Labo 1

Inleiding

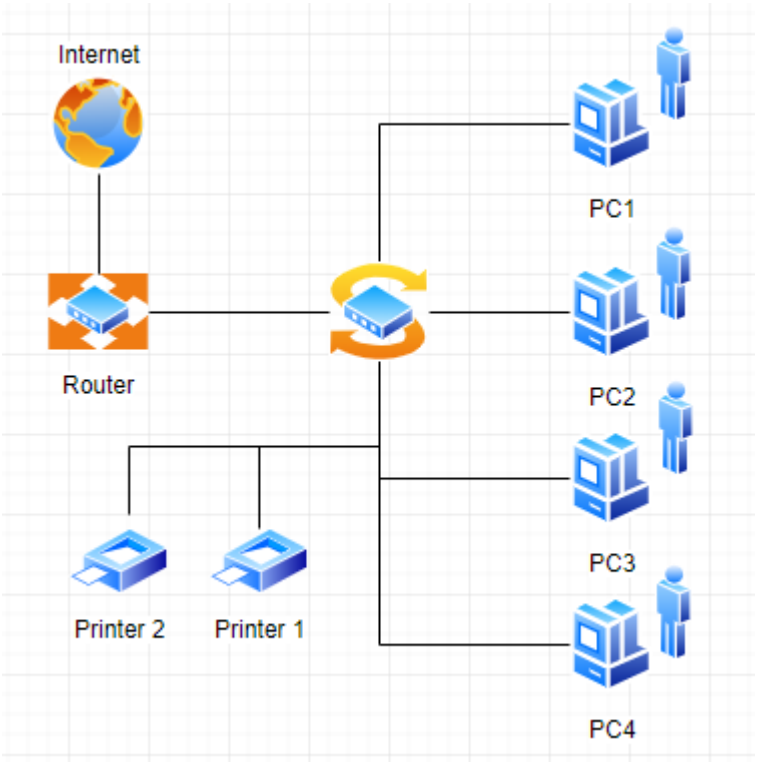
De firma Cosci heeft op dit moment een 70-tal Windows PC's. Iedere keer dat er een nieuwe werknemer is moeten de ICT-afdeling een nieuwe PC klaarmaken, er een lokaal account op maken, en deze gaan plaatsen op het bureau. Ook als iemand van afdeling verhuist moeten ze handmatig een nieuw account gaan maken op de PC die er staat. Iedere keer dat een gebruiker zijn wachtwoord vergeet, moeten zij op alle PC's waar deze gebruiker werkt aanmelden met het Administrator-account

De ICT-afdeling heeft gehoord dat dit efficiënter kan door de PC's aan een Active Directory-server te koppelen, waarop ze alle gebruikers vanop een centrale plaats kunnen beheren.

Labo omgeving

Netwerk

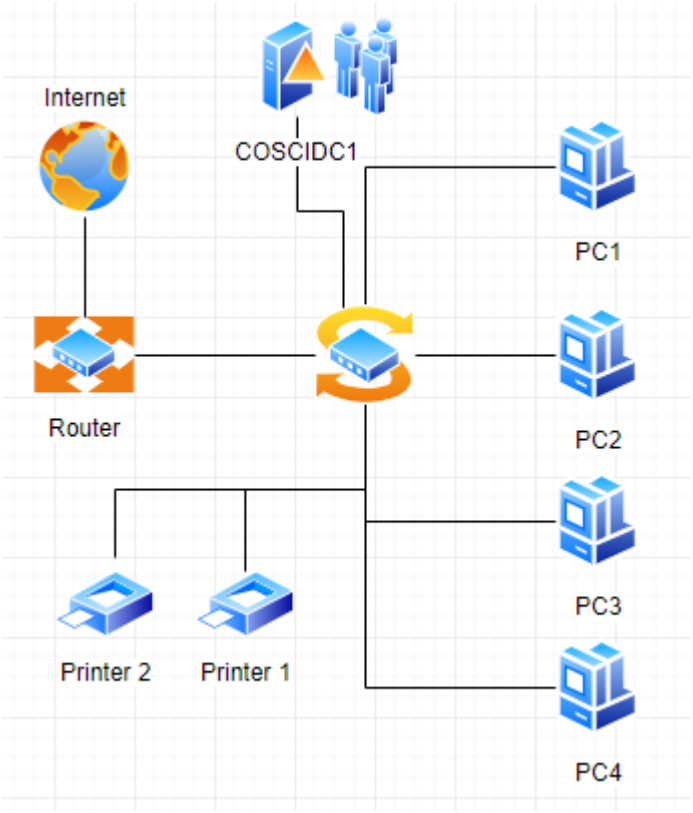
Dit is het netwerk zoals het er nu uitziet. We hebben 1 router die met het internet verbonden is. Aan de router hangt een switch, en op de switch hangen een heleboel PC's en printers.



Windows Domain

Om te beginnen aan dit labo moeten we eerst snappen wat een Windows Domain is. Een Windows Domain is een logisch netwerk, waarin alle user-accounts, computers, printers, netwerkschijven, ... geregistreerd zijn op 1 centrale server, de Domain Controller. Doordat alles centraal geregistreerd is kunnen we het ook centraal beheren. Dit geeft ons een heleboel mogelijkheden

1. Gecentraliseerd User-beheer: Alle gebruikersaccounts worden bijgehouden op de server, niet op de client PC's
2. We kunnen op de server bepalen welke users aan welke resources (printers, netwerkshares) kunnen.
3. Gemakkelijk te schalen wanneer het netwerk groter wordt.



In dit labo gaan we een Domain Controller installeren in ons netwerk, een PC toevoegen aan het domein, en kijken of we gebruikers kunnen aanmaken in de Domain Controller, die we dan laten aanmelden op onze PC.

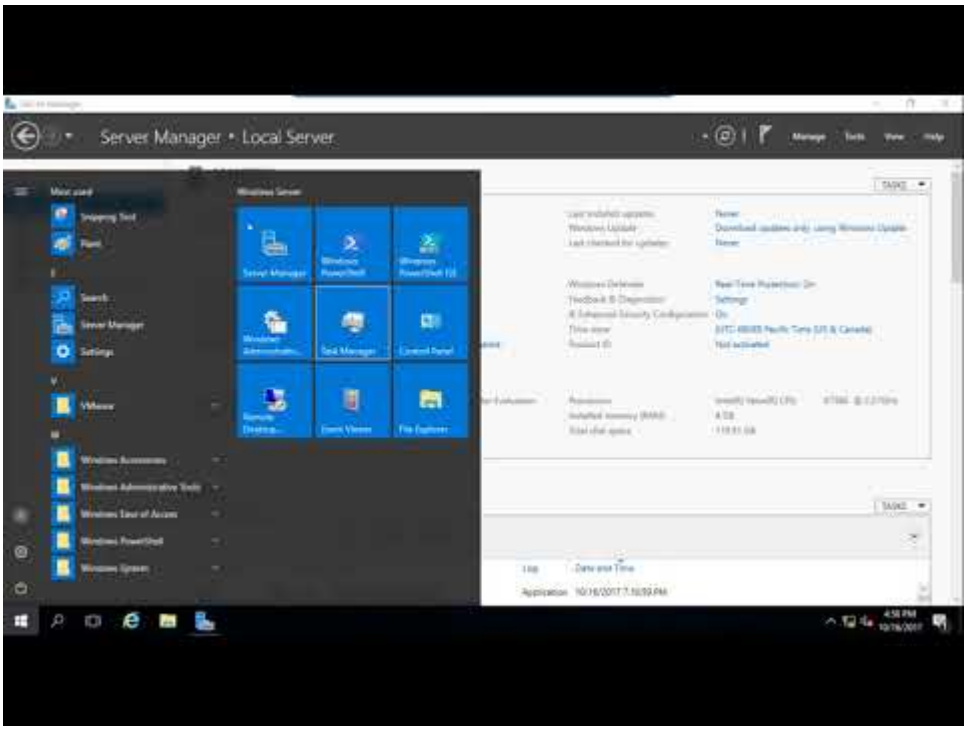
Installatie Windows

Om een Active Directory Server te installeren, moeten we eerst een Windows Server hebben.

1. Download Windows Server ISO van files.ucll.be
2. In VMWare selecteer je "Create a new Virtual Machine"
3. Je gebruikt de "typical" configuratie
4. Bij Installer-Disk-image selecteer je de ISO die je gedownload hebt. VMWare zal normaal gezien automatisch herkennen dat dit een Windows-Installatie is.
5. Je kan vanuit VMWare automatisch een user-account laten maken. Als gebruikersnaam gebruiken we "Administrator" en als wachtwoord "t".
6. Wanneer je volledig door de set-up bent gegaan zal Windows Server automatisch beginnen installeren. Op een gegeven moment vraagt de installer of je Windows Server Core of Desktop-Experience wilt gebruiken. Voor gebruiksgemak kiezen we hier voor Desktop-Experience.

Tijdens het wachten

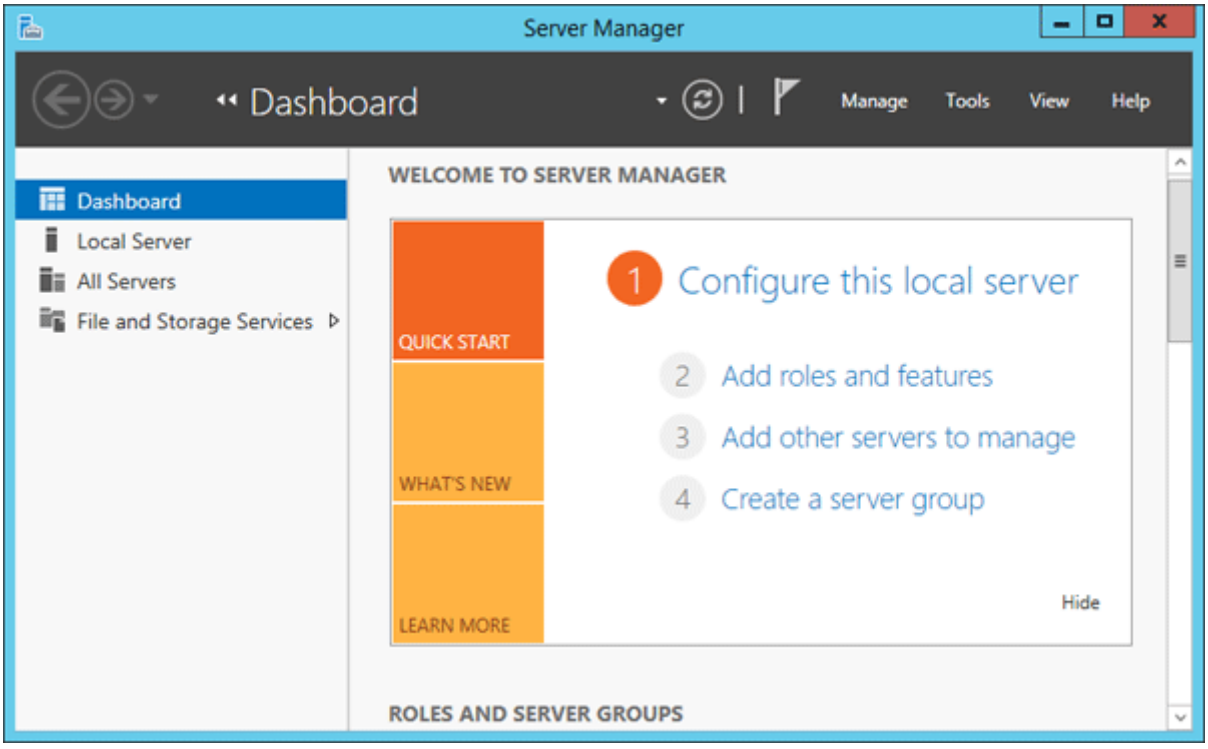
Terwijl je wacht op de installatie, bekijk je het volgende filmpje. Daarin wordt goed uitgelegd wat we allemaal kunnen doen met Active Directory, en met welke tools we Active Directory kunnen beheren.



Hiernaast willen we natuurlijk ook een client (gewone Windows 10 installatie) hebben. De procedure hiervoor is zeer gelijkaardig aan de server.

Om communicatie tussen de twee machines mogelijk te maken zal je Windows Device Discovery en File Sharing moeten aanzetten. Door dit te doen worden bepaalde poorten op de firewall opengezet, die belangrijk zijn voor het delen van bestanden en informatie voor Windows-machines. De gemakkelijkste manier is om de verkenner te openen en naar 'Netwerk' te gaan. Er verschijnt bovenaan een gele balk die meldt dat device discovery uitstaat. Je kan deze aanzetten door er op te klikken. Dit moet je uiteraard op beide machines doen. **Test hierna of de twee machines elkaar kunnen pingen.**

Windows Server Manager



Roles en features

Veel van de configuratie op Windows Server wordt gedaan in de Windows Server Manager, een programma dat standaard geïnstalleerd is op alle installaties van Windows Server. Met deze tool kan je een heleboel extra zaken op je machine installeren, zoals Active Directory, een DHCP server, een Fax-server, ... Deze zaken noemen we 'Roles', de "primaire" programma's.

Daarnaast kan je ook features installeren. Features zijn programma's of add-ons die niet zozeer impact hebben op de functionaliteit van de primaire services, maar extra functies voorzien. Een heel bekende feature is bijvoorbeeld Powershell, de bekende scripting-taal van Microsoft, die we in dit vak nog regelmatig zullen tegenkomen.

Servers

Natuurlijk, zoals de naam het zegt, is de primaire functie van de Server Manager het beheren van de Windows Server. Je kan deze tool echter ook op een lokale PC geïnstalleerd worden op zo vanop afstand servers te beheren. Dit hoeft niet op de desktop van de server zelf uitgevoerd te worden. Je kan servers toevoegen onder "Manage>Add Servers". Alle info over de servers die je hebt toegevoegd vind je onder 'All Servers'. Bij een nieuwe installatie staat daar natuurlijk maar 1 server, degene die we net geïnstalleerd hebben.

Installatie Active Directory

User Directory

Zoals we daarjuist gezegd hebben worden in een Domein alle gebruikersaccounts centraal bijgehouden. De database waarin deze worden opgeslagen noemen we een 'Directory'. Er zijn een heleboel Directory-softwarepakketten (OpenLDAP, Samba, FreeIPA, 389 Directory Server, ...) maar verreweg de meest gebruikte is en blijft Windows Active Directory. Deze kunnen we natuurlijk heel eenvoudig installeren op onze Windows Server.

Voorbereiding

Eerst en vooral gaan we de server een logische naam geven. Open de Server Manager en ga naar 'Local Server'. Klik daar op de computernaam, vervolgens op 'Change...'. We geven de server de naam 'COSCIDC1' (zie netwerktekening). Om die wijzigingen door te voeren moet je de server opnieuw opstarten.

Stel ook een statisch IP in. Hiervoor neem je best het IP dat door de DHCP-server is toegekend, samen met het subnet-mask en de default-gateway.

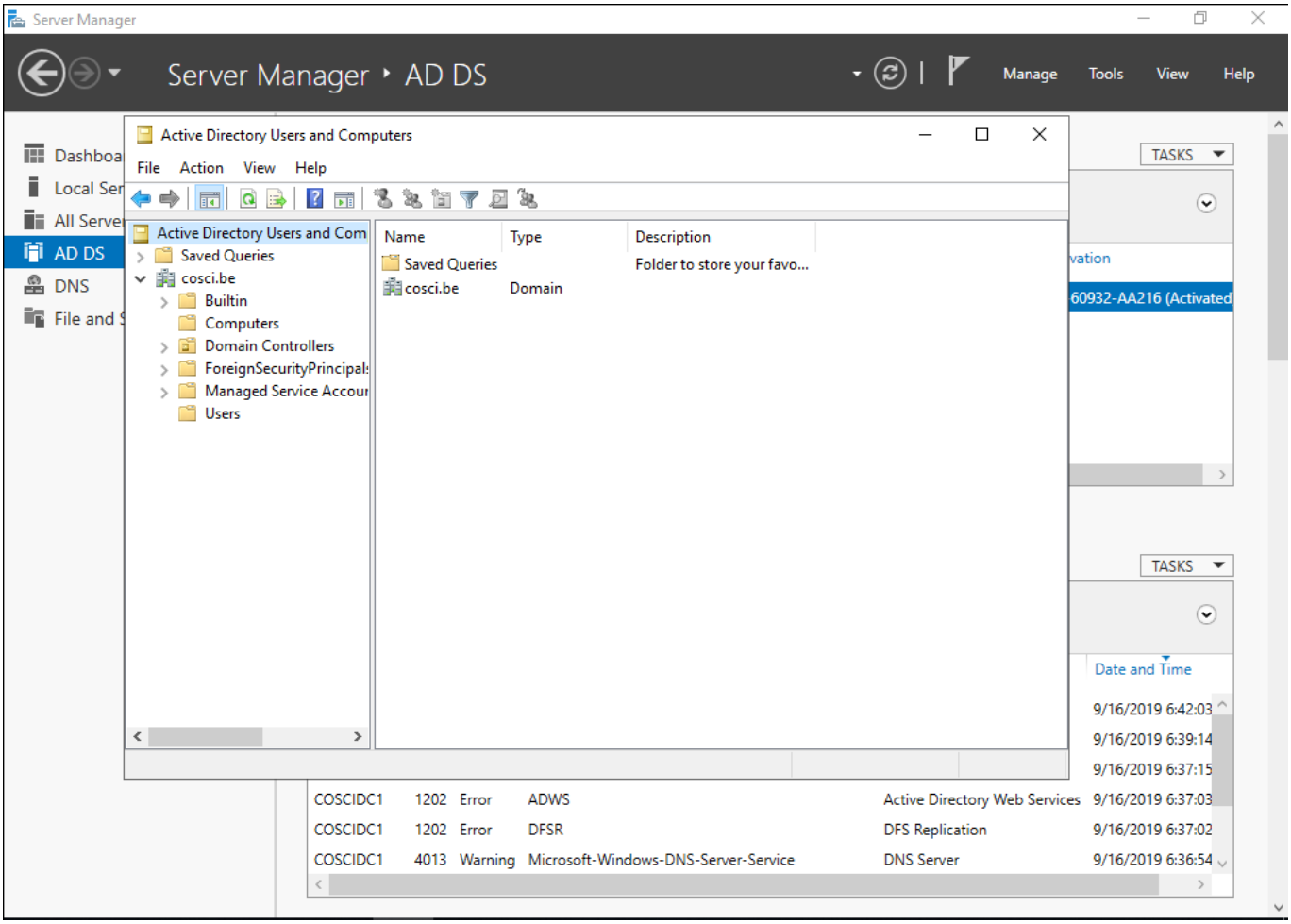
Installatie

1. Klik in Server Manager op "Manage" rechtsbovenaan en selecteer "Add Roles and Features".
2. Bij Installation Type kies je voor "Role-based or feature-based installation".
3. Onder "Server Roles" kies je voor "Active Directory Domain Services", het belangrijkste onderdeel van Active Directory. Pas als dit onderdeel op de server geïnstalleerd is, spreken we van een Domain Controller.
4. Loop verder door de installatie. Deze begint vanzelf. Wanneer de installatie gedaan is krijg je de melding "Configuration required". Klik door op "Promote this server to Domain Controller". Je krijgt een venster "Deployement configuration."

5. Gezien dit onze eerste Domain Controller is, willen we een nieuwe forest maken. Er wordt gevraagd om een "Root domain name". Die is in ons geval cosci.be, de domeinnaam waarvan we willen vertrekken voor de rest van onze domeinen.
6. In Domain Controller laten we Domain Name System (DNS) server aangevinkt. Dit zal automatisch een DNS-server installeren voor het domein cosci.be, wat we later in de labo's nog nodig zullen hebben.
7. Onder additional options laten we de NetBIOS domain name staan op 'COSCI'. Dit is een verkorte naam waarmee we later kunnen verwijzen naar het domein.
8. Loop verder door de installer. De server moet herstart worden nadat de installatie voltooid is.

Controle

Als je alle bovenstaande stappen hebt gevolgd, heb je nu een Active-Directory server geïnstalleerd, met als root-domain cosci.be. Daarnaast is er ook automatisch een DNS-server geïnstalleerd, met de juiste records voor cosci.be. Om dit na te gaan openen we het programma "Active Directory Users and Computers". Als je alles goed gedaan hebt zie je cosci.be als domein staan.



Een PC verbinden met het domein

Natuurlijk willen we de PC's nu verbinden met het domein. Hiervoor moeten we eerst de Domain Controller die we zonet hebben ingesteld configureren als DNS-server voor onze client.

Hierna gaan we onze PC identificeren in het domein. Dit doen we door naar de Systeem-instellingen van de client te gaan (Open verkenner, rechtermuisknop op 'Deze pc' en klik op eigenschappen), en daar te kiezen voor 'Instellingen wijzigen'. Van hieruit klik je op wijzigen, geef je de PC een logische naam, en als domeinnaam geef je 'cosci.be' in. Hierna vraagt de PC om een gebruikersnaam en wachtwoord, waar je

administrator-credentials van de Domain Controller moet invullen. De verbinding wordt verder automatisch gemaakt, en er wordt gevraagd om de PC opnieuw op te starten om de wijzigingen door te voeren.

Wat gebeurt hier nu eigenlijk?

Wat gebeurt er allemaal in de achtergrond? Doordat we onze server als Domain Controller hebben ingesteld, worden alle DNS-queries van de client naar de server gestuurd. Op de server hadden we al een DNS-server geïnstalleerd toen we de Active Directory installeerden, dus onze server kan op die queries ook antwoorden. Toen we in de PC 'cosci.be' als domein opgaven, ging de PC dus een DNS-query uitsturen voor 'cosci.be', naar onze server. Deze DNS-query is echter een beetje speciaal, hij zoekt namelijk niet gewoon naar het IP-adres van het domein, maar naar een heel specifiek record, een SRV-record. Een SRV-record is een record in DNS waarin je een bepaalde service beschrijft, alsook het ip, de poort, en de priority van deze service.

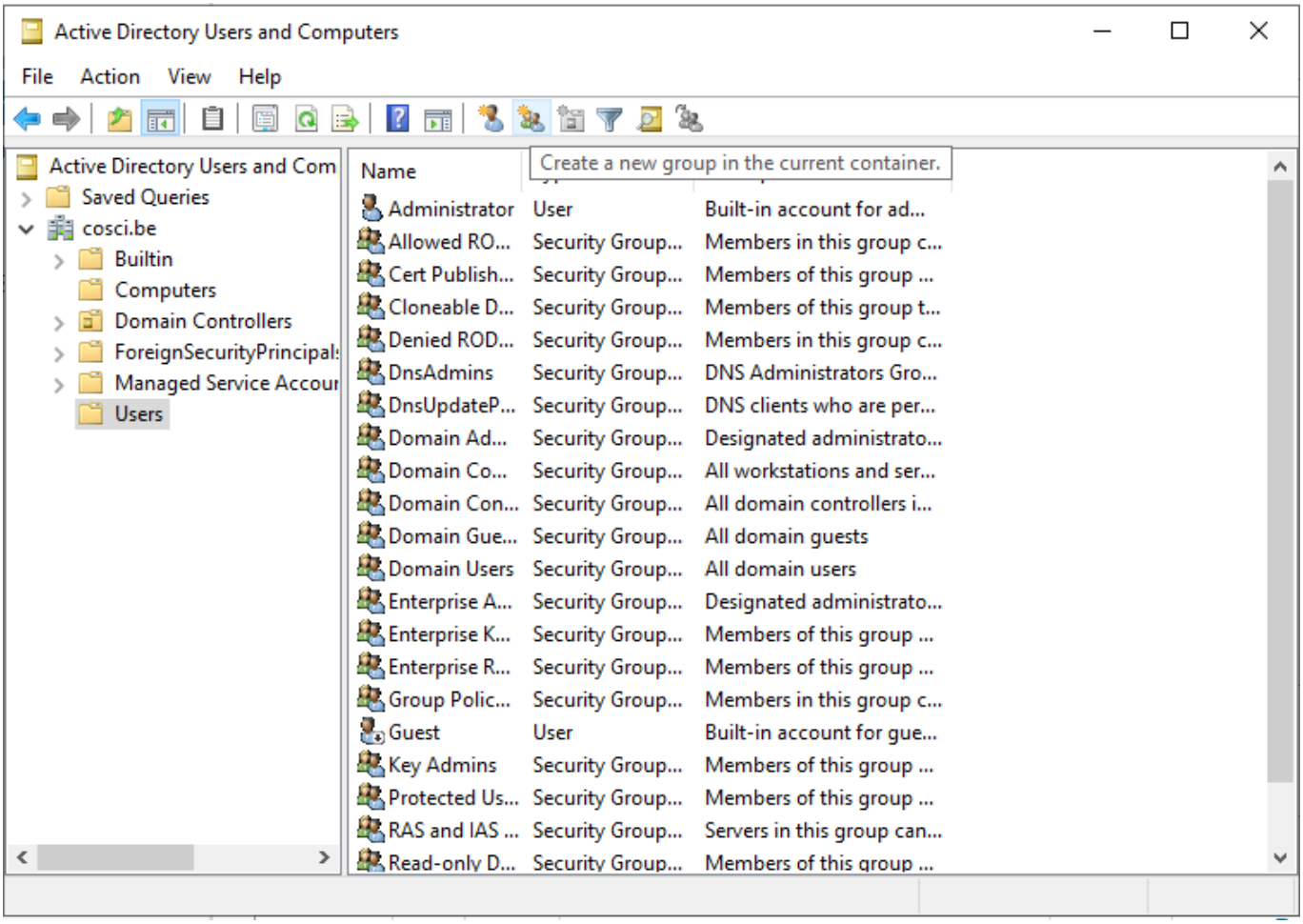
Hieronder zie je de afdruk van een NSLookup. Op een gegeven moment wordt er een query gedaan naar '_ldap._tcp.dc._msdcs.cosci.be', en de client krijgt als antwoord het IP en de poort waar het op draait. Dit gebeurt ook in de achtergrond wanneer we een client identificeren in het domein.

Test dit zeker zelf ook eens uit. NSLookup is een tool die je veel nodig gaat hebben voor het opsporen van problemen. Het volledige commando hier uitleggen met al zijn opties is omslachtig. De help-functie en Google zijn uw vriend.

```
C:\Users\Administrator.COSCI>nslookup
Default Server:  UnKnown
Address:  192.168.29.129

> set type=all
> cosci.be
Server:  UnKnown
Address:  192.168.29.129

cosci.be        internet address = 192.168.29.129
cosci.be        nameserver = coscidc1.cosci.be
cosci.be
        primary name server = coscidc1.cosci.be
        responsible mail addr = hostmaster.cosci.be
        serial  = 25
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
coscidc1.cosci.be       internet address = 192.168.29.129
> _ldap._tcp.dc._msdcs.cosci.be
Server:  UnKnown
Address:  192.168.29.129

_ldap._tcp.dc._msdcs.cosci.be   SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = CosciDC1.cosci.be
CosciDC1.cosci.be       internet address = 192.168.29.129
>
```

Gebruikers aanmaken in het domein

De volgende stap is om gebruikers aan te maken in het domein. Hiervoor gaan we terug naar de server, en openen we de Active Directory Users and Computers-tool (ADUC). Als je de tab cosci.be openklikt, zie je een aantal voorgemaakte mapjes staan. Als je op Computers klikt, zal je de PC die we zonet hebben geïdentificeerd zien staan. Als je op Users klikt zie je een heleboel voorgemaakte groepen en enkele users. In deze map willen we een nieuwe groep maken, met de naam 'System Administrators'.



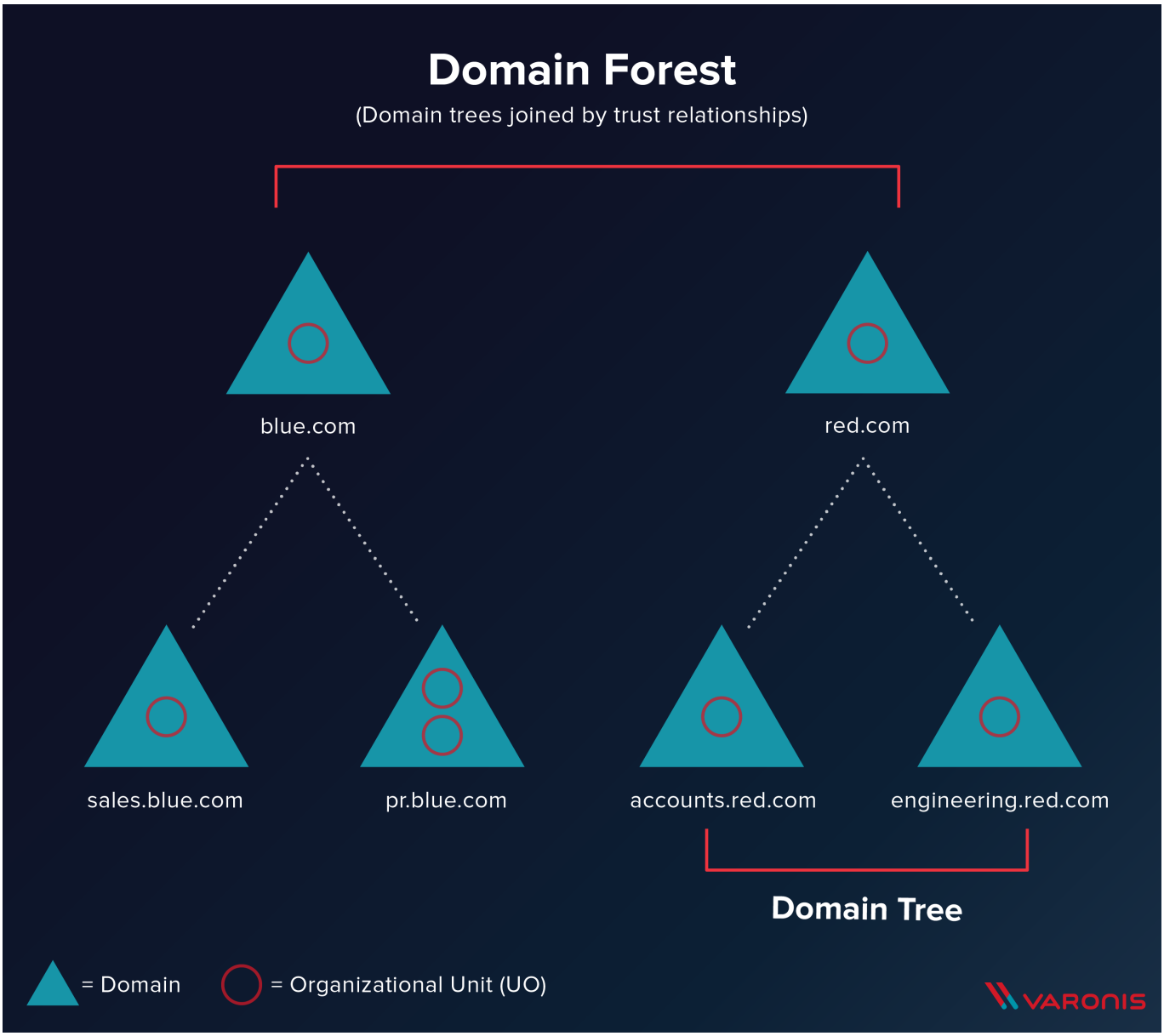
We laten de Group Scope op global staan, en als Group-type kiezen we Security. Daarna maken we een nieuwe user, waar je je eigen gegevens mag invullen. Als User Logon name mag je in principe invullen wat je wilt, maar het gemakkelijkste is om het formaat voornaam.familienaam te hanteren. Ten slotte voegen we de user die we net gemaakt hebben toe aan de groep System Administrators.

Als je dit allemaal gedaan hebt kan je terug naar de PC gaan, klik je op andere gebruiker, en meld aan met voornaam.familienaam en het wachtwoord dat je hebt ingesteld.

AD Design

Wat we nu eigenlijk hebben gedaan is het opstellen van een Single Domain Active Directory. Er zijn echter een aantal gevallen waarin we misschien naar meer gecompliceerde setups willen gaan.

Trees en forests



In bovenstaande afbeelding stelt iedere blauwe driehoek een Domain Controller voor. Zo zie je dat het bedrijf blue.com een DC heeft voor hun domeinnaam. Hun bedrijf is echter zo groot dat ze ervoor gekozen hebben dit nog verder op te splitsen in subdomeinen. Voor deze subdomeinen hebben ze ook een aparte DC gemaakt, en deze gekoppeld aan de bestaande DC voor het root domein. (Herinner je een van de eerste stappen van de installatie van Active Directory, waar je moet kiezen tussen een nieuw domein aan te maken, of een DC koppelen aan een bestaand domein). Hierdoor krijg je een soort hiërarchische verhouding, en spreken we van een Domain Tree. Alle resources die in een van de subdomeinen worden toegevoegd, zijn in alle subdomeinen beschikbaar dankzij de automatische verbinding die door de tree wordt gelegd. De voornaamste redenen dat men dit soort architectuur hanteert is als men zeer grote organisaties heeft, trafiek wilt verminderen naar de root, ...

Daarnaast is het ook mogelijk om verschillende trees van verschillende domeinen aan elkaar te koppelen via een trust. Stel bijvoorbeeld dat blue.com beslist te gaan samenwerken met red.com, kan men een trust tussen de 2 trees leggen, waardoor de resources van de ene tree naar de andere overgedragen worden. Zo gaan gebruikers van blue.com zich zelfs in de gebouwen van red.com kunnen aanmelden op de PC's.

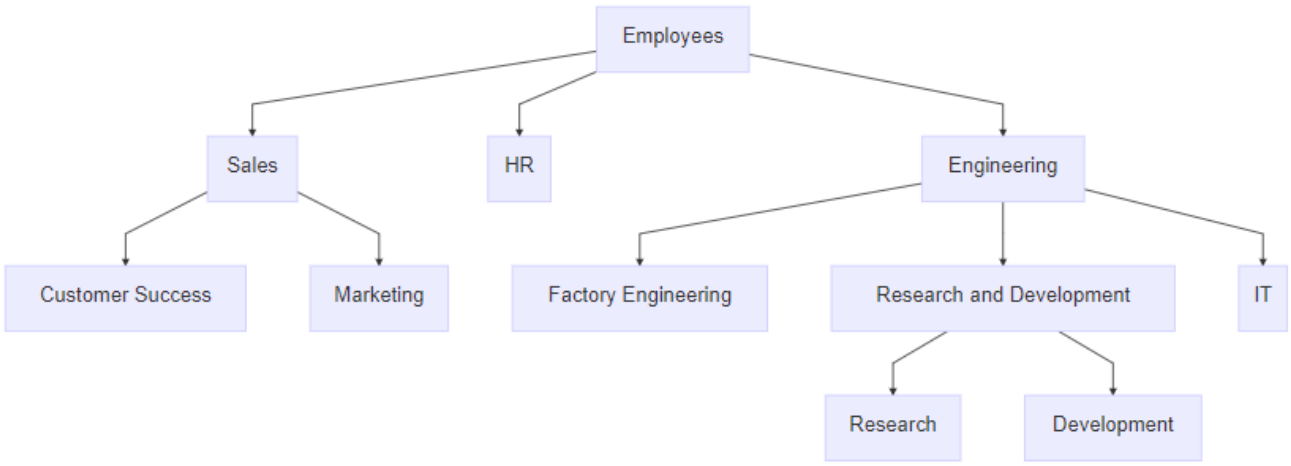
Voor meer info over design van een Active Directory, lees je best dit artikel.

Organizational units & groups

Wat echter veel meer voorkomt zijn organizational units & groups. Eerst en vooral is het verschil tussen de 2 te snappen. Organizational Units reflecteren vaak de structuur van de organizatie, bijvoorbeeld de OU "Werknemers", waaronder dan de OU "HR", de OU "Sales" en de OU "Engineering" zitten. Ze werken van een grote groep, naar steeds specifiekere groepjes, in een omgekeerd hiërarchisch model. OU's erven altijd de rechten en configuratie over van hun parent, maar kunnen verder gespecifieerd worden. Ze worden vooral gebruikt om Group Policies op te configureren. Een gebruiker kan ook maar in 1 van de OU's zitten, en heeft dus alleen effect van de OU waar hij inzit en degene die erboven liggen. We komen later in de labo's hier nog op terug.

Groepen daarentegen, hebben minder sterk die hierarchie, en dienen vooral voor het rechten geven op bepaalde bedrijfsresources. Een gebruiker kan wel in meerdere groepen zitten. Ook groepen kunnen genest worden, simpelweg door een groep lid te maken van een andere groep. Alle leden zullen bijgevolg ook door de configuratie van die groep beïnvloed worden. Daarnaast kan je aan groepen ook zaken als gedeelde mailboxen koppelen.

Probeer nu op de root van het domein de volgende structuur aan te maken met behulp van OU's.



Maak daarnaast ook de volgende groepen.

1. IT-admins
2. Wifi-users
3. BadgeReader-users
4. Employee-administration

En voeg IT-Admins als een groep toe aan Wifi-users. Voeg jezelf ook toe aan de IT-admins groep, en controleer of je daarmee ook toegevoegd bent aan de Wifi-users groep.

Scripting

Bij systeembeheer komen altijd repetititieve taakjes kijken, en dat is bij Windows Active Directory niet anders. Daarom heeft Windows een heel krachtige scripting-taal, namelijk Powershell. Powershell is een taal ontwikkeld door Microsoft, wat maakt dat het enorm goed kan interageren met zaken als AD. Daarom hieronder enkele oefeningen.

Users maken

Ontwikkel eerst en vooral een scriptje waarmee je 1 user kan aanmaken, als je de opties voornaam en naam meegeeft. De gebruikersnaam wordt automatisch ingesteld op voornaam.familienaam

Veel users aanmaken

In het labo vind je een Excel-bestand met een heleboel namen. De bedoeling is dat je deze namen allemaal automatisch inleest en de gebruikers eruit aanmaakt.

Password resets

Maak een scriptje om het wachtwoord van een gebruiker te resetten. Wanneer het wachtwoord geresetted is wordt het gebruikersaccount automatisch ontgrendeld, de gebruiker krijgt een tijdelijk wachtwoord en moet zijn wachtwoord aanpassen de volgende keer dat hij aanmeldt.