meerdere gebruikers zodat er een opdracht kan op uitgevoerd worden
Set-ADUser	om de eigenschappen van een bestaande gebruiker aan te passen
Remove-ADUser	verwijdert de gebruiker uit de AD

Ondersteuning vragen bij een cmdlet kan met de cmdlet Get-Help gevolgd door de naam van de cmdlet waarover je uitleg wenst.

Update-Help haalt de laatste versie van de help op.

- 🛠 Vraag hulp bij de opdracht New-AdUser. Zoek het commando even op via je vertrouwde zoekmachine.

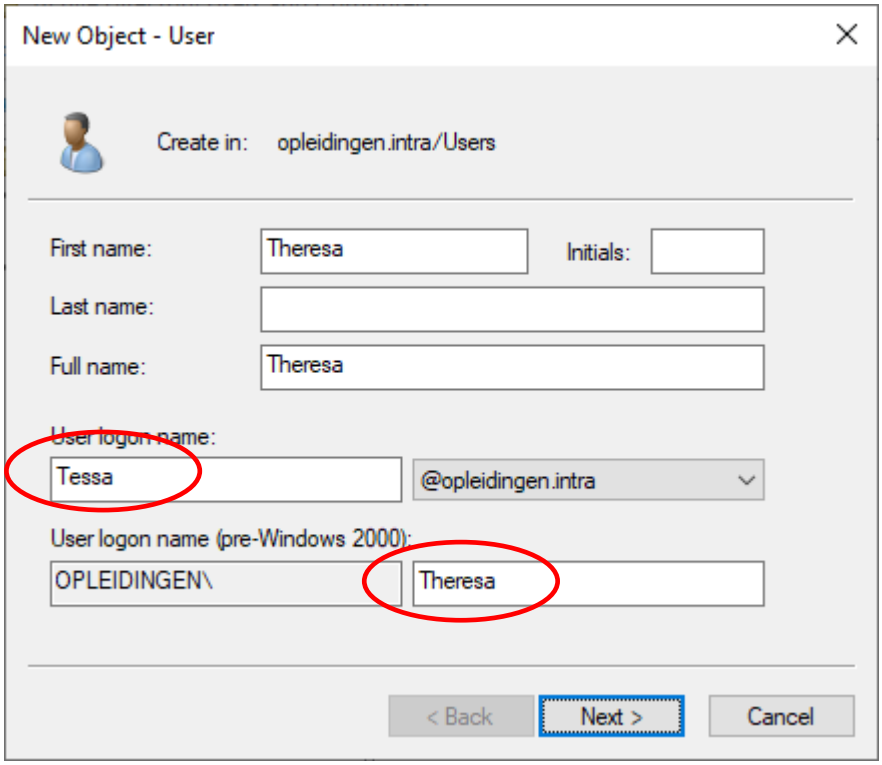
- 🛠 Maak een nieuwe gebruiker met PowerShell in de OU Genk.

Meer info over PowerShell vind je in de cursus bij de module PowerShell.

8 TOEPASSINGEN

8.1 Gebruikersaccounts

1. Maak een kopie van de administrator (beheerder) en geef die als gebruikersnaam je eigen voornaam.
2. Maak een nieuwe gebruiker in de container users en geef een verschillende naam in de vakken user logon name en user logon name (pre-Windows 2000).



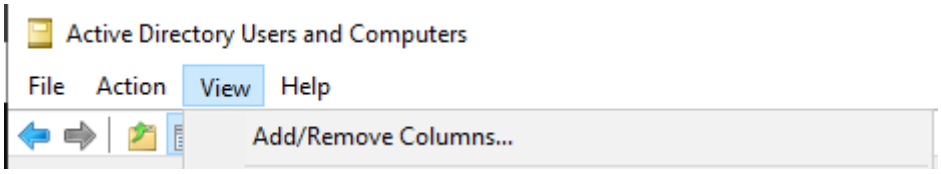
Meld met elk van de logonnamen aan op de client. Gebruik eerst Tessa@opleidingen.intra (of enkel Tessa), daarna opleidingen\Theresa

8.2 Organizational units

1. Gebruik het script setpwd.vbs om alle gebruikers in de OU CC het wachtwoord “Server2022” te geven.

2. Verplaats alle gebruikers die je geïmporteerd hebt uit ledenbe.csv naar de OU die overeenkomt met hun gemeente.

Tip:



3. Maak een OU “PC” en plaats hierin alle client computeraccounts.

8.3 Groepen

1. Maak per gemeente een groep met de cursisten van die gemeente.

2. Idem voor de instructeurs

3. Maak ook een groep waarvan alle instructeurs lid zijn en een groep waarvan alle cursisten lid zijn.

8.4 Query's in ADUC

1. Maak een query die alle gebruikers zoekt waarvan de logonnaam met een J begint. Sla de query op onder de naam LogonJ.

2. Maak een query die alle uitgeschakelde accounts opzoekt. Noem de query Uitgeschakeld.

9 COLOFON

Sectorverantwoordelijke:	
Cursusverantwoordelijke:	Jean Smits
Didactiek:	
Lay-out:	
Medewerkers:	Vakgroep netwerkbeheer
Versie:	Januari 2024
Nummer dotatielijst:	